Internal Audit – The Challenge

Handouts

Day 1, 7th of September

The 2006 European Conference of Internal Audit

6–8 September, 2006

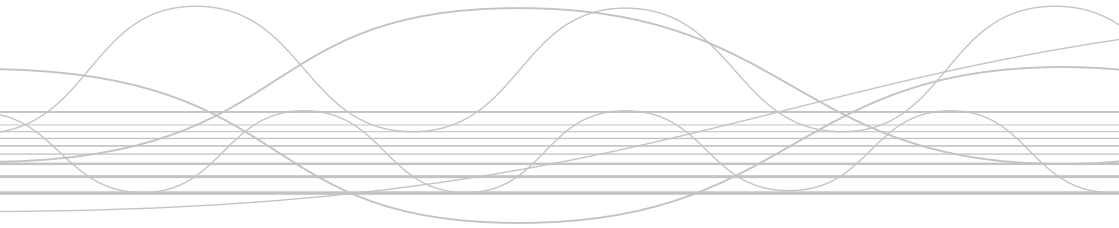
Hilton Helsinki Kalastajatorppa

ECIIA

European Confederation of Institutes of Internal Auditing

Contents

Conference opening



WELCOME !

6 – 8 September, 2006

Hilton Helsinki Kalastajatorppa

The Institute of Internal Auditors
Finland
1956–2006

European Confederation of Institutes of Internal Auditing
The Institute of Internal Auditors - Finland

General Session 1
Status of the Profession in Europe

Richard Nelson (GBR)
Chairman of the ECIIA Board

ECIIA
Conference 2006
Internal Audit - The Challenge

Richard Nelson
President ECIIA

Helsinki, Finland
6th to 8th September 2006

ECIIA Helsinki Conference

Status of the Profession in Europe

The Challenges

- Rapid Change
- Greater Opportunities
- Challenge to Perform
- Potentially More Legislation
- More Direction from the EU
- An Opportunity to be Grasped

History

- The IIA, Inc. was founded in 1941 in New York City, USA
- First chapter outside of United States was formed in 1944 in Toronto, Canada
- First chapter outside North America was formed in 1948 in London, England

ECIIA

- Founded 1982
- Confederation of 31 countries
- Management Board from 8 countries
- No individual members only countries

The IIA Vision

The IIA will be the **global voice** of the internal audit profession:

Advocating its value, promoting best practices, and providing **exceptional service** to its members.

ECIIA Purpose

- To represent internal audit to European Union and any other European institutions of influence.
- To promote the profession within the wider geographic area of Europe and the Mediterranean basin.

ECIIA Vision for Internal Audit

- The IIA to be recognised as the primary body representing internal audit in Europe.
- For internal audit to be recognised as a vital component in an effective organisation.
- To have a consistent approach and understanding across Europe.
- The IIA standards and code of ethics become the accepted standard across Europe.
- Our members to be recognised as the experts in the field of internal auditing.
- To be the first port of call on internal audit matters.

The Five Pillars of Governance

- Shareholders
- The Board
- Executive management
- Statutory auditors
- Internal auditors

EU Actions

- The Winter Report
  - Corporate governance statement
  - Internal controls
  - Risk management systems
  - Public interest entities

EU Actions

- Listed companies
- AC to monitor effectiveness of: I/C, risk management systems and internal audit
- European Corporate Governance Forum
- Group of non governmental experts on corporate governance

EU Conclusions

- No European SOX 404
- No European wide risk management or internal control framework
- No European governance code

Internal Audit Role

- To review the corporate governance processes within the organisation to ensure ‘fit for purpose’
- To provide reasonable assurance about the adequacy and effectiveness of the risk management and control framework in place
- To provide assurance that the significant risks are being managed effectively
- To facilitate the strengthening and improvement of the corporate governance framework

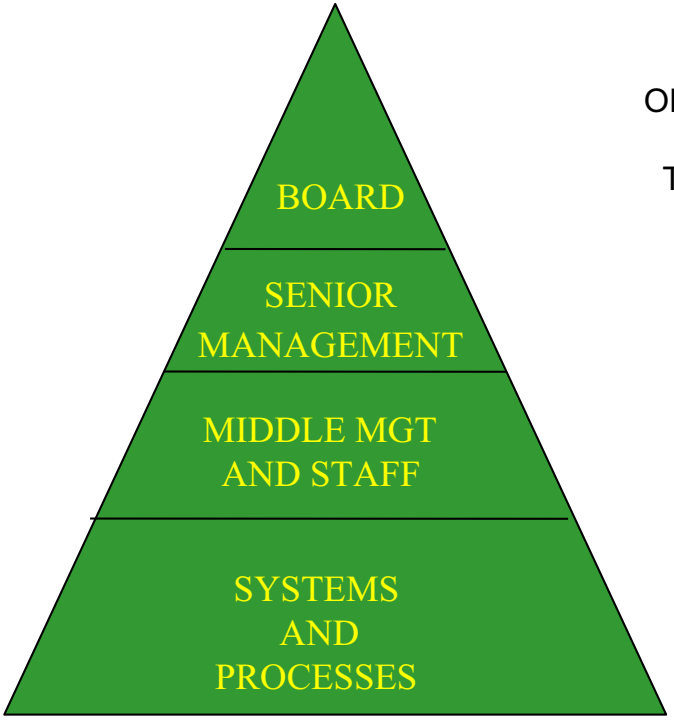
Principles of Good Governance

- Stakeholder input to the business.
- Relevant and reliable public reporting.
- Avoidance of excessive power at the top of the business.
- A balanced board composition.
- A strong, involved board of directors.
- A strong independent element on the board.
- Effective monitoring of management by the board.
- Competence and commitment.
- Risk assessment and control.
- A strong audit process (both internal and external).

Enterprise-Wide Risk Management

A structured, consistent and continuous process across the organisation for identifying, assessing, deciding on responses and reporting on opportunities and threats that affect the achievement of its objectives.

ERM Process



STEP 1

OBJECTIVES & TARGETS

STEP 2

THREAT IDENTIFICATION & MITIGATION

STEP 3

ASSURANCE

Assurance on Risk Management

- Strategy and objectives setting
- Risk identification and analysis
- Adequacy of response to risk including cost effectiveness
- Accuracy of monitoring
- Response to issues shown up by monitoring
- Response to critical incidents and near misses

ERM and Internal Audit -The Safeguards

- ***Management is responsible for risk management.***
- Internal audit should not:
  - Undermine management accountability
  - Manage risks on managements behalf
  - Make risk management decisions
  - Give assurance on any part of the risk management framework for which they have responsibility.

Internal Audit's Role in ERM

Advantages of a Risk Based Approach

- Enables an annual opinion
- Focuses audit on the big issues
- Gives the Board control over audit
- Responsive to changing events
- More interesting and challenging work

How Internal Audit Can Help

- Educate the board
- Review the risk management process
- Audit the key risks
- Establish communications with directors
- Review the operation of the board
- Be a centre of excellence
- Assess how companies deal with the unexpected

Overview of IA Requirements

- Competent professionals
- Independence of internal audit
- Properly resourced
- Covers all type of risks
- No limit to the scope of work
- Encourage EU to require firms to have effective internal audit as one of the key components of good governance

Traditional Internal Auditors Attributes:

- Analytical skills
- Financial expertise
- Internal control expertise
- Writing skills
- Logical thinking
- Fraud detection skills

Benchmarking: What Should be the Role of the Internal Auditor?

• Checker	44.6%
• Advisor	57.0%
• Consultant	45.6%
• Management sparring partner	34.7%
• Other	32.1%

Source: Global Audit Information Network Flash Survey – June 2003

Future Influences on IA

- Corporate Governance
- Information & communications technology
- E - commerce
- Relationship with the Board
- Increased demand for IA
- Business risks

Future Influences on IA

- Working with other risk management professionals
- Demand for independent assessment of IA
- Need to improve understanding about IA
- Facilitation expertise
- Globalisation of business and job market

Critical Characteristics of the 21st Century Internal Auditor

- Risk-based orientation
- Global perspective
- Governance expertise
- Technologically adept
- Business acumen
- Creative Thinking and Problem Solving
- Strong ethical compass
- Facilitation/Communication and Coaching skills
- Leadership

Best Practices

- Apply the IIA Code of Ethics
- Have an Audit Charter
- Internal audit to have direct reporting line to the Chief Executive and the Board
- Internal audit key objective to support the Board by providing assurance about the risk management systems
- Audit Committee to ensure internal audit is adequately resourced and staffed.

Best Practices

- To have a quality assurance process for internal audit.
- To use a business risk based internal audit approach.
- To promote internal controls that mitigate risks across the organisation
- To cooperate with other assurance providers

The Opportunities

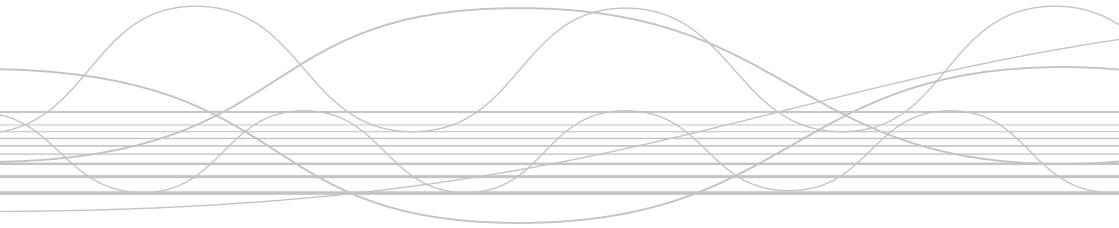
- The future is bright
- Be proactive
- Be a leader
- Seek to become a trusted advisor to your Board
- Aim to surprise and delight
- The opportunity is there for the taking

ECIIA
Conference 2006
Internal Audit - The Challenge

Richard Nelson
President ECIIA

Helsinki, Finland
6th to 8th September 2006

General Session 2
The Risk Intelligent Internal Auditor



Rick D. Funston (USA), Principal, US Practice Leader, Governance,
Risk Oversight and Enterprise Risk Management, Deloitte
Eric Hespenheide (USA), Managing Partner, Global Internal Audit Services, Deloitte

The Risk Intelligent Internal Auditor

Presented to the ECIIA
Eric Hespenheide
Rick Funston
September, 2006

This presentation is incomplete without the accompanying discussion

Outline

- Why is risk management such a hot topic?
- What is wrong with risk?
- The value proposition for improving risk intelligence
- The evolution of risk assessment
- A new paradigm for risk assessment
- The implications for the enterprise and internal audit

Where Would We Be Without Risk?

- How many of your jobs depend on risk?
- How many of your companies would prosper if they didn't take risk?

"A ship is safe in a harbor – but that's not what ships are for." **John A. Shedd**

Why Is Risk Management Such a Hot Topic?

- **Unanticipated Losses**
  - Stakeholder activism
  - Changes in customer preferences
  - Commodity price spikes
  - Adverse changes to laws and regulations
  - Cyber security & privacy protection
  - Business discontinuities / supplier disruptions
  - Technology obsolescence
  - Failed acquisitions
- **Regulation**
  - NYSE listing requirements
  - Sarbanes-Oxley assertions
  - SEC reporting requirements
  - Federal sentencing guidelines
  - Kontra G
  - Turnbull
  - King
  - Euronext
  - Basle
- **Market Expectations**
  - Shareholder activism
  - Increased pressure by rating agencies
- **Public Image**
  - Highly visible litigation
  - Growing media attention
  - Company reputation risks
  - Executive compensation
- **Corporate Governance**
  - Board and Audit Committee responsibilities
  - Executive Management responsibilities
  - External risk reporting responsibilities

The Role of the Audit Committee

NYSE Listing Requirement

- *"While it is the job of the CEO and senior management to **assess and manage the company's exposure to risk**, the audit committee must discuss guidelines and policies to govern the process by which this is handled."*

- *The audit committee should discuss the **company's major financial risk exposures and the steps management has taken to monitor and control such exposures**.*

Major Financial Risk Exposure

"It seems reasonable that the risk factors you disclose in your financial statements should be included in the risk analysis."

Janice O'Neill
Senior Vice President Corporate Compliance
New York Stock Exchange
March 16, 2006

Rating Agency ERM Criteria

Moody's

- Risk Governance
- Risk Management
- Risk Analysis & Quantification
- Risk Infrastructure & Risk Intelligence

Standard & Poor

- Policies
  - Governance & Risk Culture
  - Risk Appetite & Strategy
  - Risk Control
  - Risk Disclosure
- Methodology
  - Valuation Techniques
  - Model Vetting & Back Testing
- Infrastructure
  - Risk Architecture
  - Operations

What is Risk?

- Risk is the potential for loss of value or the sub-optimization of gain
- Risk may be caused by an event (or series of events) that can adversely affect the achievement of your objectives.
- The objectives of the enterprise are to:
  - protect the value of its existing assets
  - create new or future value.

What's Wrong With Risk?

Two Schools of Thought

- Risk taking is bad and needs to be avoided
- Risk taking is good and needs to be managed

Value Preservation

The market severely punishes failure to **protect existing assets** (some risks are bad)

- Traditional domain of risk management
- Bottom-up and focused on operations, reporting and compliance
- Vast majority of current risk specializations focus on risks to existing assets yet do so in isolation
- Traditional risk assessment is probabilistic and quantitative – does not typically address risk at the extremes
- Unrewarded risk i.e., no premium for taking these kinds of risks when compared to the severity of the punishment when detected

Value Creation

The market rewards the ability to **create and sustain future growth** (some risks may be good)

- The new domain is managing risks to future growth
- Without risk, there is no reward. This is the basis of capitalism i.e., putting capital at risk and making profitable bets.
- Better understanding the profitability of big bets, risks to success and how to overcome them
- Probabilities don't apply
- Top down focus on mission critical risks to strategy and execution
- Rewarded risk-taking i.e., company can receive a premium for successfully taking and managing risks associated with new products, new markets, new business models, alliances, acquisitions etc.

10 Most Frequently Publicly Disclosed Risks*

Grow Protect

Rank	Disclosed Risk	Frequency
1	Economic Conditions / Trends	294
2	Adverse Legal / Regulatory / Environmental Changes	288
3	Competitors & Competitive Actions	281
4	Business Interruption (e.g., supply Interruption and Natural Disasters/Severe Weather	277
5	Litigation / Intellectual Capital Issues	213
6	M&A Strategy / Execution / Integration	192
7	Political Stability / Country Risk	189
8	Unanticipated changes in Consumer Demands/Preferences	187
9	Inability to Develop / Market New Products	156
10	Terrorist Activities / War / Civil Unrest	149

*Unpublished research of 10Q, 10K and 20F's Deloitte 2005

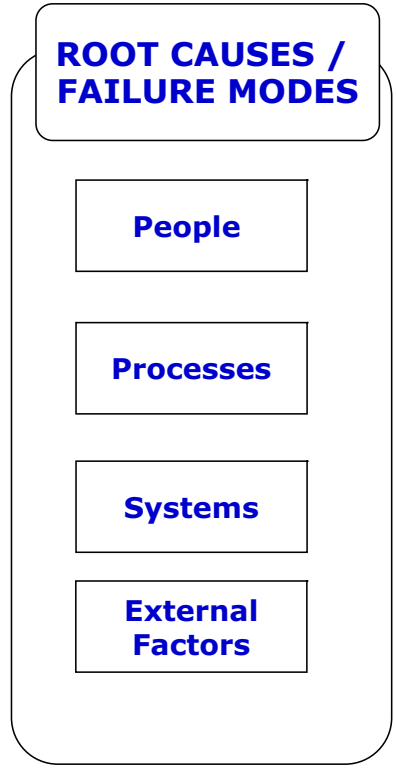
What is your organization's current level of "shock resistance" to these kinds of risks?

*Unpublished survey results of over 1,300 respondents

Understanding Risks to Value

Management is responsible for creating and preserving value in the enterprise

1. How can the enterprise fail to achieve its value objectives?
2. What would cause the enterprise to fail?
3. What would be the effects of the failure?
4. What is currently being done to prevent, detect, correct or escalate such failure?
5. What is our vulnerability to such failure?
6. What further actions are required to cost-effectively mitigate value at risk?
7. How do we get reasonable assurance existing mitigation is reliable & effective?

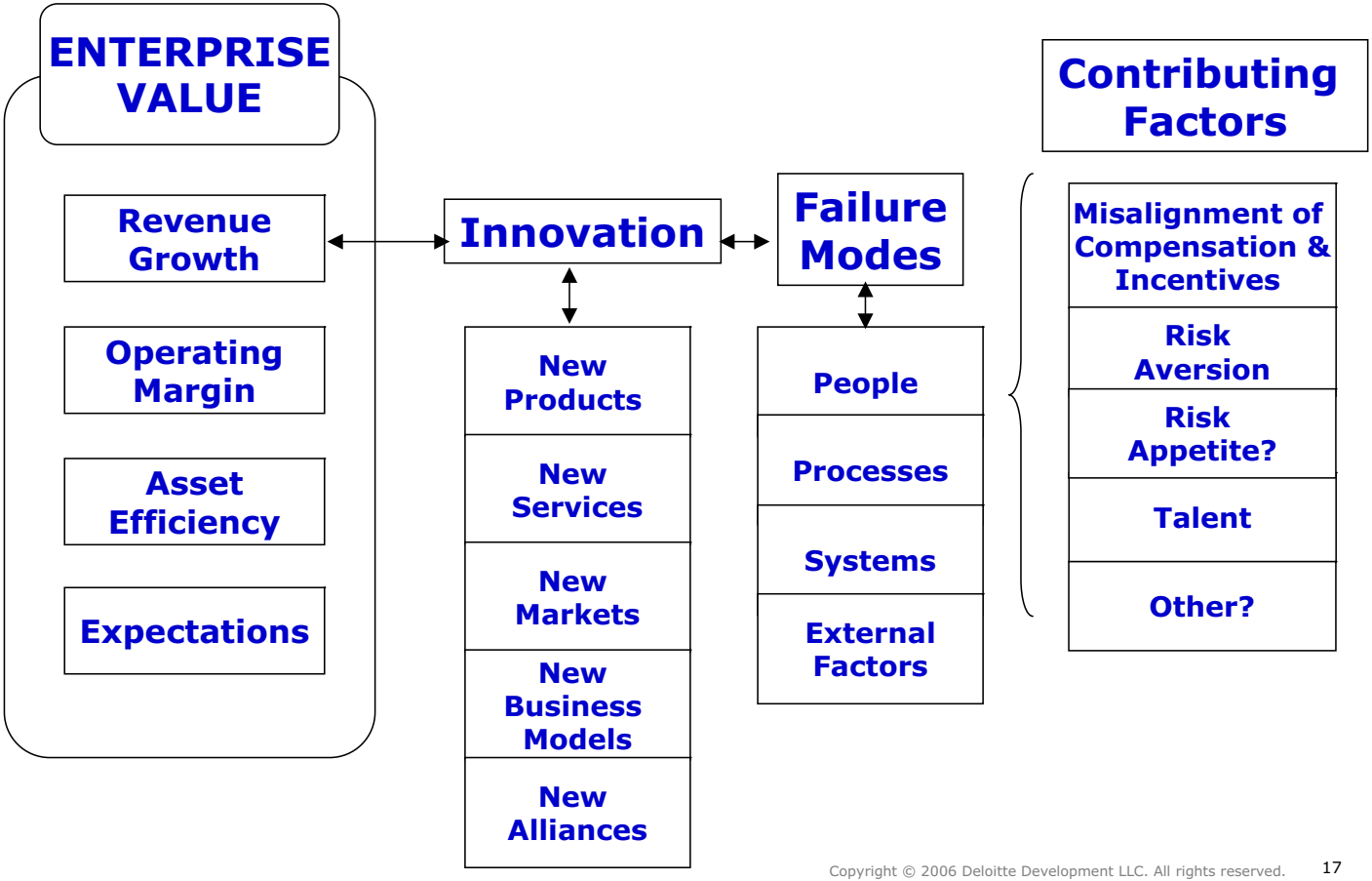


Innovation & Risk Management

When It's Risky – Complacency Can Kill!!!

But When You Are Very Good at Managing Risk – You Can Take More Risk!!!

Innovation & Risk



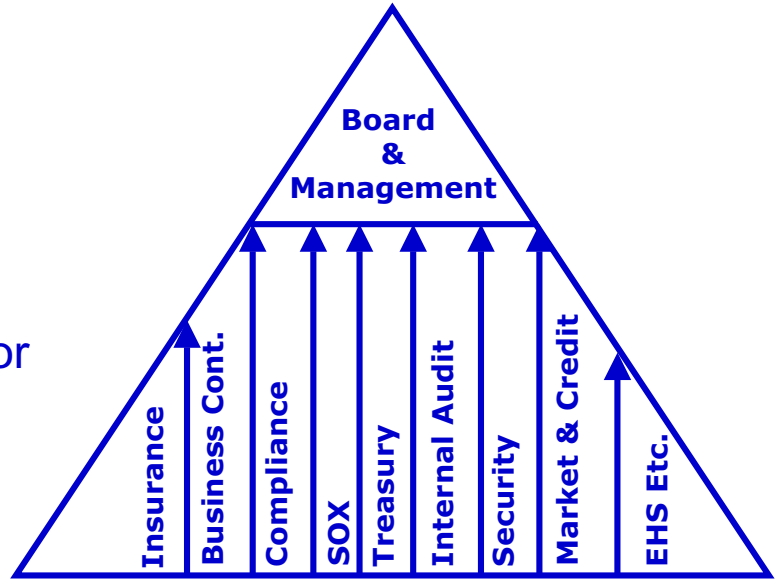
No One is Immune to Value Killers and No One is Perfect

- Almost 50% of global 1000 companies lost 20% or more in share price in less than a month during the past 10 years – some never recovered
- 80% of losses were due to interaction of multiple risks
- Almost all organizations have risk management located in specialist silos
- Most major losses were as the result of a series of high impact but low likelihood events

The Value Killers
Deloitte Research, 2005

Today's Typical Risk Silos

- Deep specialization
- Bottom Up
- Inefficient (no commonality)
- Hard to get portfolio view
- Ineffective response to major value losses that cut across functions
- Focus is on risks to control and existing assets



Focus of action is deep specialization within the wider organization

~ 20% of benefit from top management effort and implementation
~ 80% of benefit from full organizational effort and implementation

From Silos to Integrated

Silos are less effective and efficient

Integration:
Scenarios
Offsets
Correlations
Domino effects

The Risk Intelligent Enterprise

- Top Down & Bottom Up
- Maintain deep specialization
- Improve cross-functional efficiency (commonality where it makes sense)
- Easier to get portfolio view
- More effective response to major value losses that cut across functions
- Focus is on risks to value (existing assets and future growth)

Focus of action is risks to value, top down & alignment across the risk specializations

~ 20% of effort to get 80% of benefit from top management implementation

Harmonization, Synchronization and Rationalization

1. Harmonize

- Establish common language
- Standardize policies, practices and reports
- Clarify roles and responsibilities (gaps and overlaps)
- Produce a portfolio view to better understand and manage risk interactions
- Improve ability to rely on one another's work

2. Synchronize

- Coordinate cross-functionally for improved anticipation, preparedness, response and recovery
- Coordinate timing of requests for information
- Smooth workload demands

3. Rationalize

- Eliminate gaps / redundant structures, processes & controls
- Reduce / eliminate duplication of effort related to assessment, testing, reporting, etc.
- Reduce burden on the business and related expense growth

What is Risk Intelligence?

Rewarded Risk Taking		**Risk Aversion**
All Enterprise Risks	**N**	**Financial Statement Risk**
Consistent	**O**	**Ad Hoc**
Forward-looking	**T**	**Historical**
Risks to Value		**Risks to Control**
Gross & Net Risk		**Impact & Likelihood**
Assurance of Mitigated Value	**J**	**Assume Effectiveness**
Scenarios	**U**	**Single Events**
Speed of Onset is Critical Variable	**S**	**Speed is Constant**
Integrated (Built In)	**T**	**Bolted On**
Risk Management can be Free		**Increased Costs**
Effective & Efficient		**Specialist Silos**
Sustainable Capability		**"One Off" Assessments**

The Value Proposition for Improving "Risk Intelligence"

"Brakes actually help cars go faster"

- Enterprises that are most effective and efficient in managing risks to future growth and existing assets will, in the long run, outperform those who are less so.
- Competitive advantage requires calculated risk taking for reward.
- Calculated risk taking and protection of existing assets requires risk intelligence in an uncertain environment.

But Have Our Risk Assessment Models Kept Pace?

The Role of Internal Audit

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the *effectiveness of risk management, control, and governance processes*."

Source: ***The International Standards for the Professional Practice of Internal Auditing*** **(*Standards*) The Institute of Internal Auditors**

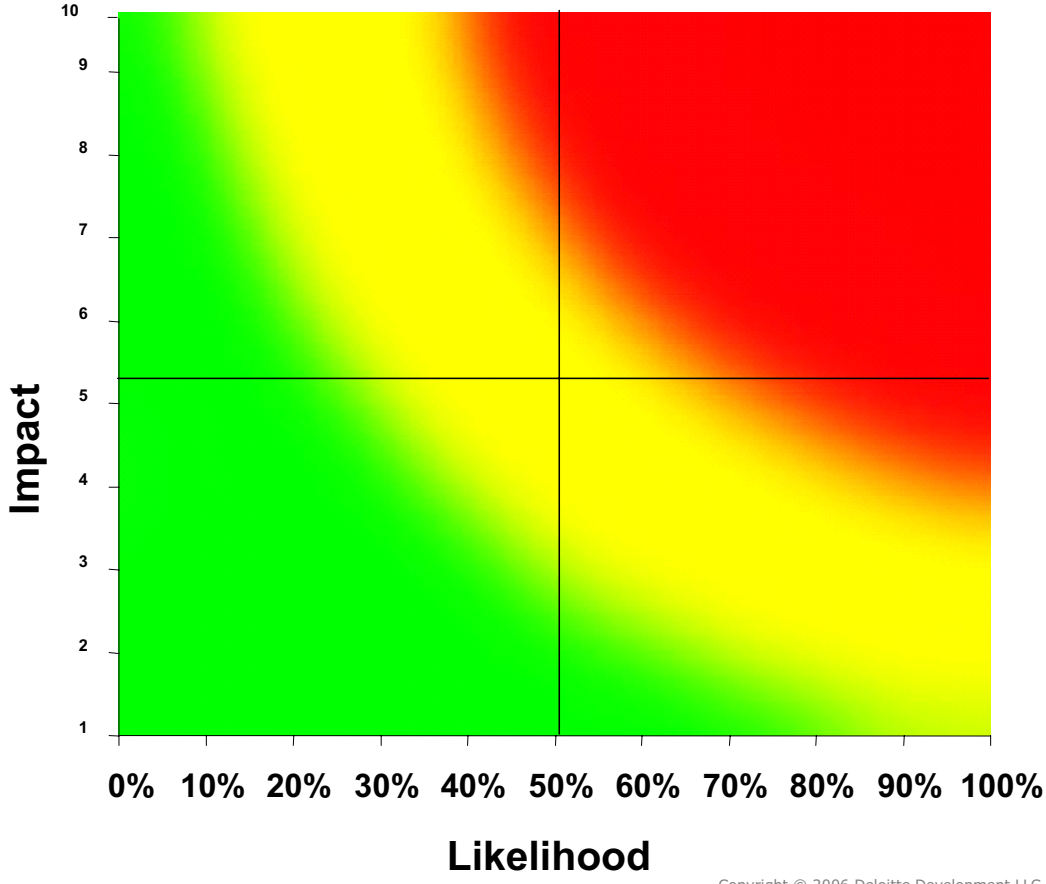
Balancing IA Roles

Internal Audit's Role	Major ERM Activities
Core/Safe – consistent with Standards	• Giving assurance on the risk management process
	• Giving assurance that risks are correctly evaluated
	• Evaluating risk management processes
	• Evaluating the reporting of key risks
	• Reviewing the management of key risks
Should be performed with certain safeguards	• Facilitating identification and evaluation of risks
	• Coaching management in responding to risks
	• Coordinating ERM activities
	• Consolidated reporting on risks
	• Championing establishment of ERM
	• Developing risk management strategy - BOD approval
Should not be performed by internal audit	• Setting risk appetite
	• Imposing risk management processes
	• Providing management assurance on risks
	• Making decisions on risk responses
	• Implementing risk responses on management's behalf
	• Assuming accountability for risk management

A Quick Self-assessment of Your Current Internal Audit Risk Assessment Model. Do You:

1. Assess primarily risks, entities, processes or systems or all of these?
2. Differentiate between rewarded and unrewarded risk?
3. Assess impact and likelihood?
4. Allocate audit resources to highest impact and most likely risks?
5. Clearly differentiate between inherent and residual risk?
6. Provide assurance on mitigated value?
7. Evaluate inherent and residual risk simultaneously?
8. Address high impact / low likelihood events?
9. Address scenarios and series of events not just individual events?
10. Support harmonization, synchronization and rationalization of risk intelligence?

Impact and Likelihood



Current IA Risk Assessments

Typically:

- Start with a blank sheet of paper
- Audit individual entities, processes and systems
- Audit those with highest impact and probability
- Do not differentiate between inherent & residual risk
- Address risks as separate, unrelated events
- By their nature, audit plans avoid dealing with risks that are outside of their scope
- So what happens to the rest of the risks?

Inherent and Residual Risk

- Inherent (Gross) risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
- Residual (Net) risk is the risk that remains after management's response to the risk.
- Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then considers residual risk.
- Effective enterprise risk management requires that risk assessment be done both with respect to inherent risk and also following risk response.

COSO ERM 2004

Probabilistic Modeling

Suitable		Unsuitable
Recurring situations	⟷	Rare/Non-recurring situations
Large body of data	⟷	Small body of data
Subject to known rules	⟷	Rules are unknown/forming
Stable	⟷	Unstable / rapid change
Patterns Observable	⟷	Patterns not readily observable
Controllable	⟷	Uncontrollable (External) Factors
Limited range of outcomes	⟷	Unlimited range of outcomes
Combinations lead to known results	⟷	Combinations lead to unknown results

Predictability is a Thing of the Past

"Predictions about the likelihood of multi-causal losses actually depend on sound understanding of cause-and-effect relationships or on a detailed loss history, and the risks of the future have neither of the two."

Swiss Re " The Risk Landscape of the Future"

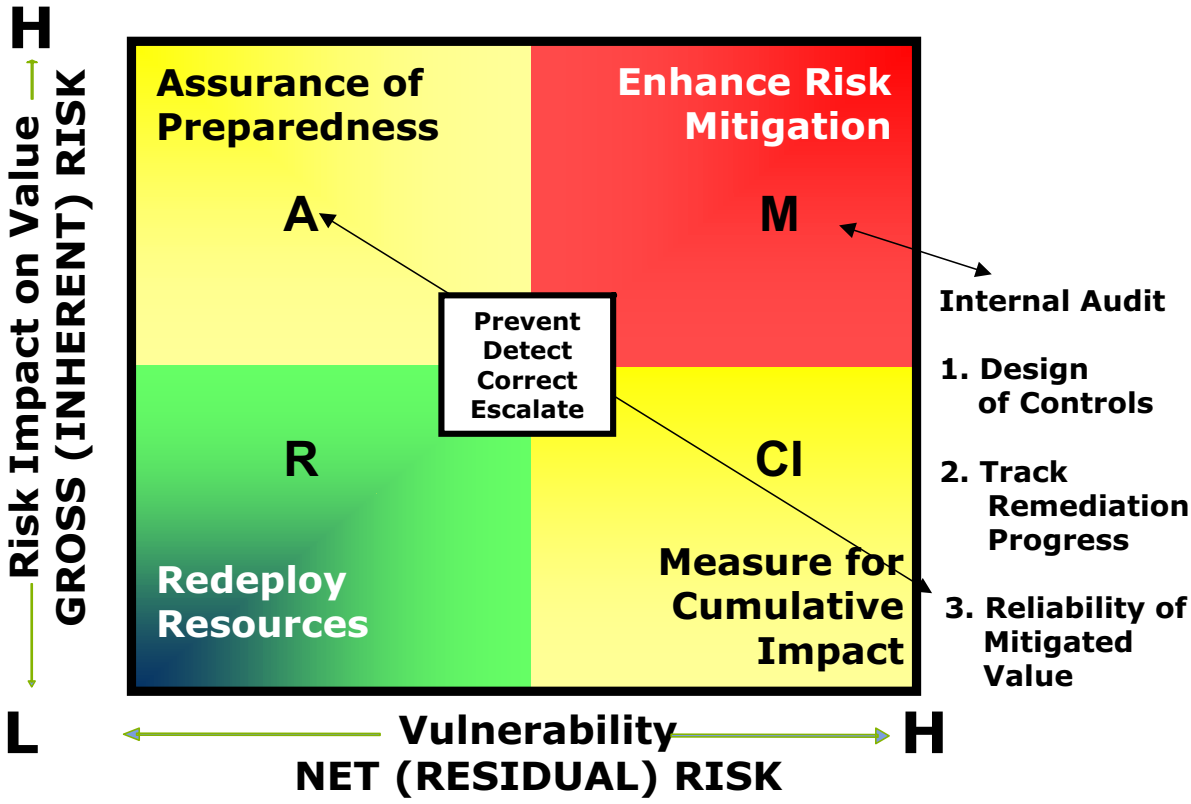
The Fallibility of Probability

- Little or no predictive value
- Major value losses are often high impact / low likelihood

9/11	1997 Asian Financial crisis
Dot com bubble	Financial scandals
Oil / commodity price spikes	Natural disasters
Danish cartoons	???

- Biases management to direct resources to high impact / high likelihood events
- Typically focuses on single events rather than a series of events or domino effects
- Audit activities are often mis-directed to the red zone

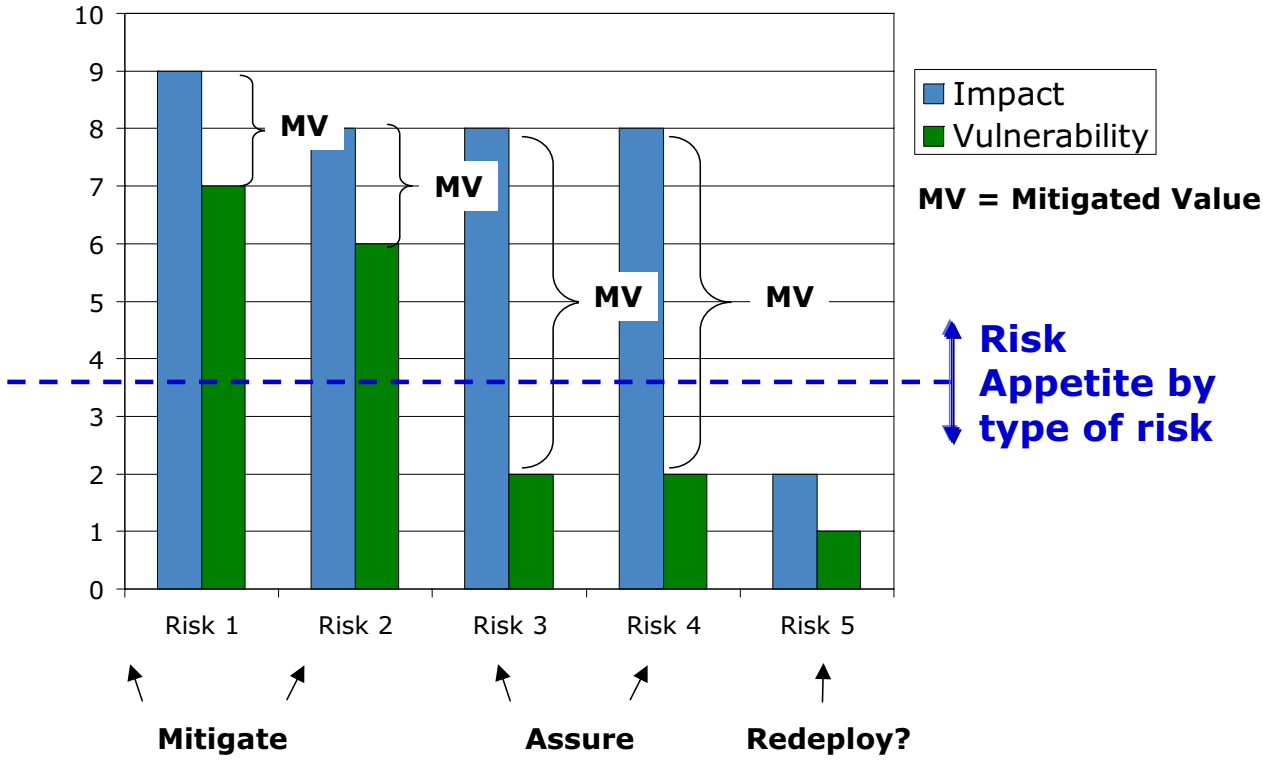
The New Paradigm



Risk Assessment Model

Illustrative

Gross Risk – Net Risk = Mitigated Value



Mitigated Value Example

Illustrative

Gross (Inherent) Risk **$100MM**	**Mitigated Risk Value** **$35MM**	**RISK MITIGATION** •Management Reviews •Functional Responsibility •Risk Transfer (Insurance) •Disaster Recovery Plans •Performance Metrics •Inventory Buffer	**ASSURE** •Assurance Plan prioritized by Mitigated Risk Value •Criticality •Effectiveness and efficiency of mitigated value plan
Risk Appetite	**Net (Residual) Risk** **$65MM**	•Data Center Vulnerable •Environmental Liability •Contract Penalties •Contract Weaknesses •Market share loss •Reputation loss •Litigation	**MITIGATE** •Rank by highest value to mitigate down to risk appetite threshold •Assign executive risk owners •Identify most important and controllable improvements •Identify response alternatives •Develop hierarchy of cost of mitigation
$5MM			**REDEPLOY?** **CUMULATIVE IMPACT?**

IMPACT (Gross Risk)

Adapted from the IIA's SIAS Number 9, "Risk Assessment"

- Financial
  - **Asset size, liquidity, or transaction volume**.
  - Cost of prior risk experience (direct hits and near misses)*
- Stakeholders
  - **Impact on customers, suppliers**
- Reputation*
- Legal/Regulatory*
  - **Impact on government regulations**
- Environment, Health and Safety*
- Speed of Onset*

*Deloitte Impact Criteria

Vulnerability (Net Risk)

1. Control Effectiveness (People, Process and Systems)
   - Ethical climate/pressure on management to meet objectives
   - Competence, adequacy, and integrity of personnel
   - Adequacy and effectiveness of the system of internal control
   - Management judgments and accounting estimates
   - Degree of computerized information systems
2. Speed of Response - Detection, Response, Recovery
3. Complexity
   - Complexity or volatility of activities / Geographical dispersion
4. Response to Prior Risk Experience
   - Acceptance of audit findings and corrective action taken
   - Date and results of previous audits
5. Rate of Change (expansion or contraction)
   - Organizational, operational, technological, or economic.
6. External Conditions
   - Competitive conditions / Financial and economic conditions.

Most Vulnerabilities Are Known in Advance

"Before 9/11 the Federal Emergency Management Agency listed the three most catastrophic disasters facing America: a terrorist attack on New York, a major earthquake in San Francisco and a hurricane strike on New Orleans…."

New York Times, Sept. 9, 2005

"95% of all computer vulnerabilities are known in advance."

Computer Emergency Response Team
Carnegie Mellon

Implications for Internal Audit

1. Audit individual risks, entities, processes and systems in descending order of mitigated value and criticality
2. Audit controls for those risks with highest impact / low vulnerability
3. Differentiate between inherent and residual risk
4. Prioritize based on vulnerabilities not probabilities
5. Give appropriate guidance as to where and what to audit
6. Address what should be done with risks that are outside of the audit scope
7. Address potential interactions among specific risks, entities processes and systems
8. Understand and address scenarios

Implications for Internal Audit

M = High Impact / High Vulnerability

- Provide assistance in design of controls where impact and vulnerability are high
- Track progress on remediation plans

A = High Impact / Low Vulnerability

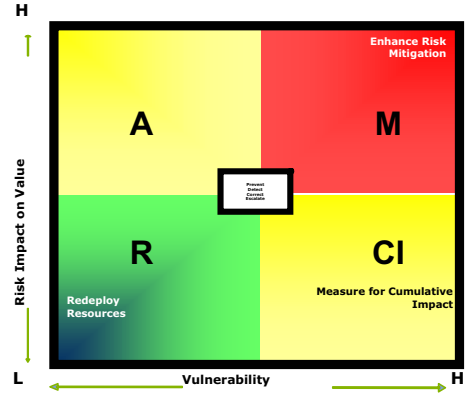
- Obtain assurance confidence in preparedness is justified

R = Low Impact / Low Vulnerability

- Obtain assurance on effectiveness
- Identify ways to improve efficiency

CI = Low Impact / High Vulnerability

- Assess cumulative impacts and frequency



Risk Intelligent Internal Auditor Should:

- Identify risks to value and control
- Assess scenarios and chains of events
- Assess gross and net risk
- Provide assurance on mitigated value
- Factor in speed of onset and response
- Recognize many regulators still use impact and likelihood criteria
  - Resistance can be expected
  - If needed, look at likelihood of residual risk
- Harmonize, synchronize and rationalize risk assessment criteria and processes with other risk assessors where it makes sense
  - Reduce burden on business
  - Improve effectiveness and efficiency

Invitation to Participate in an ERM Benchmark Survey

- Survey launched in April 2005. Over 80 companies have submitted responses, spanning all major industries.
- Recently updated and "evergreen"
- Will provide interim reports to all survey participants.
- Framework for a series of Regional ERM Roundtables.
- In order to participate in the survey and receive copies of reports, please follow the survey link: https://www.surveymonkey.com/s.asp?u=617131944186
- Completion of the survey should take less than 30 minutes.

All individual responses will be kept confidential. Please submit only 1 survey response per company.

Questions?

Key Contacts

Rick Funston
Principal, National Practice Leader
Governance and Risk Oversight
rifunston@deloitte.com
office: +1-313-396-3014

Eric Hespenheide
Managing Partner, Global Internal Audit Services
ehespenheide@deloitte.com
Office: +1-313-396-3163

A-1
Risk Management and Assurance at NOKIA Group

Mikko Routti (FIN)
Director, Risk Management and Assurance
Nokia Corporation

Risk Management in Nokia Group

Mikko Routti, Director, Risk Management and Assurance

ECIIA 6-8.September

NOKIA
Connecting People

Nokia is about Connecting People

- Nokia is the world's largest manufacturer of mobile devices and a leader in mobile network equipment, solutions and services.
- We also provide equipment, solutions and services for corporate customers.

- Ranked by Interbrand as the world's 6th most valuable brand in 2005
- Nokia has refocused its brand strategy
- Deepening consumers' emotional connection with the brand
- Emphasis on 'very human technology'
- Opening of Nokia Flagship Stores

NOKIA
Connecting People

Nokia at a Glance

	2005	2004	Change, %
Net sales (EUR million)	34 191	29 371	+16
Operating profit (EUR million)	4 639	4 326	+7
Operating margin, %	13.6	14.7	
Earnings per share, diluted, EUR	0.83	0.69	+20
Research and development (EUR million)	3 825	3 776	+1
Personnel (year-end)	58 874	55 505	+6

- Head office in Finland, operations around the world, sales in more than 130 countries
- Nokia sold its one billionth phone in 2005
- June 19, 2006: Nokia and Siemens to merge their communications service provider businesses. Nokia Siemens Networks 2005 pro forma revenues EUR 15.8 billion.

NOKIA
Connecting People

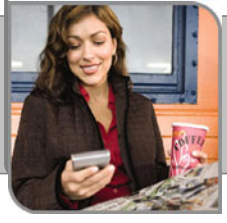
Nokia is Organized for Growth

Business Groups

Horizontal Groups

- Customer and Market Operations
- Technology Platforms
- Brand and design
  Developer support
  Research and venturing
  Business infrastructure

Mobile Phones	Multimedia	Enterprise Solutions	Networks



Corporate Functions

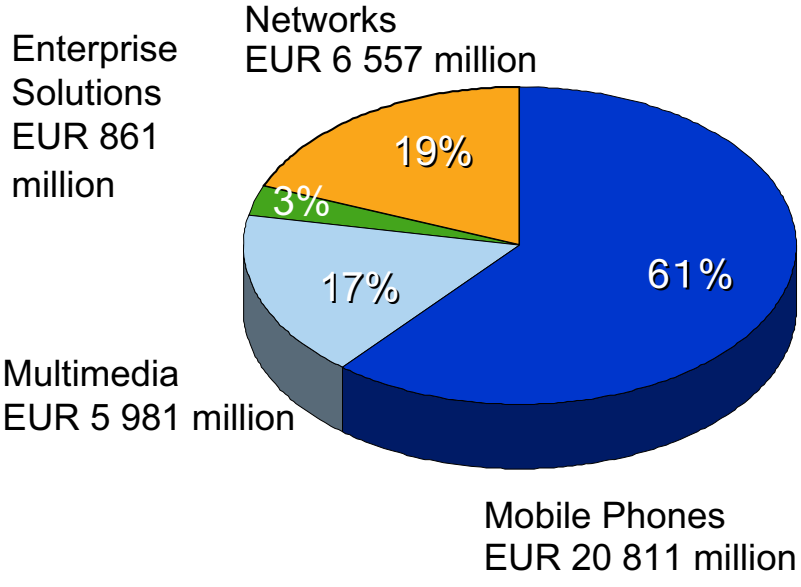
NOKIA
Connecting People

Our Customers

- Operators
- Businesses
- Consumers

NOKIA
Connecting People

Net Sales by Business Group



Full-year net sales by business group, EUR million

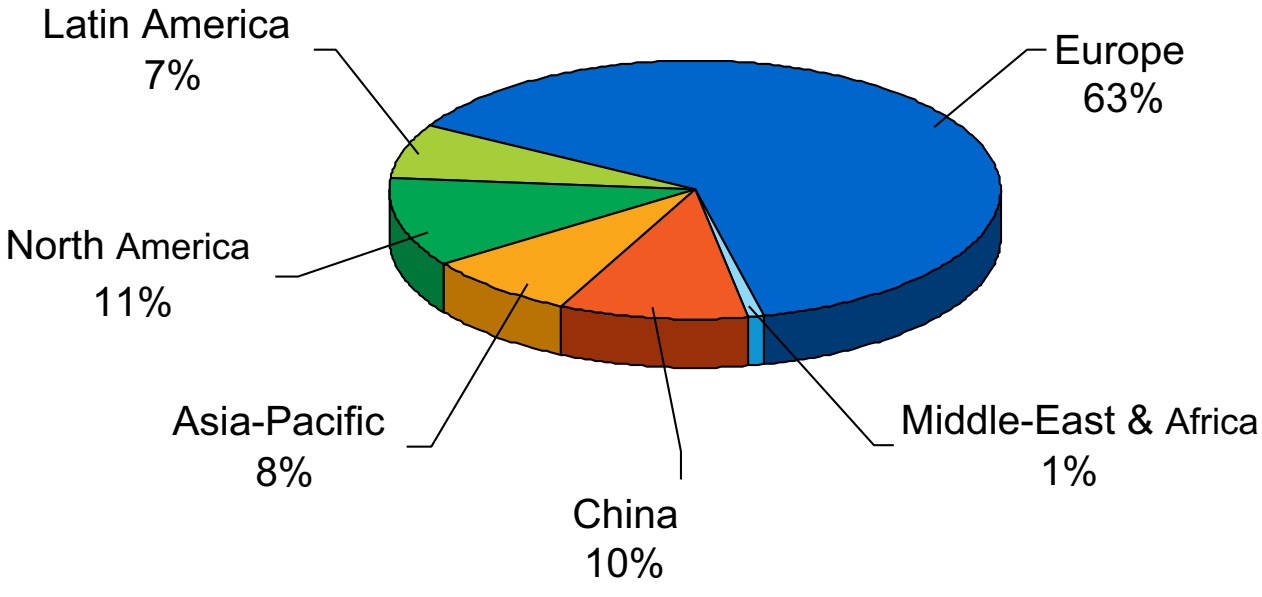
	2005	Revised* 2004
Mobile Phones	20 811	18 521
Multimedia	5 981	3 676
Enterprise Solutions	861	839
Networks	6 557	6 431
Eliminations	-19	-96
Nokia	34 191	29 371

** Nokia's 2004 financial accounts reflect the retrospective implementation of IFRS 2 and IAS 39R.*

NOKIA Connecting People

Our People

Diversity is at the heart of our business

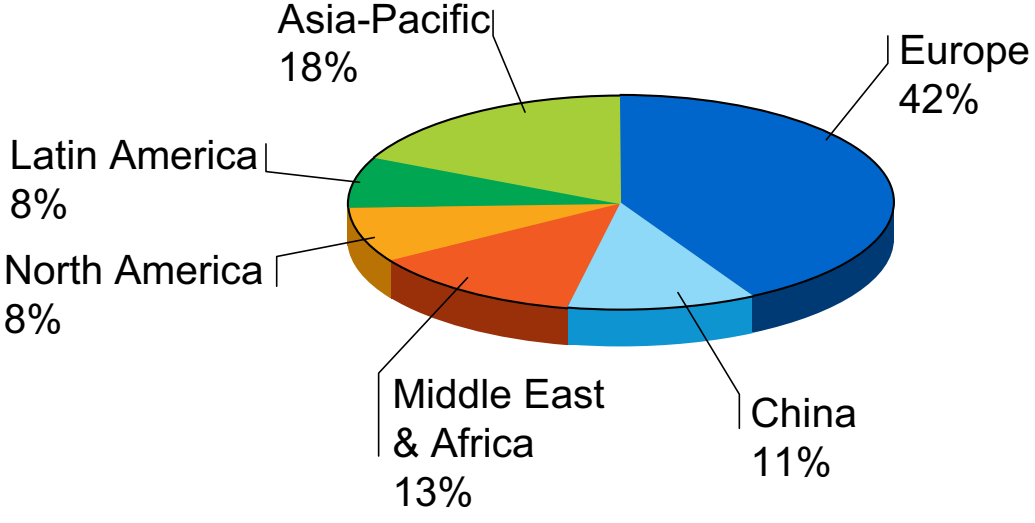


NOKIA
Connecting People

Balanced Global Market Presence

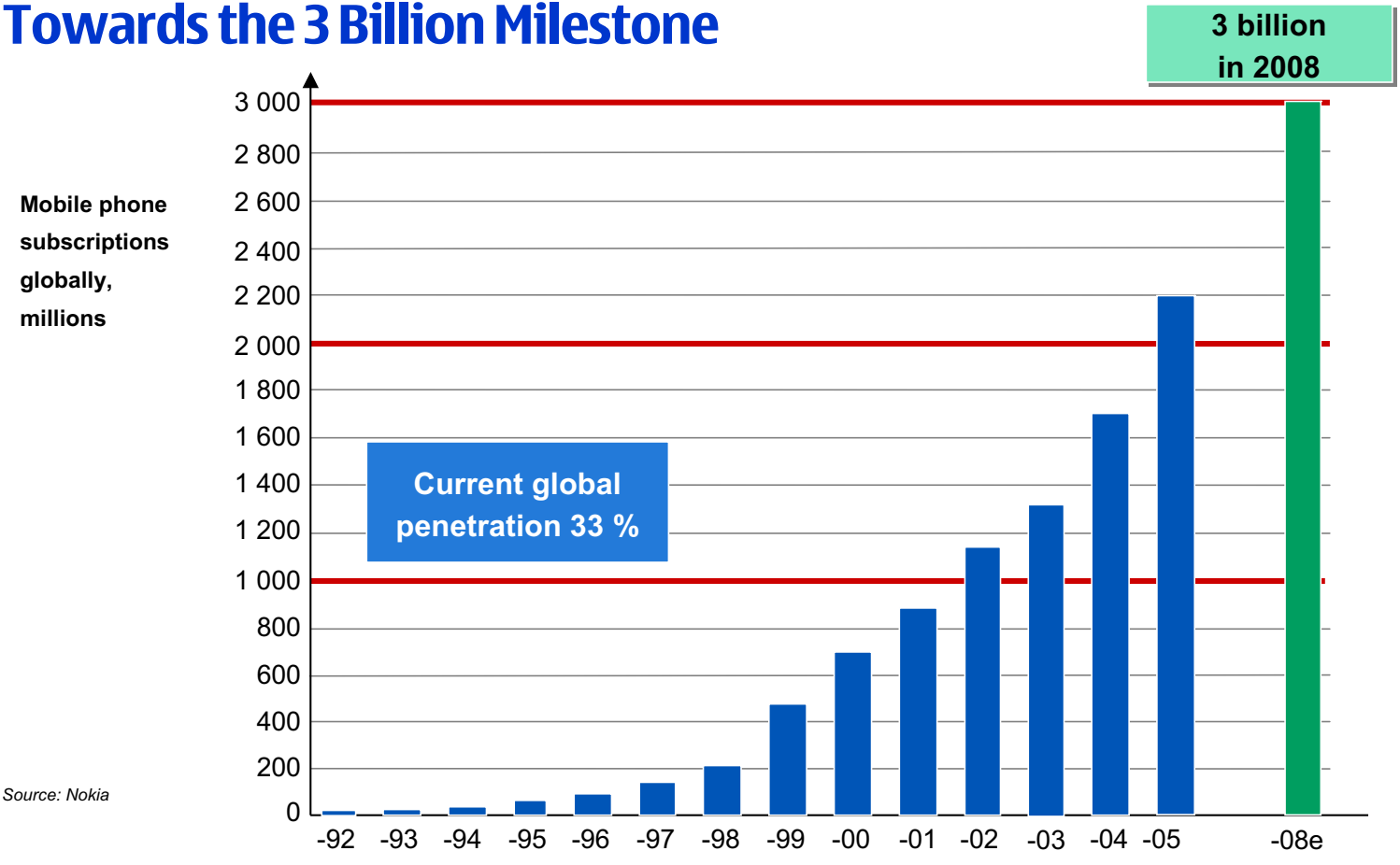
Net sales 2005:

EUR 34 191 million



NOKIA
Connecting People

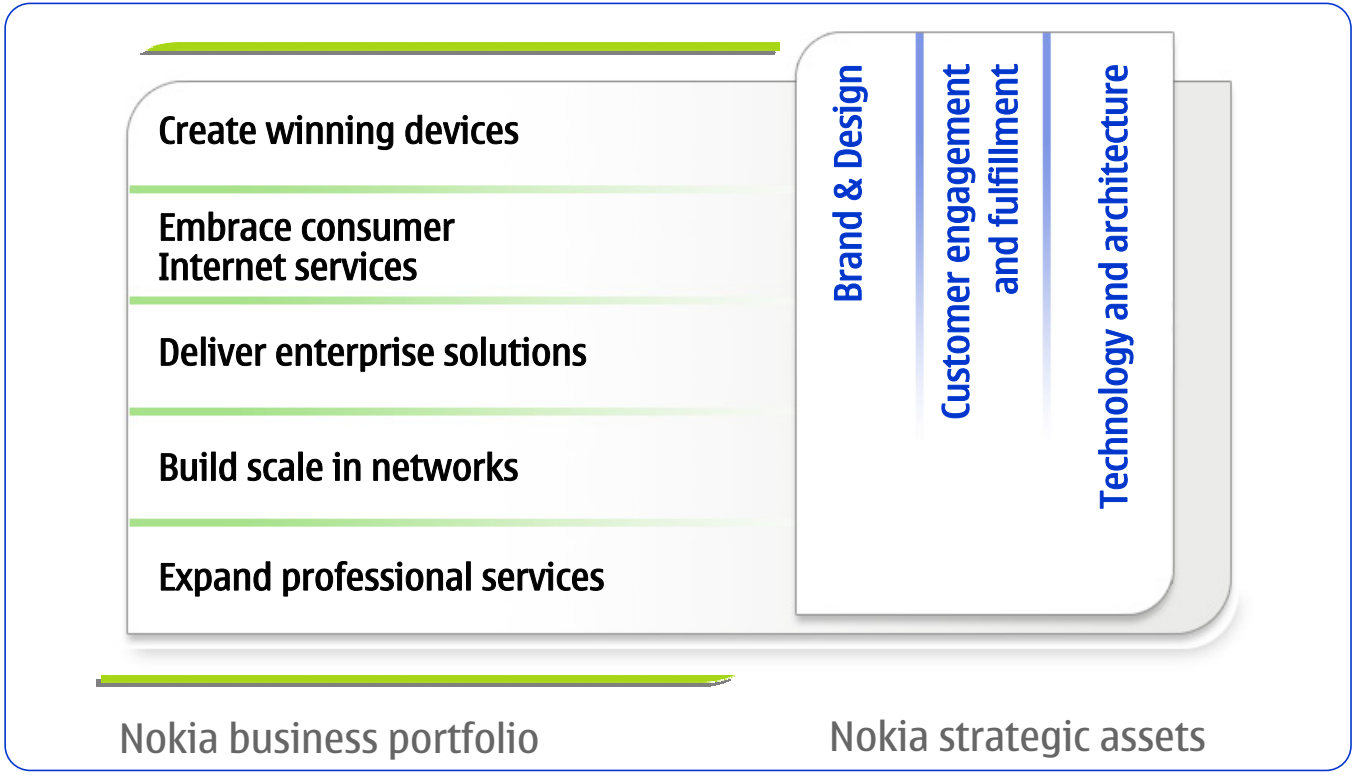
Towards the 3 Billion Milestone



Source: Nokia

NOKIA
Connecting People

Nokia Strategy



NOKIA
Connecting People

Leader in Corporate Responsibility

Index		Ranking	Previous ranking
FTSE4Good	03/06	included	included
Dow Jones (DJSI World) (Communications technology)	09/05	2	1
Dow Jones (Stoxx) (European technology)	09/05	2	1
SiRi Global Profile 500 (top 10 stocks in Europe)	10/02	1	2
OEKOM (industry: env. +soc.) biennial	02/05	2 (out of 10)	4 (out of 19)
Fortune Most Admired	03/06	20 Industry leader	26 Industry nr 3
• Social Responsibility subcategory ranking		Industry: nr 2	

NOKIA
Connecting People

What is "Risk" and "Risk Management" in our context

"Risk is any uncertainty that affects Nokia's objectives and the achievement of the optimum result" **(Nokia's Risk Policy)**

- Philosophy: holistic risk management (ERM), but focus on business risks
  - covers **any** material risks (instead of pre-defined risk areas)
    - strategic
    - operational incl. hazards
    - finance
  - Lost Opportunity – is definitely a risk
- Risk identification is integral part of direction-setting in planning process
  - Key risks identified against business targets -systematic cycle
  - Material risks reported regularly to top management and board
  - RM is not a separate process or action but a normal business practice
    - part of Group management system
    - part of operational work as a quality assurance practice

Risk Types help to identify and classify risks

NOKIA'S RISK UNIVERSE
internally and externally driven risks

NOKIA RISK TYPES

- Strategic risks
  - Acquisitions and partnerships
  - Brand
  - Corporate Culture
  - Global and regional economy
  - Markets
  - Nokia Operational Model
  - Product portfolio
  - Technology
- Financial risks
  - Capital allocation
  - Capital availability
  - Capital structure
  - Counterpart/credit risk
  - Foreign Exchange
  - Interest rate
- Operational risks
  - Compliance
  - Customers & marketing
  - Environmental
  - Execution and Process efficiency
  - Hazard risks
  - Human resources
  - Information/reporting
  - IT
  - Logistics
  - Manufacturing and care
  - Misconduct
  - Political risks
  - Quality
  - Security
  - Suppliers & contractors

NOKIA Connecting People

Example: Risk Factors - Nokia 20 F Annual Report filed with SEC

Headlines:

- *Our sales and profitability depend on the continued **growth of the mobile communications industry** as well as the growth of the new market segments within that industry in which we have recently invested. If the mobile communications industry does not grow as we expect, or if the new market segments on which we have chosen to focus and in which we have recently invested grow less than expected, or if new faster-growing market segments emerge in which we have not invested, our sales and profitability may be adversely affected.*
- *Our results of operations, particularly our profitability, may be adversely affected if we do not successfully manage **price erosion related to our products**.*
- *We must develop or otherwise acquire **complex, evolving technologies** to use in our business. If we fail to develop these technologies or to successfully commercialize them as new advanced products and solutions that meet customer demand, or fail to do so on a timely basis, it may have a material adverse effect on our business, our ability to meet our targets and our results of operations.*
- *We need to understand the different markets in which we operate and meet the needs of our customers, which include mobile network operators, distributors, independent retailers and enterprise customers. We need to have a **competitive product portfolio**, and to work together with our operator customers to address their needs. Our failure to identify key market trends and to respond timely and successfully to the needs of our customers may have a material adverse impact on our market share, business and results of operations.*

NOKIA
Connecting People

Cont'd

- ***Competition*** *in our industry is intense. Our failure to respond successfully to changes in the competitive landscape may have a material adverse impact on our business and results of operations.*
- ***Reaching our sales, profitability, volume and market share targets*** *depends on numerous factors. These include our ability to offer products and solutions that meet the demands of the market and to manage the prices and costs of our products and solutions, our operational efficiency, the pace of development and acceptance of new technologies, our success in the business areas that we have recently entered, and general economic conditions. Depending on those factors, some of which we may influence and others of which are beyond our control, we may fail to reach our targets and we may fail to provide accurate forecasts of our sales and results of operations.*
- *Our sales and results of operations could be adversely affected if we fail to efficiently manage our* ***manufacturing and logistics*** *without interruption, or fail to ensure that our products and solutions meet our and our customers' quality, safety and other requirements and are delivered in time.*
- *We depend on our* ***suppliers*** *for the timely delivery of components and for their compliance with our supplier requirements, such as, most notably, our and our customers' product quality, safety and other standards. Their failure to do so could adversely affect our ability to deliver our products and solutions successfully and on time.*

NOKIA
Connecting People

Cont'd

- *We are developing a number of our new products and solutions **together with other companies**. If any of these companies were to fail to perform, we may not be able to bring our products and solutions to market successfully or in a timely way and this could have a material adverse impact on our sales and profitability.*
- *Our operations rely on complex and highly centralized **information technology systems** and networks. If any system or network disruption occurs, this reliance could have a material adverse impact on our operations, sales and operating results.*
- *Our products and solutions include increasingly complex technology involving numerous new Nokia patented and other proprietary technologies, as well as some developed or licensed to us by certain third parties. As a consequence, evaluating the protection of the technologies we intend to use is more and more challenging, and we expect increasingly to face claims that we have infringed third parties' **intellectual property rights.** The use of increasingly complex technology may also result in increased licensing costs for us, restrictions on our ability to use certain technologies in our products and solution offerings, and/or costly and time-consuming litigation. Third parties may also commence actions seeking to establish the invalidity of intellectual property rights on which we depend.*
- *If we are unable to **recruit, retain and develop appropriately skilled employees**, we may not be able to implement our strategies and, consequently, our results of operations may suffer.*
- *The global networks business relies on a **limited number of customers** and large multi-year contracts. Unfavorable developments under such a contract or in relation to a major customer may affect our sales, our results of operations and cash flow adversely.*

NOKIA
Connecting People

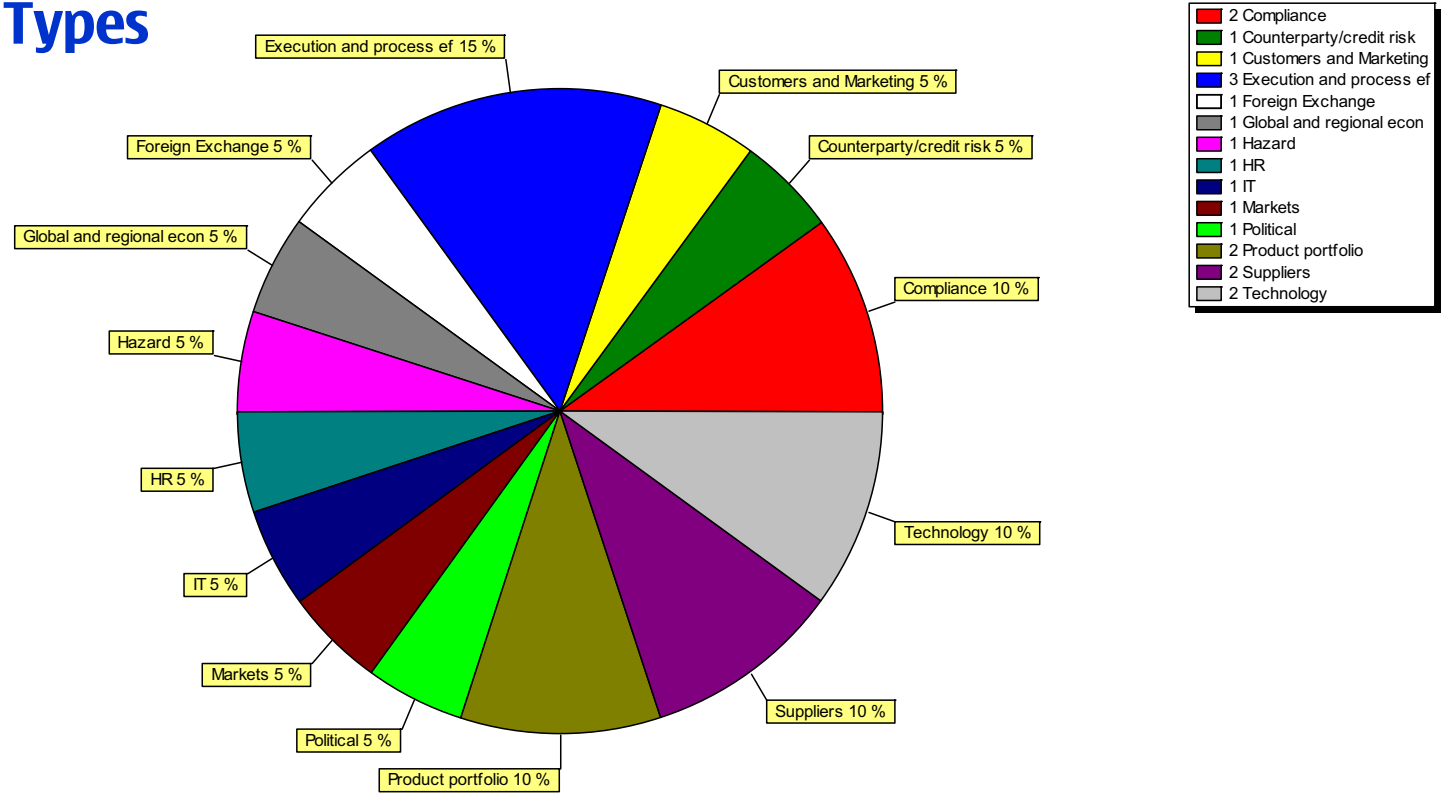
Cont'd

- *Our sales derived from, and assets located in, **emerging market countries** may be adversely affected by economic, regulatory and political developments in those countries. As sales from these countries represent an increasing portion of our total sales, economic or political turmoil in these countries could adversely affect our sales and results of operations. Our investments in emerging market countries may also be subject to other risks and uncertainties.*
- *Our sales, costs and results are affected by **exchange rate fluctuations**, particularly between the euro, which is our reporting currency, and the US dollar, the UK pound sterling and the Japanese yen as well as certain other currencies.*
- ***Customer financing** to network operators can be a competitive requirement and could affect our sales, results of operations, balance sheet and cash flow adversely.*
- *Allegations of **health risks** from the electromagnetic fields generated by base stations and mobile devices, and the lawsuits and publicity relating to them, regardless of merit, could affect our operations negatively by leading consumers to reduce their use of mobile devices or by causing us to allocate monetary and personnel resources to these issues.*
- *An unfavorable outcome of **litigation** could materially impact our business, financial condition or results of operations.*
- *Changes in various types of **regulation** in countries around the world could affect our business adversely.*
- *Our **share price** has been and may continue to be volatile in response to conditions in the global securities markets generally and in the communications and technology sectors in particular.*

NOKIA
Connecting People

20F Risk Factors data categorized into Risk Types

example



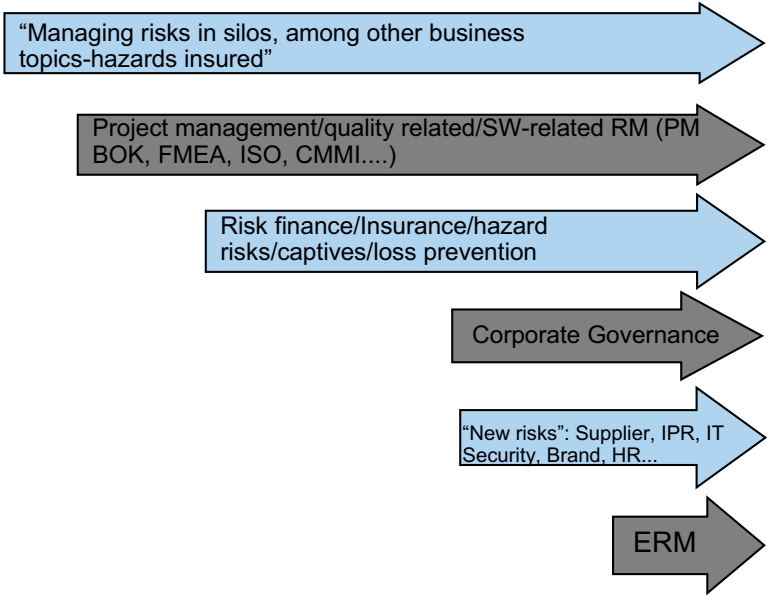
Why have we invested into ERM?

From 1998-2003, 10% of Fortune 1000 companies lost 55% or more of shareholder value within a one-month period. Most of these companies lost value because of strategic risk.

Source: Lippincott Mercer

NOKIA
Connecting People

Evolution of Risk Management Thinking



Nokia RM CONCEPT 2005

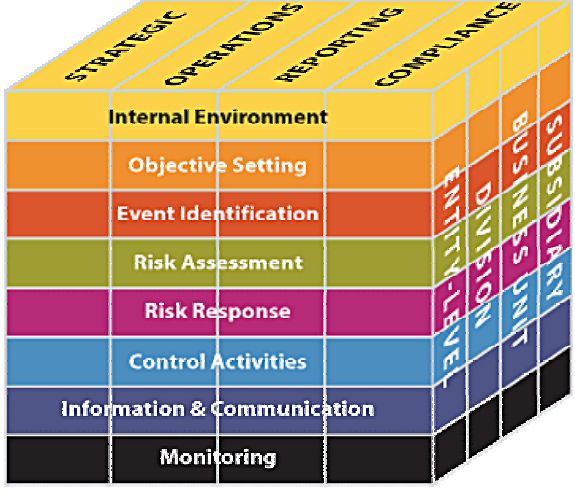
1. **Governance**
   - AC, CFO reporting
   - Steering
2. **RM Infrastructure**
   - Policy, language
   - assurance model
   - One team
3. **Methodology**
   - Common language
   - Linkage to Planning
   - RM cycle, process
4. **Key practices**
   - KRL
   - RM CSA
   - RM PA
5. **People**
   - Roles, training
6. **Tools**
   - KRL, Risk Log
   - N-Risk
7. **Benchmarks**
   - COSO ERM

NOKIA
Connecting People

The COSO ERM Framework is a useful benchmark

Entity objectives can be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance



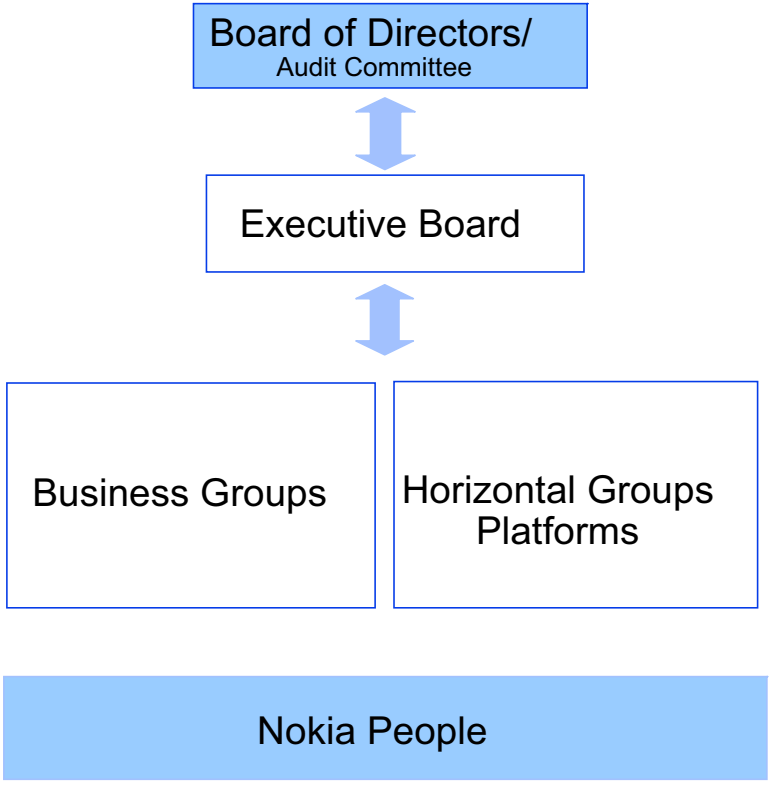
Source IIA: Applying COSO ERM

NOKIA
Connecting People

Risk Management as part of Corporate Governance

1. **Managing business risks is a normal management responsibility**
   - RM activity can bring assurance on how that is going on
   - Management process incl. planning and SRMS set a supporting framework
2. **Organizing RM activity - Regulatory Guidance:**
   - NYSE: Duties of Board/ Audit Committee and key risks as part of 20F Annual Report
   - HEX: Corporate Governance recommendation: description of RM system
3. **Specific external requirements**
   - Internal Control – SOX-COSO/COBIT
   - Financial RM: IAS 32.56
4. **Quality etc. external standards**
   - ISO, BS
   - PM BOK, CMMI, FMEA, PAS 56
5. **Internal guidance**
   - Risk Policy
   - Treasury Policy, Security Policy, Code of Conduct, HR policies etc.

Roles and Responsibilities have been defined



Board of Directors/Audit Committee

- Approves Group's Risk Policy
- Reviews its implementation
- Reviews regular Key Risk reports
- Can initiate assessments

Executive Board

- Approves Risk Management Approach
- Determines how to implement Policy
- Reviews Group's regular Key Risk reports
- Communicates about risk appetite
- Can initiate assessments

Business and Horizontal Groups

- Implement Policy at operational level
- Identify own key risks and manage them
- Key risks regular management information
- Regular key risk report to Nokia level

Risk Management Support Team

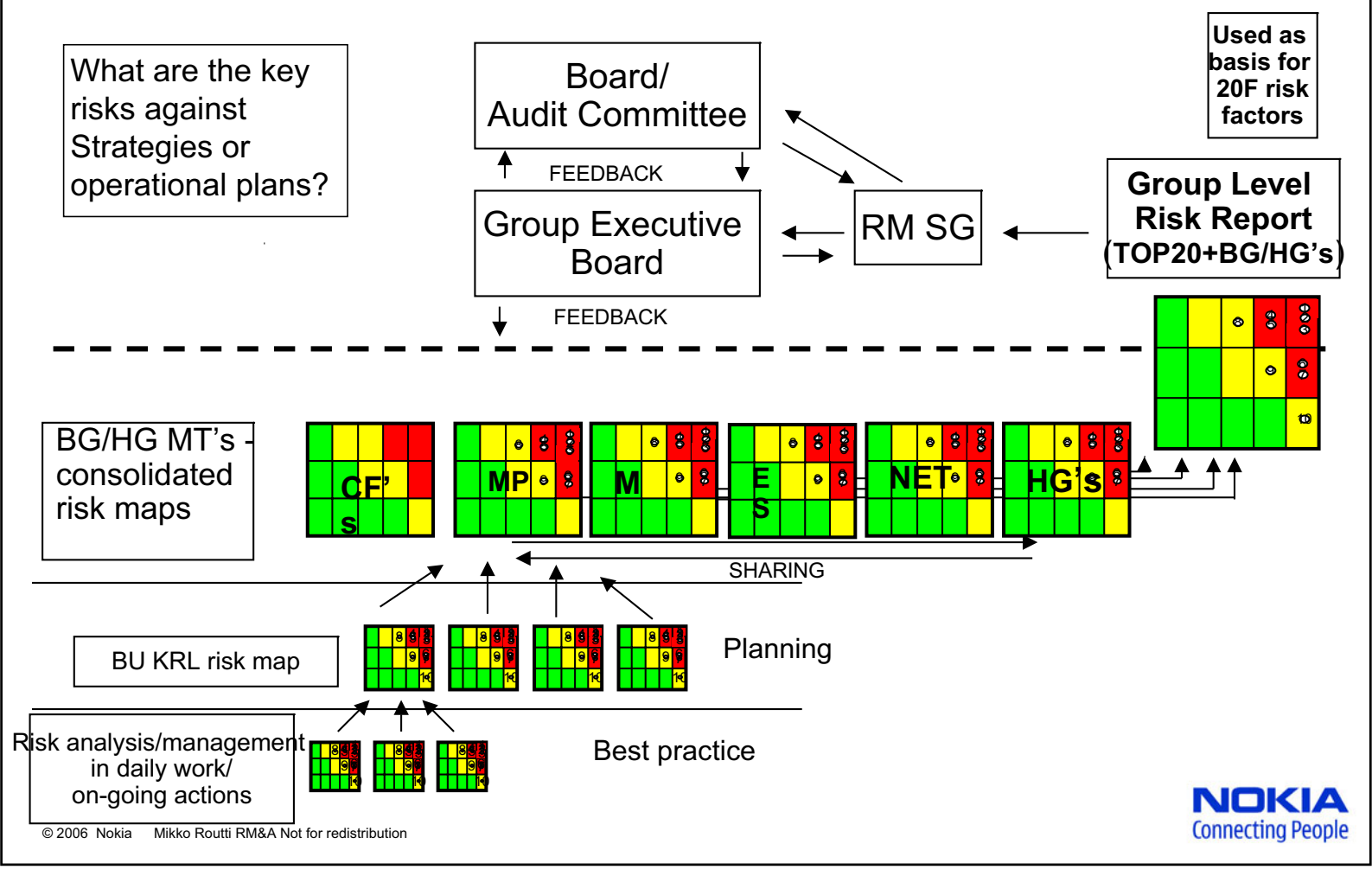
- Supports Policy implementation
- Develops good practice methods
- Consolidates group wide risk reporting
- Review risk management maturity through assessments

Nokia People/Individuals

- Responsible for managing own risks

NOKIA
Connecting People

Flow of Risk Data around planning process



NOKIA
Connecting People

Simple interfaces to document and analyse risks

- **Risk data** is processed by utilizing common Risk template
- **PP Risk Maps** are created based on the collected Risk data:

1. **Risk ID**
2. **Risk event**
3. **Root cause and related factors**
4. **Consequences**
5. **[EUR impact (if can be estimated)]**
6. **Estimated impact (using a scale of 1-5)**
7. **Estimated probability (using a scale of 1-3)**
8. **Risk rate (calculated by Excel)**
9. **Expected actions**
10. **Action Owner**

KEY RISK TEMPLATE

By:

Entity / Area of business:

Date created:

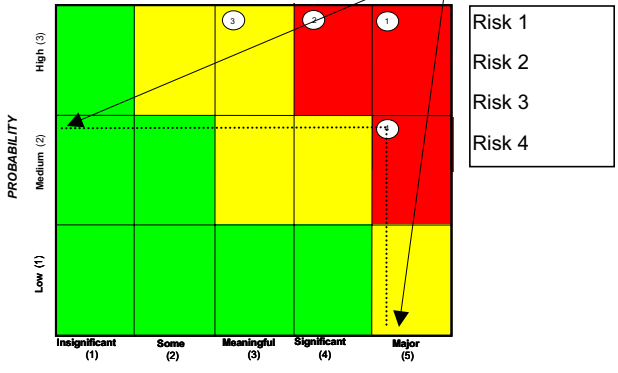
Team monitoring date:

Please see the explanation notes behind each to

Sort all by Top-Down

Risk ID	Strategy, STP1H or STP2H	Root causes of risk event	RISK EVENT	Consequences	Estimated Impact during 3 years (MEUR)	of which may actualise during next STP period (MEUR)	Estimated impact scale (1-5)	Estimated probability scale (1-3)	Risk Magnitude
1							5	3	HIGH
2							4	3	HIGH
3							3	3	MEDIUM
4							5	2	HIGH
5									N/A
6									N/A

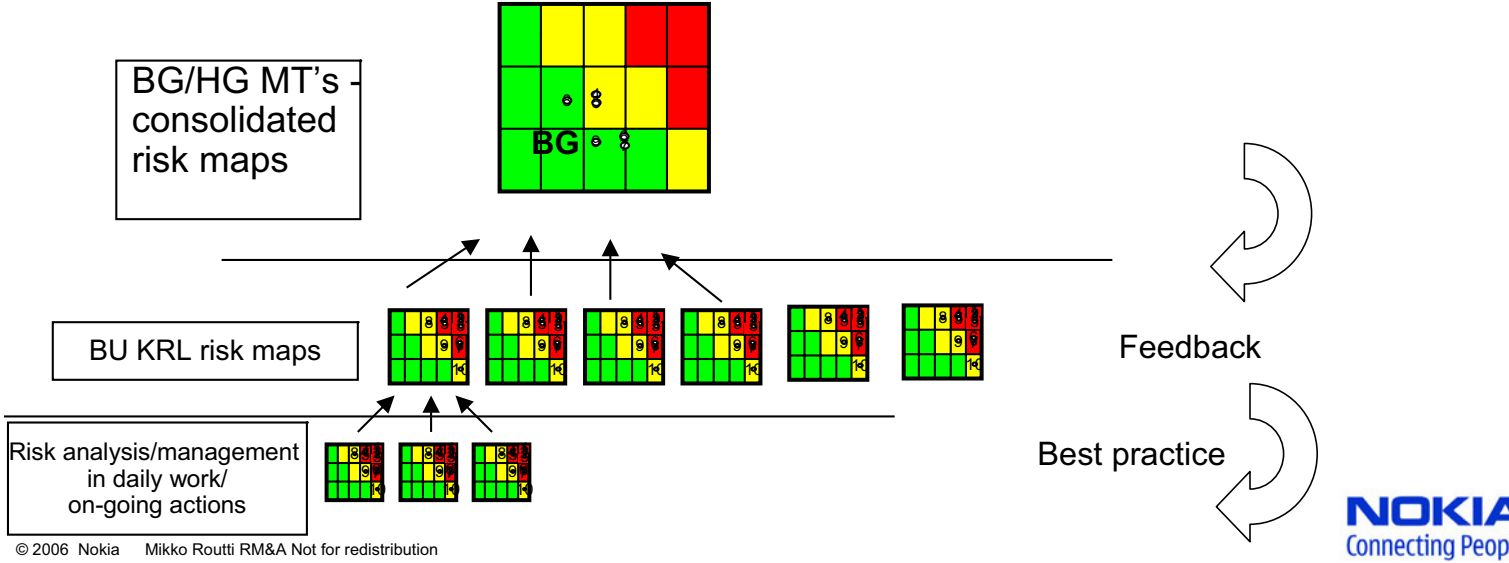
Key Risk Map



NOKIA Connecting People

Operative RM in daily work and projects

- risk management in daily work and projects (Project RM)
- best practice: BU's/teams follow their risks on on-going basis
- LRP/STP planning: a snap-shot created for reporting
- BG/HG/CF normal follow-up of key risks/agreed actions (qtrly, monthly)



NOKIA
Connecting People

Common language requires common vocabulary

example

A

Accepted risks
Description of risks which exist but business owners have decided not to mitigate them. However, some of them will be actively followed

Action owner
Person who is responsible that risk controlling actions are planned, agreed, documented and implemented.

Assurance
Nokia's approach to bring visibility and assurance to management and the Board on key risk areas and on the design and effectiveness of risk controls in business processes. Assurance means also the comfort the individual manager gets from risk management and control actions

Assessment
An analysis about the current state of processes and their maturity compared to defined benchmarks

I

Impact
The evaluated loss/effect in qualitative and monetary terms

Internal control
Internal control consists of measurement and monitoring of business objectives and performance, supported by quality, control, risk and monitoring processes

M

Maturity
Defines the level of understanding, framework and implementation of the issue in question

O

Objective
A goal that has an achievable, well-defined target level of achievement.

P

Probability
The likelihood of risk event occurance by taking the current controls into account

Problem
Problem - a realised issue which can be defined as a consequence of a risk event identified at earlier stage

R

Risk
Any uncertainty that affects the objectives and achievement of optimum result.

Risk analysis
A process step in risk management. Risks are categorized and consolidated, risk scenarios are completed for main risk events and risk effects, probabilities and utility losses are estimated for all risk scenarios

Risk appetite
Risk appetite expresses the organizations willingness to take risks. Risk appetite is defined at the end by the board and can vary between risk areas and categories.

Risk effect / consequence
The combined impact of risk event and resulting reactions to goals

Risk event
An occurrence of an incident with some negative consequences

Risk factor
A known fact or characteristic that influences some risk event

Risk identification
A process step in risk management. Potential threats to the project are identified using a chosen approach

Risk magnitude
Significance or size of the risk. Determined by a risk's probability of occurrence and (utility) loss would cause.

Risk management authority
Ultimate decision making authority is defined in risk management mandate. Authority is to decide which approach to risk is to be taken in unclear situations.

Risk management coach
A Nokia person with professional skills and responsibilities in other areas but additionally authorized by his/her superiors and qualified for assisting the implementation of risk management activities within his/her respective area.

Risk management mandate
An explicit definition of the scope, frequency, focus, responsibility and chain of authorities in a specific area for risk management

Risk management mandate definition
A process step in risk management. The scope and frequency of risk management and the relevant stakeholders are defined in this step

Risk monitoring
A process step in risk management. Risk controlling actions and chosen/new risks are monitored in an agreed forum and interval.

Risk owner
Risk owner is the function or person who is responsible for managing the risk and takes the upside and downside to the P&L

Risk prioritization
Ranking of risks. Risk scenario probabilities are estimated and utility losses of scenarios are ranked separately for each relevant stakeholder

Risk scenario
A combination of risk elements that describe the causes, triggering events and the impact of a risk. Normally a scenario consists of a risk event, risk reaction and risk effect set

Risk tolerance
The grade of risk aversion defined by a company's ability to be exposed to various risks. Main criteria for defining risk tolerance are financial, operational and ethical measures

Root cause
The original reason for risk to exist.

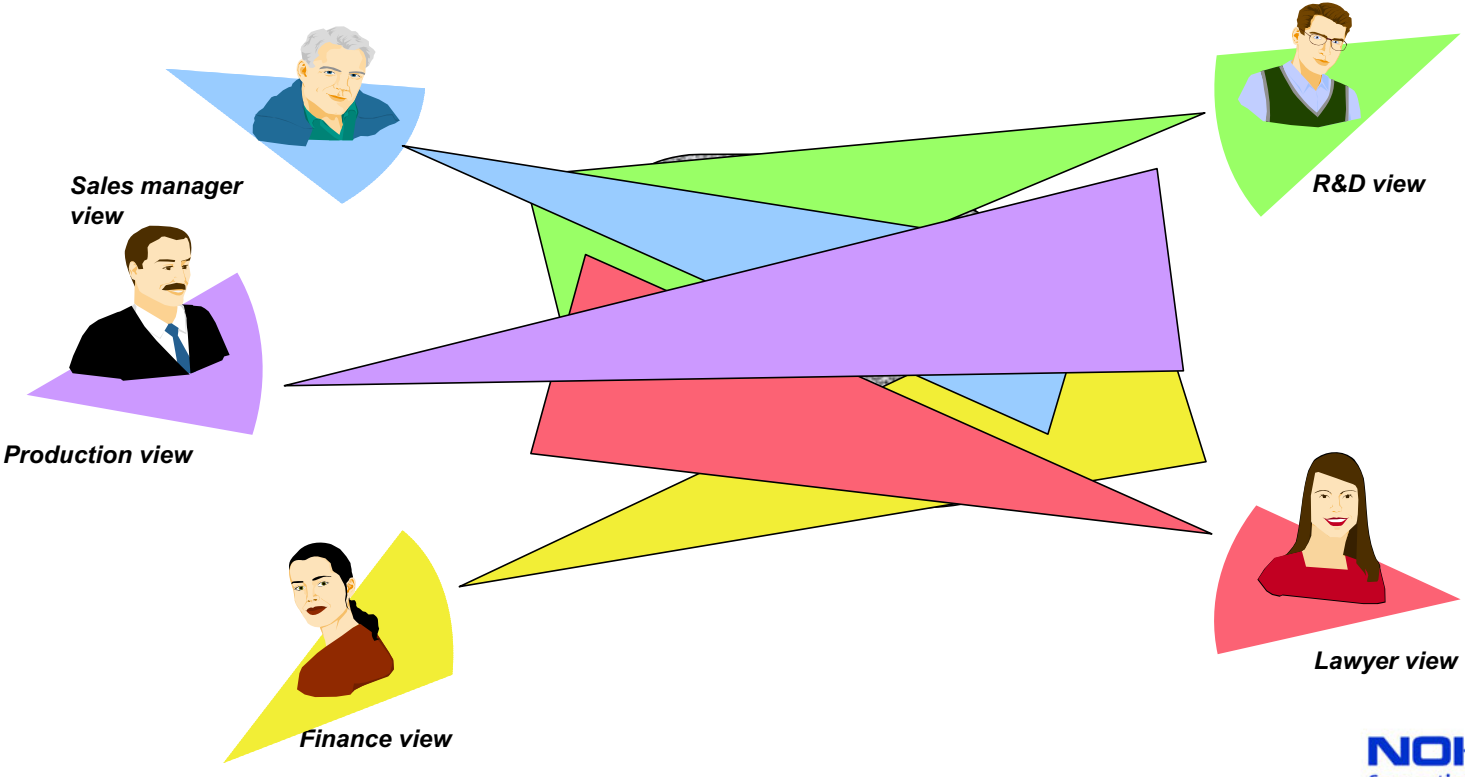
S

Stakeholder
Any individual, group, organization, or institution who can affect or be affected by the work goals or their results

Self Assessment
A concept designed for the organization and individuals to be able to define its own maturity and status at defined areas.

NOKIA
Connecting People

Risk Workshops give wider coverage



NOKIA
Connecting People

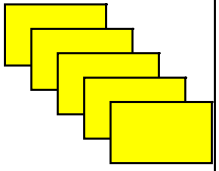
Identification: Checklists vs. Brainstorming

Checklists

- Pros
  - Fast and easy to use
  - Standardize results
  - Cover a broad area
  - May prompt thinking new risks
- Cons
  - Cause fatigue
  - Do not encourage creativity
  - May be biased due to a different domain
  - Do not encourage finding situation specific risks

Brainstorming

- yellow stickers etc

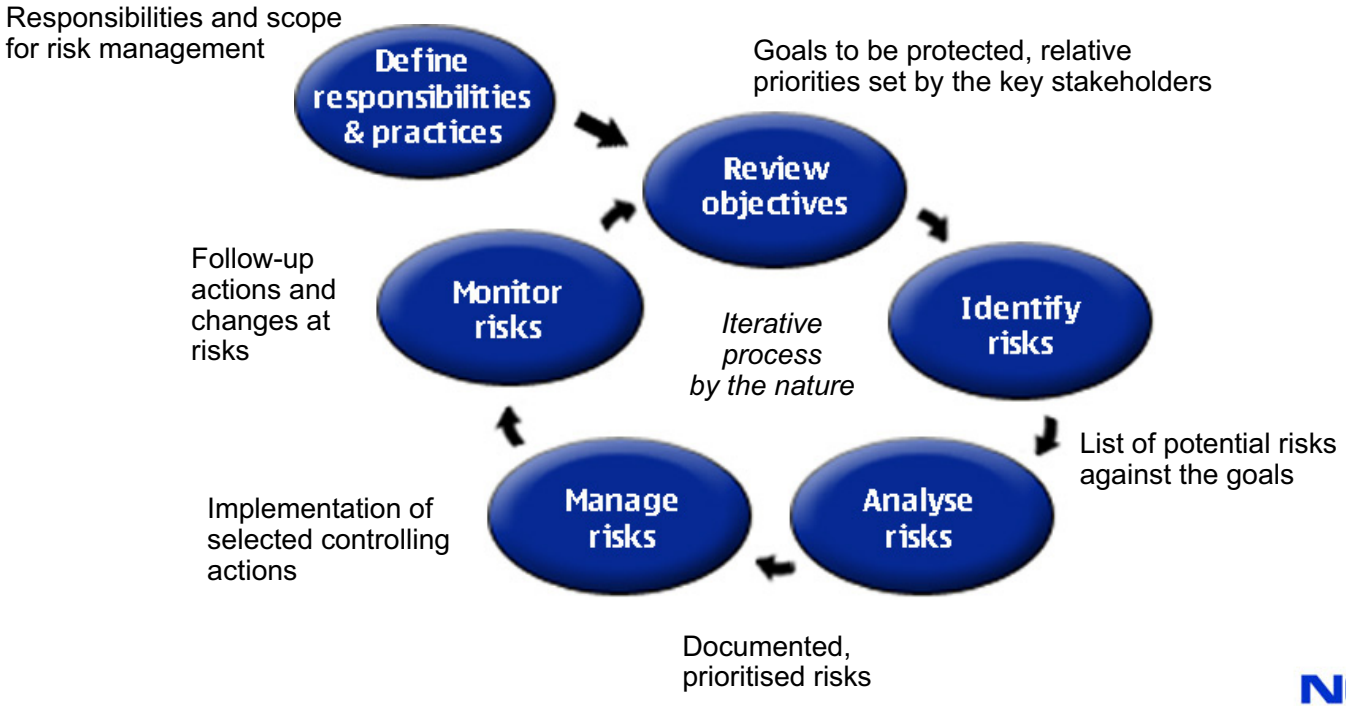


- Pros
  - Fast and easy to use
  - Leverages local expertise and insight
  - Keeps participants active
  - Develops commitment
- Cons
  - Requires facilitation or training
  - Meeting dynamics may bias results
  - Dependent on participants experience

NOKIA
Connecting People

RM Process Cycle – used in major projects/ cases

It describes elements which should exist in a good process or project



NOKIA
Connecting People

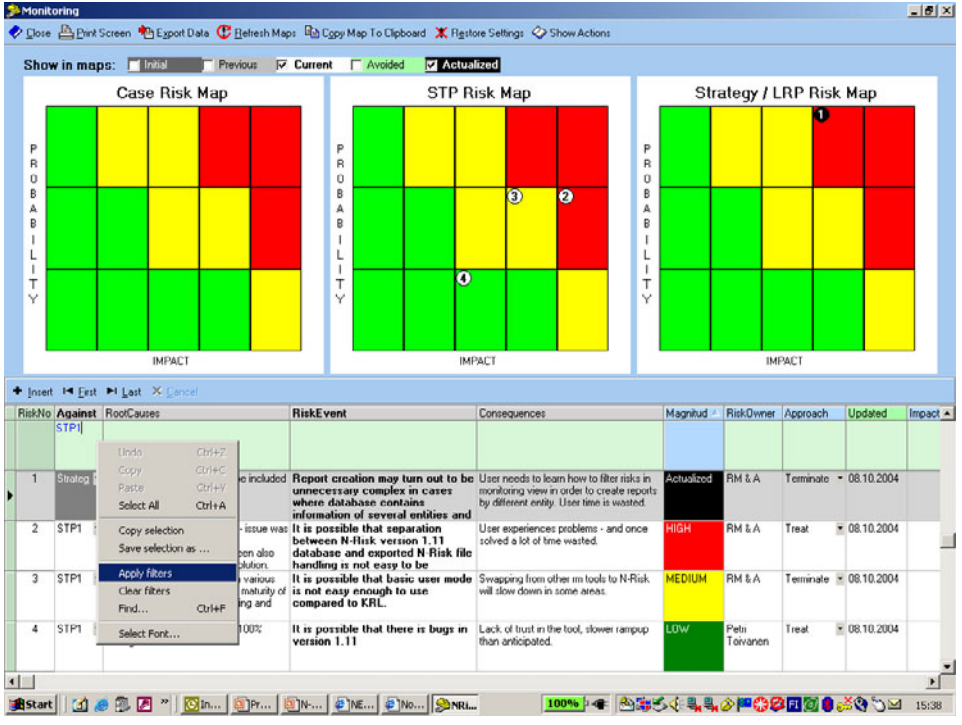
N-Risk Tool for analysing and storing risk data

- Supports to define risks in **meaningful** way, and to **compare** and **share** risk data

- **All in one tool set**
  - Basic/advanced user modes
  - Data import/export
  - Automatic key risk map creation

  - Action database
  - Actions summary table

  - Automatic history recording



NOKIA
Connecting People

Metrics for (self)-assessing RM maturity

Example section with illustrative scores. However, the maturity report shows only the average of approach and deployment

Rating	Approach	Rating	Deployment
1	Mechanism for planning work and target setting exists	1	Planning cycle is followed and objectives are documented
1	Risk identification and analysis methodology exists	1	Risk idenfication and analysis done as part of planning process
1	Risk management actions are defined		Actions are systematically implementing
1	Follow-up system is defined	1	Risk Management is integrated to reporting processes
	Practices and Roles are agreed and documented		Agreed structures are followed in practice
4	**TOTAL POINTS IN APPROACH**	**3**	**TOTAL POINTS IN DEPLOYMENT**

How do we follow "the market"? - Example

- ✓ **Embed Risk Management into Existing Processes**: Global risk management exemplars are not creating new and separate risk processes to identify, measure and mitigate risks, but instead are **embedding risk discipline into existing** processes—strategic planning, forecasting, KPIs, incentives, and the capital budgeting process. Embedding risk management in existing processes minimizes reporting burdens and ensures risks will be considered in all business decisions.

- ✓ **Decentralize Most Risk Management**: Leading CFOs are resisting the adoption of centralized ERM because of its dubious benefits and its inordinate costs. Instead, they are keeping most responsibility for identifying and mitigating risk in the line, not the corporate center.

- ✓ **Adopt a Limited Role for the Center**: The best risk management role for the center is to **aggregate and prioritize business unit risks**, to communicate risk exposure and mitigation strategies to stakeholders, and to **partner with the business** units to help them manage risks more effectively.

- ✓ **Encourage Appropriate Risk Taking**: Unfocused, overly inclusive risk tracking and mitigation initiatives may have the unfortunate impact of stifling business unit innovation, overloading business unit finance directors, and creating a culture of "incrementalism."

- ✓ **Allow for Flexibility in Risk Assessments**: The challenge that most CFOs face when creating a new risk assessment process is that **templated assessments typically result in superficial risk evaluations** from the line, but the **absence of templates makes it difficult to aggregate business unit risks** at the enterprise level. To solve these challenges, leading companies customize sections of templated questionnaires by business unit and/or allow for commentary on additional risks. Companies that **do not use** templates facilitate risk aggregation by providing the line with clear risk categories and definitions.

Source: CFO EXECUTIVE BOARD

Conclusions

- focus is in **proactively managing the business risks** the company itself needs to manage, rather than responding to external issues
- risk reporting is integrated into planning process both short and long term; unified risk terminology, and common but scaleable metrics
- key risks are identified and validated in business units, business groups and executive team, before reporting to Board. Content is basis for 20F SEC report
- methods to assess team's RM maturity (how good we are in this?) and to assess any risk area, current practices and learn
- all practices are focused on providing **on-time, 80/20 correct, and actionable** view on future events rather than provide complex modelling

- Thank You, Questions or Comments?

A-2
Lessons learned from the SOX exercise

Maria Nikula (SWE)
Vice President, Group Internal Audit
Volvo Construction Equipment Group

Lessons Learned from the SOX Exercise

within

Volvo Construction Equipment

Maria Nikula

VP Internal Control

Volvo Construction Equipment

- Develop, manufacture & market construction equipment
- Active on all continents; 60+ entities
- Net Sales € 3.8 billion
- 15% of the Volvo Group in terms of Net Sales and Operating Income

Construction Equipment

Background

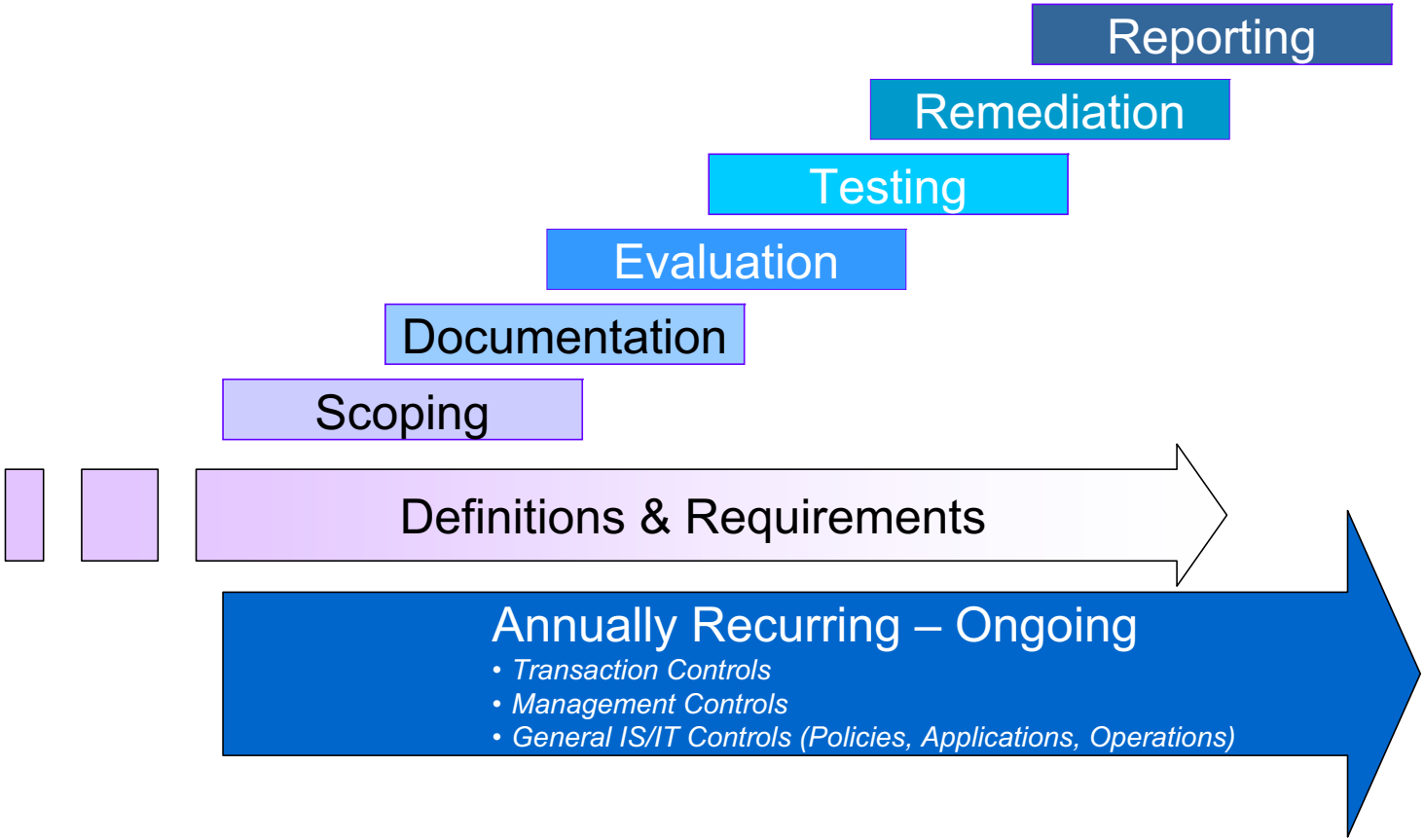
SOX project

Pre-study

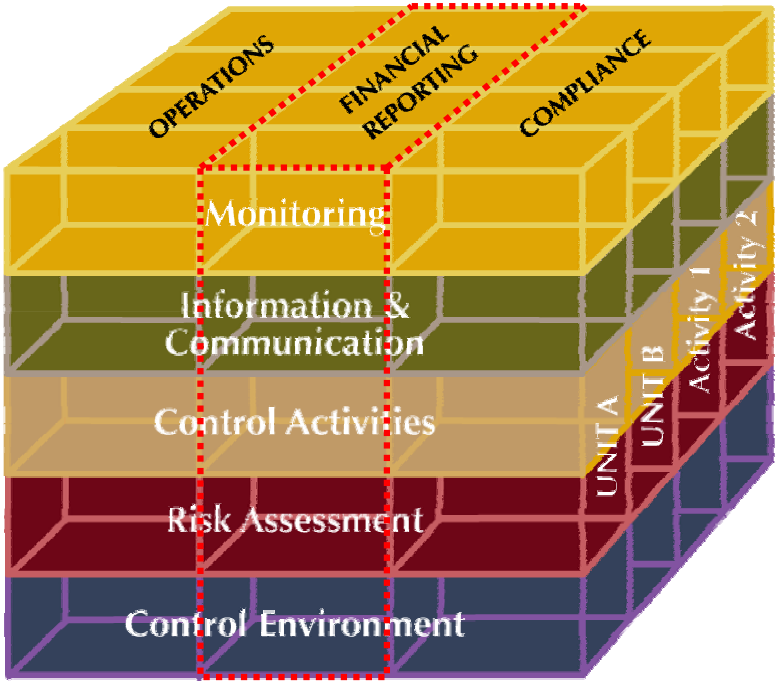
Project organization

1. **Management Controls**: all entities
   - *Control Environment*
   - *Risk Assessment*
   - *Information & Communication*
   - *Monitoring*
2. **Transaction Controls**: major entities & processes
   - *Control Activities*
3. **[General IS/IT Controls**: major entities**]**

The SOX Project



COSO Framework

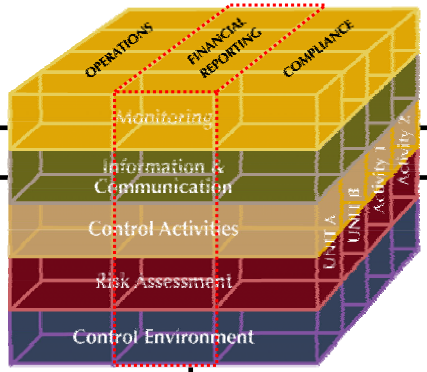


Monitoring

- Walk the talk
- Consistency
- Responsibility & delegation
- Role of
  - Internal Control
  - Internal Audit
  - External Audit

Information and Communication

- Availability
- Info packages & E-learning
- Buy-in
- *Global issues*
  - *Language*
  - *Culture*
  - *Practicability*



Control Environment

- Basics
  - Ethical values
  - Code of Conduct
  - Assignment of authority
  - Conflict of interest
- Policies
  - Adequate & clear
  - Coordinated & aligned

Control Activities

- Understanding of purpose
- Risks ←→ Control Objectives
- Automated controls
- Documentation
- Effectiveness
- Holistic view & process improvement

Risk Assessment

- Definition
- Method
  - Relevance → FR
  - Effect → FR
  - Activities & controls
  - Responsibility
- On-going

Conclusions

- Payback
- Internal Control Awareness
- Role of Internal Audit & Internal Control

A-3
Challenges for Internal Audit in Global Player companies

Bernd Schartmann (GER)
Head of Corporate Audit & Security
Deutsche Post World Net

Deutsche Post World Net

MAIL EXPRESS LOGISTICS FINANCE

Challenges for Internal Audit in Global Player Companies

Bernd Schartmann, Executive VP Corporate Audit & Security
Deutsche Post World Net, Bonn, Germany
Helsinki, Sept 7th 2006

Agenda

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

- Categorization of a Global Player Company
- Deutsche Post World Net – DPWN
- General Potential Challenges for Global Player Companies
- Challenges for Global Player Companies‘ Internal Audit Functions
- DPWN ‘s Response to Global Player Companies’ Internal Audit Challenges

Categorization of a Global Player Company

Global Player Company

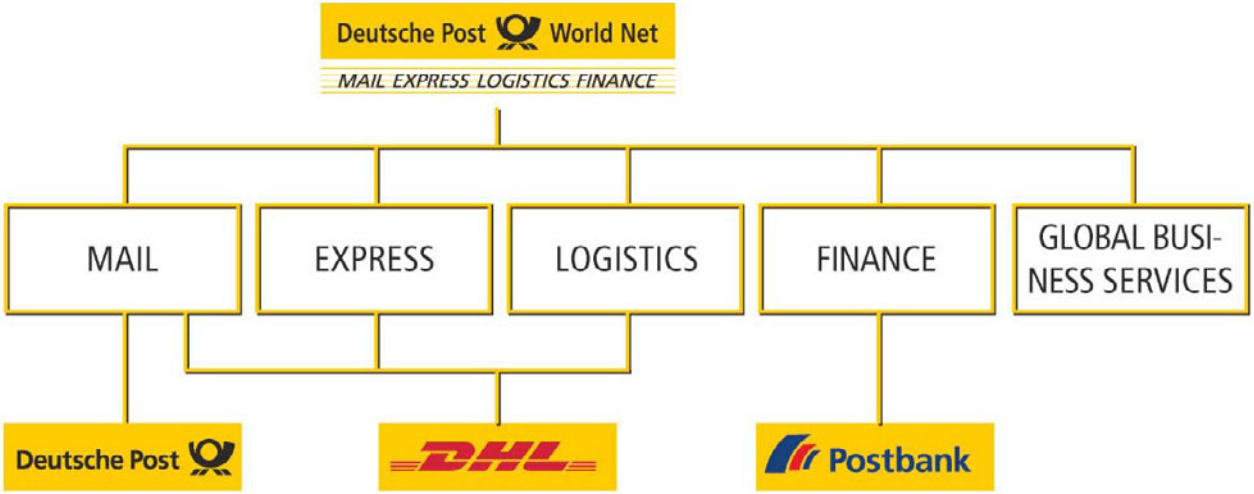
„A Global Player is a large, internationally operating company with economic power and influence over economic and political decisions. A Global Player possesses a dense information network and organizes the production and distribution of goods considering the most cost effective locations globally."

Differences to „Local Player Companies“

- Diverse management cultures
- Diverse employees cultures
- Permanent flexibility / change
- More potential conflicts of interests
- Multiple Stakeholders
- Multiple legal / compliance requirements
- High degree of structural complexity (Organization, Processes, IT)

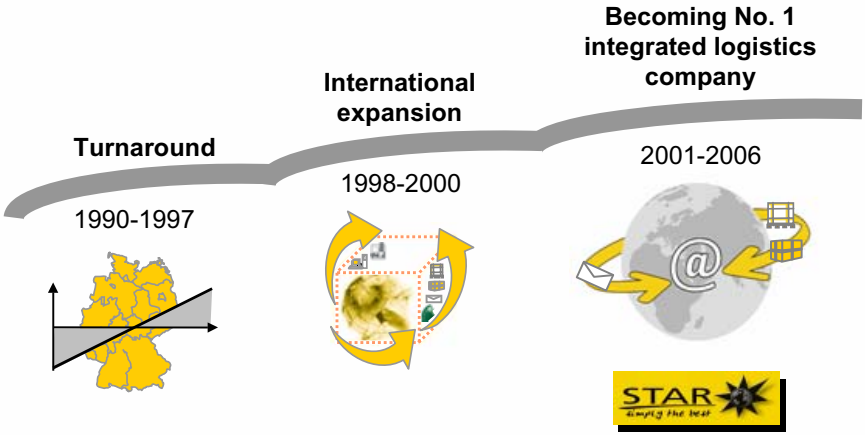
Deutsche Post World Net - a Global Player

- > 500.000 employees => DPWN is Europe´s biggest employer
- > 60bn € revenues



DPWN today

DPWN has successfully completed the third phase in its young history and today has reached the leading position



Where are we today

- Leading global player in our industry
- Leading market positions in each major segment
- Significantly improved profitability
- All built on solid financial foundations

Agenda

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

- Categorization of a Global Player Company
- Overview Deutsche Post World Net – DPWN -
- General Potential Challenges for Global Player Companies
- Challenges for Global Player Companies‘ Internal Audit Functions
- DPWN ‘s Response to Global Player Companies’ Internal Audit Challenges

General Potential Challenges for Global Players

Complexity

- Diverse business fields / markets
- High level of product customization
- Extensive number of entities
- Limited visibility into resource availability
- Limited process harmonization
- Size

International Environment – Cultural Differences

- Geographical distances, Time difference
- Communication barriers
- Multiple languages
- Different cultural habits
- Religious aspects
- Management styles
- Diverse customer taste
- Currencies, transaction costs

General Potential Challenges for Global Players

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

Competition

- Heterogeneous markets
- Local Competitions
- Fragmented pricing
- Endogen competition restrictions (e.g. Chinese Government)
- Reputational risks

Legal Requirements

- Labor law requirements
- Financial reporting requirements (IFRS, US-GAAP, HGB)
- Potential for conflict of legal requirements (e.g. SOX whistleblower hotline and local data protection laws)
- Various environmental minimum standards

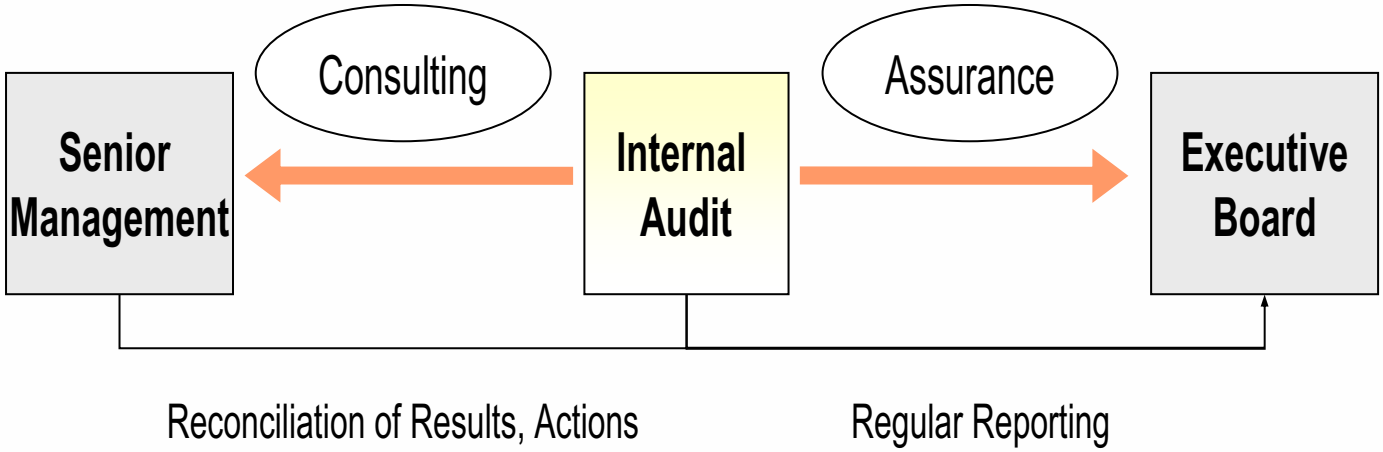
Coordination of Work Tasks

- Complex Hierarchies
- Multi Layer Organizational Structures (central, regional)
- Diverse reporting structures and reporting lines
- Incompatible communication infrastructure (incompatible systems)
- Long decision ways

Conclusion

- Global Player Companies have to meet a wide range of challenges in their everyday working tasks
- Challenges of the Global Players are at the same time challenges for their individual Internal Audit Functions
- Question is:
  - What are the precise challenges an Internal Audit Function of a Global Player Company has to meet?
  - Where should these Audit Functions focus on?

Internal Audit provides assurance and consulting services



Historical Change of Internal Audit tasks

TRADITIONAL

- **Regularity**
- Protection of assets
- Reliability of financial data
- Compliance with laws and regulations

MODERN

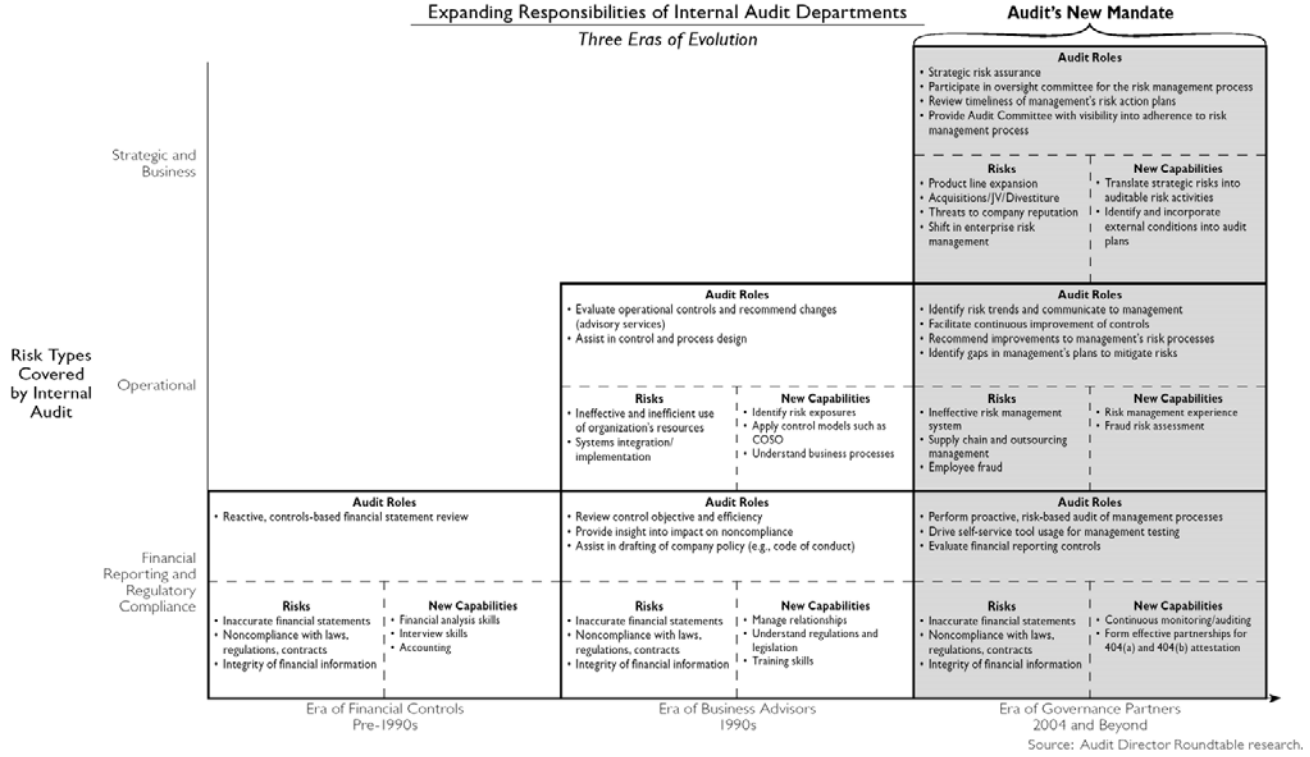
- **Achieving company objectives**
- Functionality and efficiency of company processes (Operational audit)
- Advise for the Management (Management Audit)
- Regularity (Financial Audit)

Challenges for Internal Audit Functions within Global Player companies

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

A Governance Partnership Framework

Maintaining a risk focus will drive leading Internal Audit departments to expand the scope of their future responsibilities



Source: Audit Director Roundtable research.

Reporting Lines

- Audit Committee and Board of Directors reporting lines
- Global and local reporting lines
- Direct and indirect reporting
- Difficulties in task priorisation

Internal Audit Reporting Relationships

Activity	Owner							
	Audit Committee Chair	Audit Committee (collectively)	CEO	CFO	General Counsel/ CLO	Chief Compliance Officer	CAO/ Controller	Other
Audit Plan Approval	6.9%	88.1%	2.0%	5.9%	1.0%	0.0%	2.0%	2.0%
IA Charter Approval	10.9%	85.1%	5.0%	3.0%	2.0%	0.0%	2.0%	1.0%
IA Policy Guidance	8.9%	57.4%	8.9%	14.9%	3.0%	2.0%	3.0%	9.9%
Audit Work Guidance	12.9%	38.6%	7.9%	21.8%	5.0%	1.0%	5.0%	12.9%
Audit Director Compensation/Benefits	6.9%	14.9%	19.8%	45.5%	12.9%	1.0%	2.0%	6.9%
Audit Director Performance Review	10.9%	17.8%	20.8%	44.6%	12.9%	1.0%	3.0%	5.0%
IA Budget Approval	4.0%	35.6%	16.8%	40.6%	6.9%	1.0%	3.0%	4.0%
Audit Director T & E Expense Approval	1.0%	1.0%	17.8%	45.5%	15.8%	1.0%	5.9%	9.9%

n = 101

Audit Planning

- Risk oriented Planning – Know how of company strategies and risks
  - Focusing the audit to relevant risks which threaten business objectives
  - Strong audit legitimacy and the source to initialize audit subjects
- Process oriented Planning
  - Creation of a cross-departmental view of the audit subject ignoring organizational / jurisdictional or geographical restrictions
  - Distinguishing core processes and supporting processes
  - Stable basis to develop audit subjects
- Annual and multi year planning
- Capacity planning locally and globally

Communication with Internal Audit Function

- Necessity of regular and clear communication

  -Definition of responsibilities - who is communicating to whom?

  -Definition of types of communication

  - Ad Hoc Communication, regular communication cycles

- Ways of communication

  -Formal meeting (e.g. Jour Fixes, Conferences)

  -Informal Meeting

  -Newsletters

  -Phone Conferences

  -Video Conferences

  -Email

Conclusion - Hypothesis

In order to make Internal Audit Function work effectively on global level, central steering and uniform as well as standardized approaches are necessary

to be shown on example DPWN

Agenda

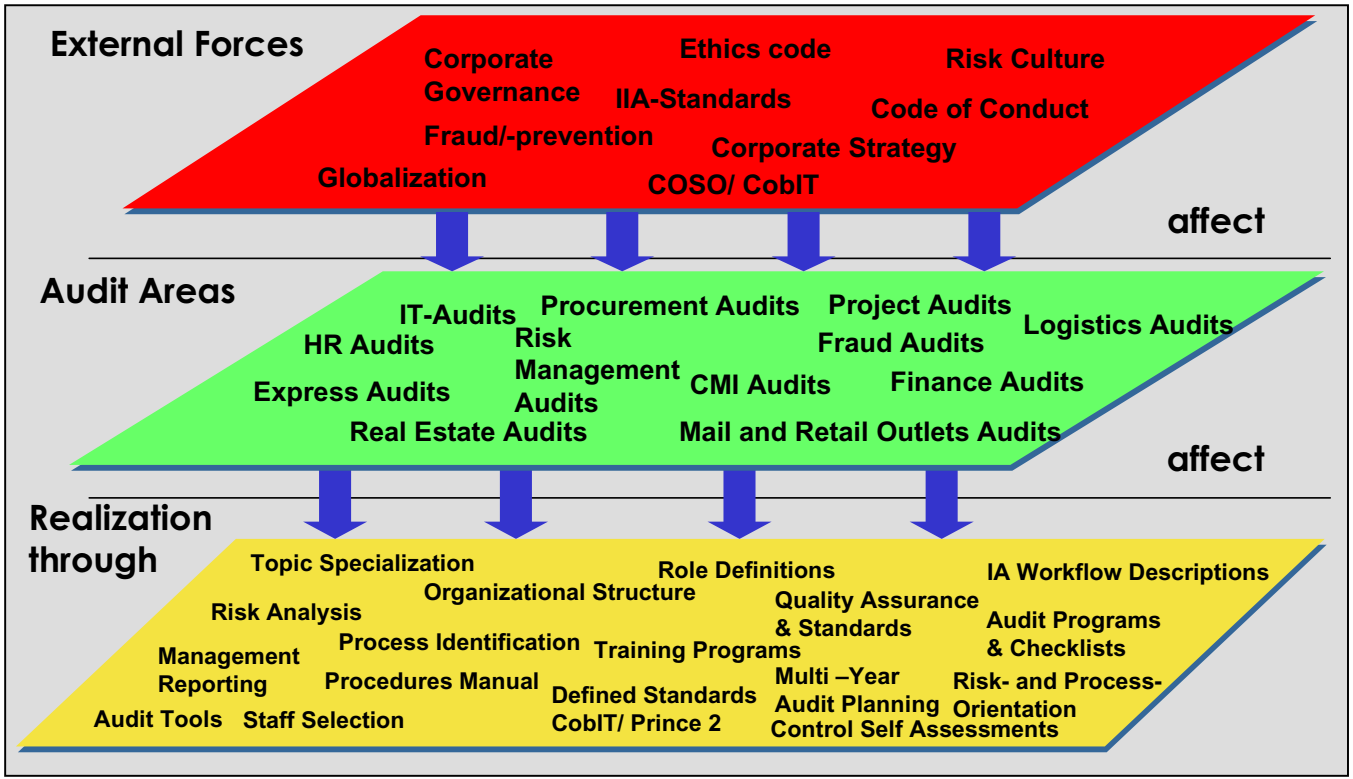
Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

- Categorization of a Global Player Company
- Overview Deutsche Post World Net – DPWN -
- General Potential Challenges for Global Player Companies
- Challenges for Global Player Companies‘ Internal Audit Functions
- DPWN ‘s Response to Global Player Companies’ Internal Audit Challenges

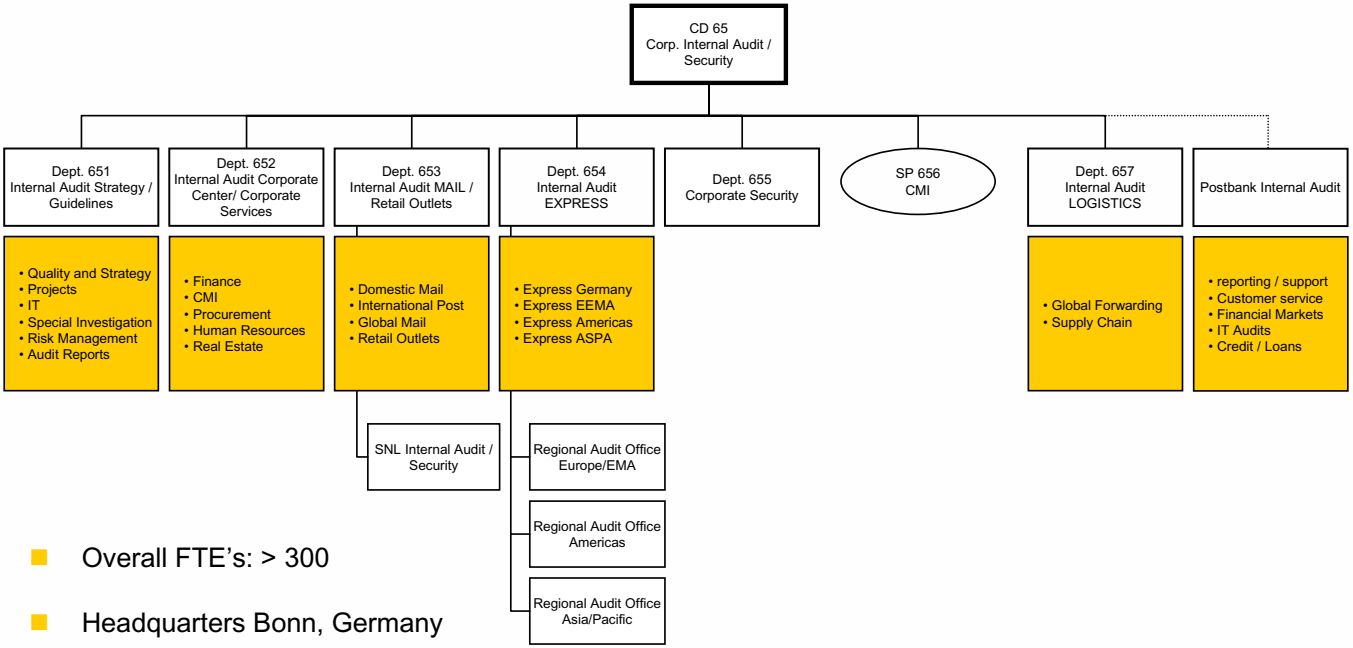
DPWN 's Response to Global Player Companies' Internal Audit Challenges

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

Internal Audit is influenced by…



DPWN Internal Audit Organisation



- Overall FTE's: > 300
- Headquarters Bonn, Germany
- International Locations: 4

Principles of the structure of DPWN Internal Audit

- Internal Audit organizational structure follows business organization structure.
  - Internal Audit Departments are mirror images of Business Units on corporate, regional and local level
  - Clear accountability and responsibilities for Audit Topics within the function
- Internal Audit of DPWN is set up within a clear Matrix organization
  - Disciplinary (administrative) responsibilities
  - Functional responsibilities
  - Responsibilities of Internal Audit have been clearly defined in "ICADE Codes"
- Direct and central reporting lines
  - All regional Audit Functions are reporting directly to their responsible Corporate Audit Function in the Headquarters
  - No reporting requirements to local or regional Business Units

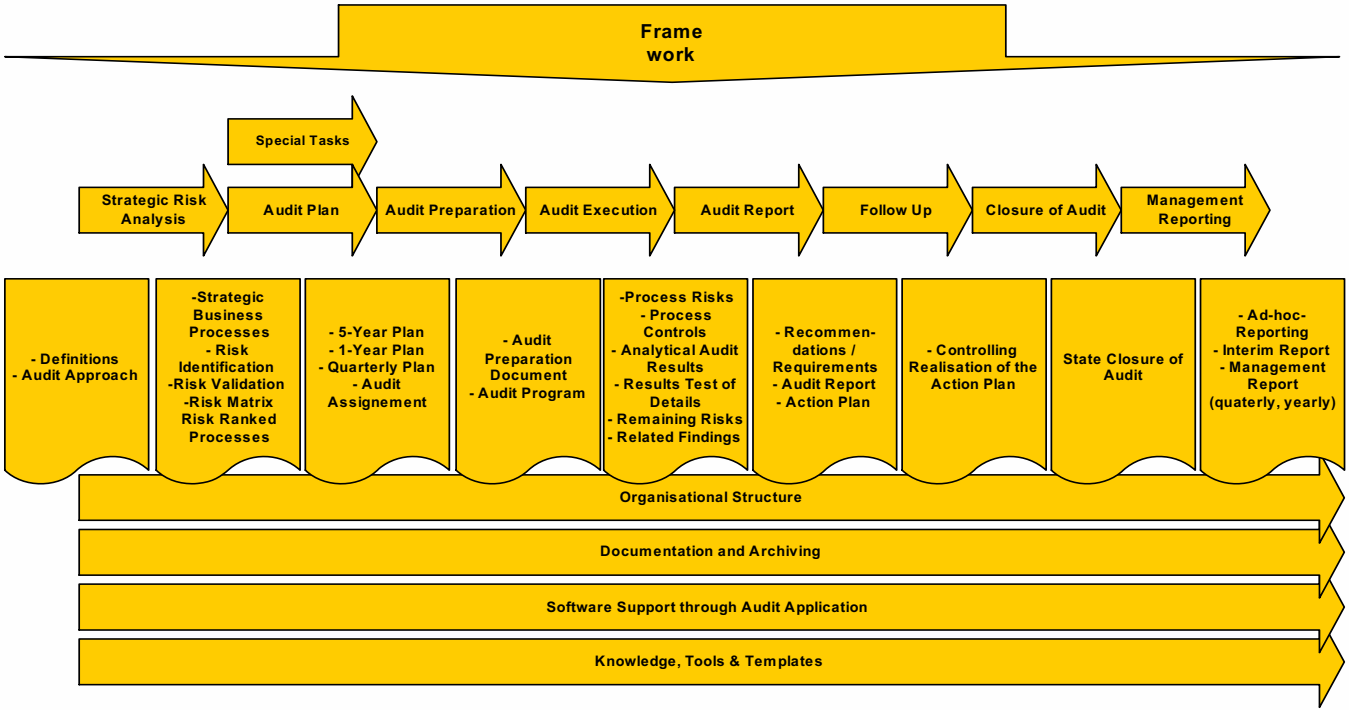
Structure of DPWN Internal Audit

- Corporate Internal Audit Function in the Headquarters is set up with overall Heads of Departments responsible for a specific Business area and Senior Experts
- The Senior Expert is the functional leader of an audit area (e.g. Finance, Logistics, IT)
- He/She is responsible for the overall coordination and execution of his audit area
  - Central contact person within the Corporate Center for all issues regarding the audit area
  - Customer Management
  - Identification and Review of strategic issues concerning the audit function
  - Development of Methods, KPI's, Audit Programs
  - Responsibility for the overall audit plan of the function
  - Scheduling of audits in close coordination with the local audit managers
  - Quality Assurance of the audit reports and audit documentation
  - Creation of Management Reports
- There is a very close working relationship between the Senior Expert in the Corporate Center and the respective audit managers in the regions.

Structure of DPWN Internal Audit

- Internal Audit Function of DPWN has a **central budget**
  - For the Internal Audit function of DPWN **all costs** (including the costs of the Regional Audit Offices) are Corporate Center Costs, as these are paid centrally.
  - It makes no difference, if people are located in the Corporate Center or in the regions, as all costs are paid out of the Corporate Internal Audit Budget.
  - Provides Independence for Internal Audit Function, as there is no dependency on local organizations or business units
  - Possibility to plan and steer Audit function on a global basis

Uniform and Standardized Audit Workflow

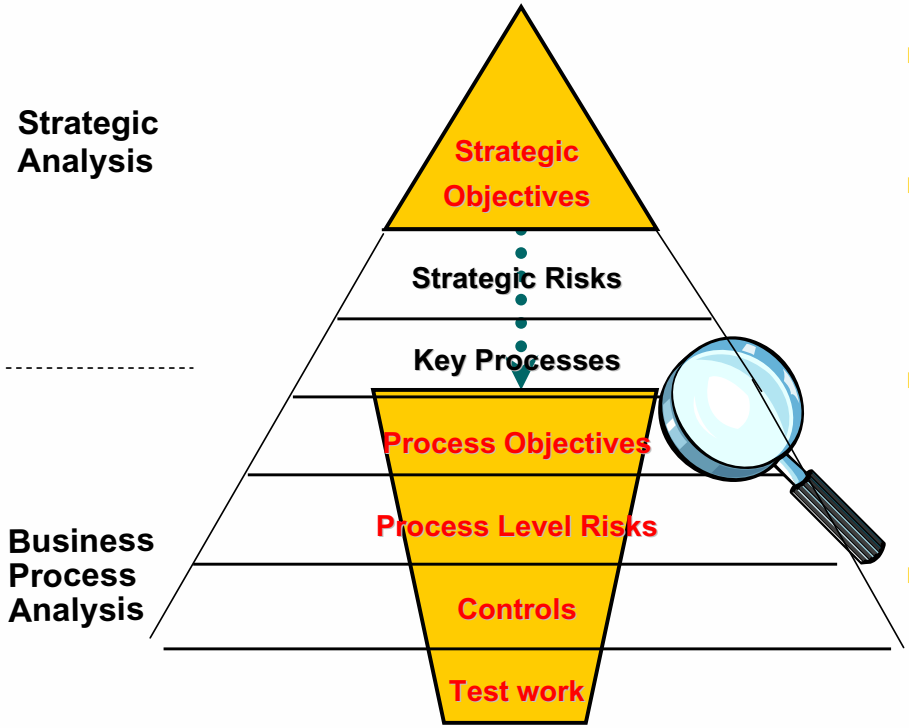


Uniform and Standardized Audit Workflow

- Standardization of Audit Work on a global scale:
  - Working Procedures for different audit functions
  - Audit Programs and Tools
  - Audit Templates
  - Audit Processes
  - Consistent and uniform audit approach
- Uniform standards eases working on a global level
- Recognition of Audit Work performed by Internal Audit globally through Board of Management is also a marketing effect for Internal Audit function

DPWN 's Response to Global Player Companies' Internal Audit Challenges

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

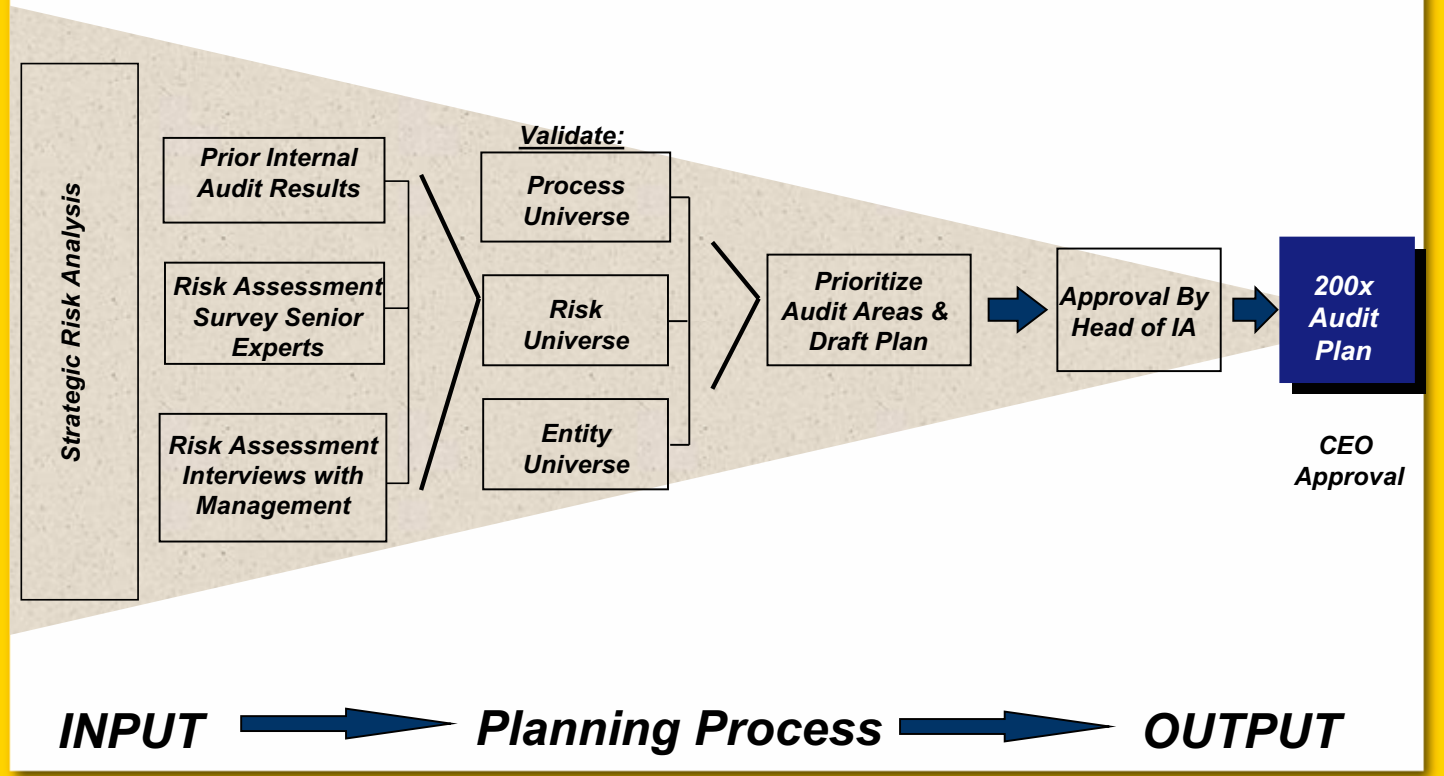


- Through the Strategic Analysis, strategic risks facing the organization are identified.
- Linking our processes to these risks helps to determine the appropriate audits to address those risks consistently throughout the organization.
- It is important to remember, that business processes have been implemented to address strategic objectives and to respond to the strategic risks.
- Hence, on the basis of the strategic risks, we have to decide, which processes and entities will be subject of the audit plan.

DPWN 's Response to Global Player Companies' Internal Audit Challenges

Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

Risk and Process Oriented Planning



Risk and Process Oriented Planning

- Standardized planning process for all Audit functions globally
- Set time frame for overall annual planning cycle has been defined
- Risk and Process oriented planning is performed on a
  - Quarterly basis (detailed planning including resource scheduling)
  - Yearly basis (planning of audit subjects per Audit function on detailed process or entity level)
  - Multi-Year basis (planning on overall process level)
- Multi-Year Planning supports to ensure that whole audit universe is audited during a set time period
- Cluster of Processes in “A-”, “B-” and “C-” Processes
  - Depending of Risk Grading (A,B,C), decision on Audit Cycle (1-5 years)
- Time buffer within audit plan to account for Special Audit Requests set by the Board of Management

Risk and Process Oriented Planning

Overview:

- 5-Year-Audit Plan
  - Defining the audit cycle of processes using a ABC-structure of materiality
  - To be updated on a yearly basis
- 1-Year Audit Plan / Quarterly Audit Plan
  - 1-Year Audit Plan is to be assigned by the chairman of the board
  - Deriving audit subjects by using
    - CSF (Critical Success Factors) and
    - KPI (Key Performance Indicators)
- Defined workflow to integrate special audit assignments (including special investigations) which are not covered by the audit plan

Implication / Benefit:

- Covering the entire „audit universe" set up by business processes – no audit free spaces
- High risk processes are to be audited on a yearly basis; all significant processes have to be audited in appropriate time periods
- 1-Year Audit Plan as an official audit legitimacy
- Adequate allocation of employees by means of specialization & qualification
- Guided management interviews are held
  - to ensure an early agreement on proposed audit subjects including adjustments & additions proposed by business units/management
  - to be integrated in the audit plan
- Time/resource buffer to respond to special audit tasks

Risk and Process Oriented Planning

- Planning is conducted centrally by Senior Experts for their specific Audit functions in the Corporate Internal Audit Department
  - Support for Planning through Regional Audit Managers
- Planning Process involves a close coordination with management in order to ensure coverage of topics which have been seen as urgent or necessary by management itself
  - Regular interview cycles with Senior Management and Board of Management
- Capacity Planning of Auditors is done centrally through the responsible Senior Experts with the support of the local Audit Managers
- Joint Audits are embedded in Global Audit Plan

Execution of Audits

- Execution of Audits follows a standardized process including a clear definition of the
  - Audit Preparation Phase
  - Execution Phase
  - Opening and Closing Meeting of an Audit
- DPWN Internal Audit executes their audits based on the annual audit plan through regional Audit teams and global audit teams
  - Global Audit teams contain a mixture of specialists from all over the world
  - Regional Audit teams are set up by specialists of a specific Regional Audit Office
- Joint Audits contain specialists from different Audit Functions (e.g. Logistics, IT, Finance) to ensure that different aspects to an audit are covered by the audit team
  - Provision of best possible support to an audited unit or entity
  - Joint Audits have to be planned centrally in order to ensure that resource allocation and capacity planning are in line with overall audit plan
- Standardized Reporting Process with the use of uniform templates

Execution of Audits

Overview:

- Emphasis on the audit preparation phase
- Standardized approach during the audit execution phase
- Established feed back workflow

Implication / Benefit:

- Timely and comprehensive audit notification & coordination with the entity to be audited
- To concentrate on the significant risks (no audit from A – Z)
- To shorten the audit time on site
- To ease the audit execution of all involved parties
- Audit activities are phased from the general perspective to detailed audit activities
- Emphasis on a process level audit
- Feed back form has to be completed by Senior Management

Management Reporting

DPWN Corporate Internal Audit uses different types of Management Reporting

- Regular Meetings with key stakeholders
  - Members of the Board of Management
  - Senior Management in the different regions
  - Scheduled Meetings twice a year to discuss upcoming and newsworthy issues
- Annual Management Report
  - Yearly Report to Board of Management about all audits performed in previous year, including major information of the audits as well as recurring findings in a specific audit area
- Semi Annual Report
  - Overview of audits performed in the reporting period, including issues for escalation, issues which request Management Attention and Follow Up’s performed

Quality Review

- A regular Quality Review is a Basis for complying with the IIA Standards

1300 – Quality Assurance and Improvement Program

The chief audit executive should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness. This program includes periodic internal and external quality assessments and ongoing internal monitoring.

1311 – Internal Assessments

Internal assessments should include:

- Ongoing reviews of the performance of the internal audit activity; and
- Periodic reviews performed through self-assessment or by other persons within the organization, with knowledge of internal audit practices and the Standards.

THE INSTITUTE OF INTERNAL AUDITORS
247 Maitland Avenue
Altamonte Springs, Florida 32701-4201, USA

Quality Review

- A regular Quality Review is mandatory by Definition in the procedures manual of DPWN Corporate Internal Audit

> The Head of the Internal Audit Corporate Department will ensure that Internal Audit has a programme for continuous quality assurance and improvement, encompassing all areas of Internal Audit’s work. This programme will include internal and external assessments and guarantees the effectiveness of Internal Audit as well as compliance with professional standards. Internal assessments will take place annually and Internal Audit Corporate Department will also undergo a quality review by an external auditor at least every five years.

Approach to Quality Review

- Standard Questionnaire with quality criteria, based on the IIA Standards 1300ff.
- Review of the compliance to the Standards regarding the audit workflow, focusing on
  - Audit Planning
  - Audit Preparation
  - Audit Execution
  - Audit Reporting
  - (Audit Follow Up and Closure)
- All participants of the audit (including the Senior Experts in the Corporate Center), as defined in the ICADE-Codes are part of the Quality Review
- Sample of Audits performed in the
  - Corporate Center,
  - Regional Audit Offices,
  - Audit Service Branch, Germany

Training and Development

- Auditors at DPWN Corporate Internal Audit have general Audit Know How but are specialized in one certain field
  - Possibility to cover all audit types with specialized auditors leads to a higher acknowledgement of audit work in the business units
- Introduction of a Global Training Concept for whole audit function, covering
  - General Audit Training
  - Business specific topics
  - Soft Skills (including language skills)
  - Management Skills
- Each Auditor has a personal development plan, which is discussed with his/her superior on an annual basis

Training and Development

- Audit Teams are set up on a global level as a mixture of experienced auditors and "fresh blood"
  - Coming from a business department inside the company moving into internal audit
  - Coming from external audit companies joining the internal audit function
  - Starting with Internal Audit after finishing university
  - Coming from a specialized area outside of the company to join Internal Audit (e.g. Architects, former Police officer, etc.)
- Department gives the opportunity to all members of the audit function to move to another Audit Office for a predefined period
  - Through Standard and uniform audit approach, working methods do not change – easy settling in for auditors
  - Possibility to gain international experience within the company

Communication

- Communication is a major instrument to keep a large and internationally operating audit department functioning
- Necessity to make everyone feeling to be part of audit function
- Clear communication of decisions and tasks to whole audit function
- Clear definition and communication of responsibilities
- Regular Meetings take place on different levels within audit function
  - Jour fixes within specific audit departments
  - Jour fixes on different management levels within the audit function
  - Meetings with the Regional Audit Offices
  - Regular Newsletters
  - Global Audit Conference (every two years)

Overall Conclusion

- Challenges arising for Global Player Companies' Internal Audit Functions can only be met through
  - a clear and defined structure of the audit organization
  - Clear reporting lines
  - Clear definition of roles and responsibilities for each level within the audit function
- The more central an audit function is steered and coordinated, the more important is a clear, regular and stringent line of communication towards all organizational levels of the audit function
- Global Player companies are flexible and rapidly adapting to change
  - Internal Audit Function has to adapt to these changes at all times and proactively has to consider possible upcoming tasks in the future
  - Otherwise, these changes cannot be handled by the Internal Audit function in the long term

The Picture of the Internal Audit Function being a "toothless Tiger" has to be seen as a Picture of the Past

Deutsche Post World Net

MAIL EXPRESS LOGISTICS FINANCE

Thank you for your interest!

Bernd Schartmann, Executive VP Corporate Audit and Security

Helsinki, 7. September 2006

A-4
Quality of Audit – the only way to success

Elisabeth Styf (SWE)
ECIIA Board Member

The 2006 European Conference of Internal Audit

Quality of Audit – the only way to success

Speaker : Elisabeth Styf (Member of the ECIIA Board)

Quality of Audit – the only way to success

As an effect of the scandals during the last 5 years

- *Increased focus on corporate governance …..*
- *Legal – regulatory, SOX, Turnbull, Basel etc. or just far-sighted Boards (senior Management…)*
- *Internal Audit strengthen – increased requirements on quality*

Quality of Audit – the only way to success

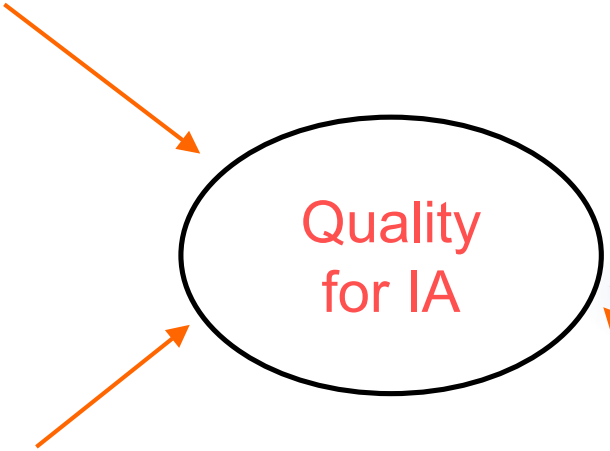
Purpose with Quality Assurance

- *Assess the effectiveness of an IA activity*
- *Assess conformance to the Standards and Code of Ethics*
- *Identify opportunities, offer recommendations for improvements*

Quality of Audit – the only way to success

Ensuring your practice is Continuous improvement oriented

Adherence to the Code of Ethics



Continued professional Development

In accordance with the Standards

Quality of Audit – the only way to success

Standard 1300

« Conducted in accordance with the standards for the professional Practice of Internal Auditing »

You must establish a quality asurance and improvement program that includes both ongoing and periodic internal QA´s and undergo an external QA every five years

.....you can delay obtaining a full external assessment and perform ***a Self Assessment with independent validation***

Quality of Audit – the only way to success

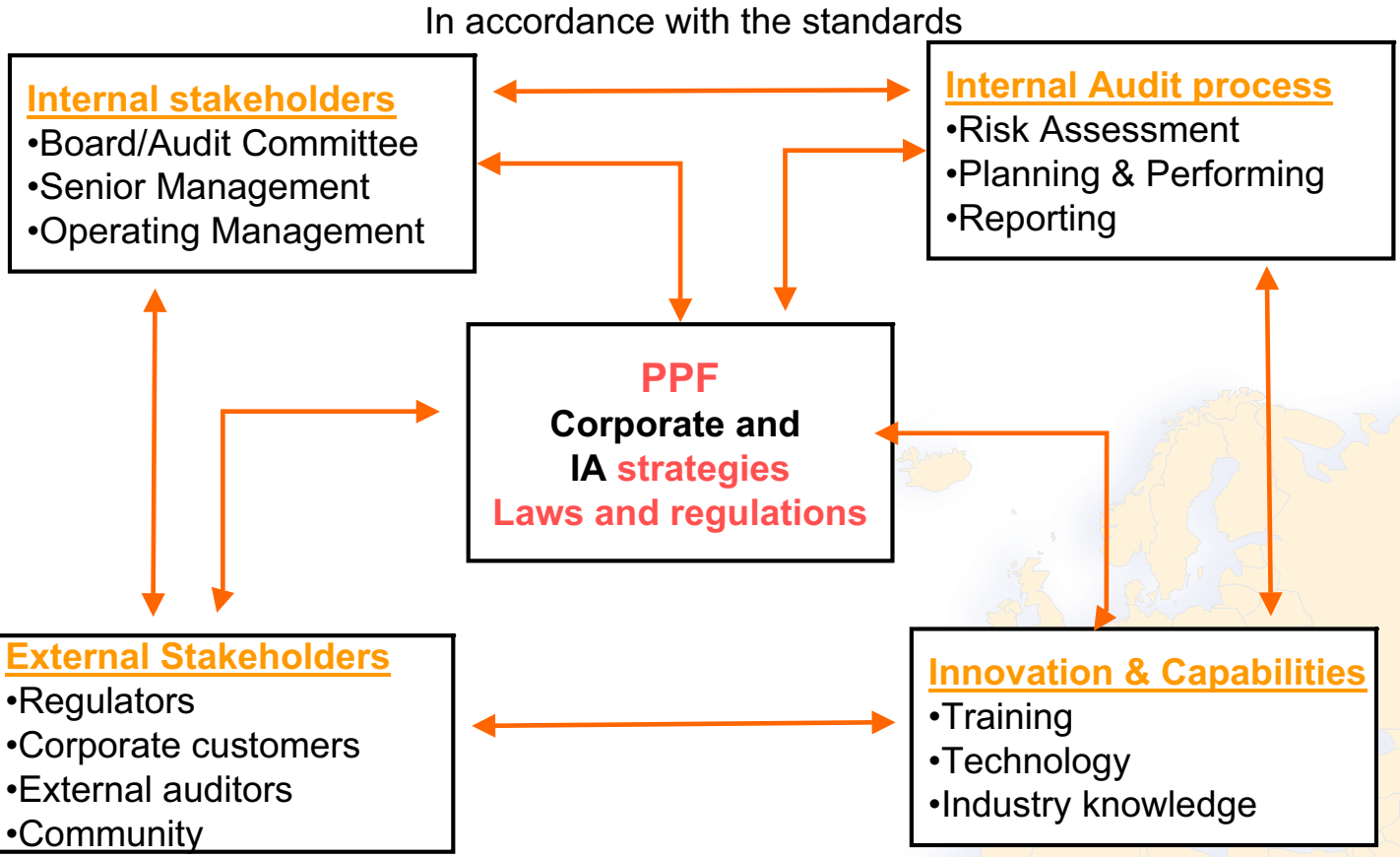
Ensuring your practice is Continuous improvement oriented

Adherence to the Code of Ethics

Continued professional Development

In accordance with the Standards

Quality of Audit – the only way to success



Quality of Audit – the only way to success

In accordance with the standards

Risk Assessment /Audit Planning
Does the audit activity assess the extent that the key risk areas are being addressed ?

Planning and Performing the audit
•Appropriate audit plans that includes scope, objectives, timing and resources allocation
• Audit performed in accordance with established methodologies and working practice ?

Communication & Reporting
Assess level of satisfaction

Internal Audit process
•Risk Assessment
•Planning & Performing
•Communication & Reporting

Quality of Audit – the only way to success

In accordance with the standards

IIA emphasize with an updated standard 2100 – IA should assist the organization in managing risks

Managements responsibility to create a professional risk management process …which means ..to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives

Example of risks

- **Strategic-opportunities** e.g. not making crucial choices among potential strategies
- **Reputation /credibility risks** e.g. compliance with laws, regulations and ethical standards
- **Funding/liquidity risks** e.g. failure to deliver funds
- **Effectiveness risks** (IT, employees etc.)

Quality of Audit – the only way to success

Nowadays it is impossible to achieve a complete and accurate picture of the past, present and future regarding various uncertainties.

- fast moving environment and technological development
- the organizations are mostly very dependent upon its relations to other actors in the environment as inter-organizational and global relationship are constantly increasing

Quality of Audit – the only way to success

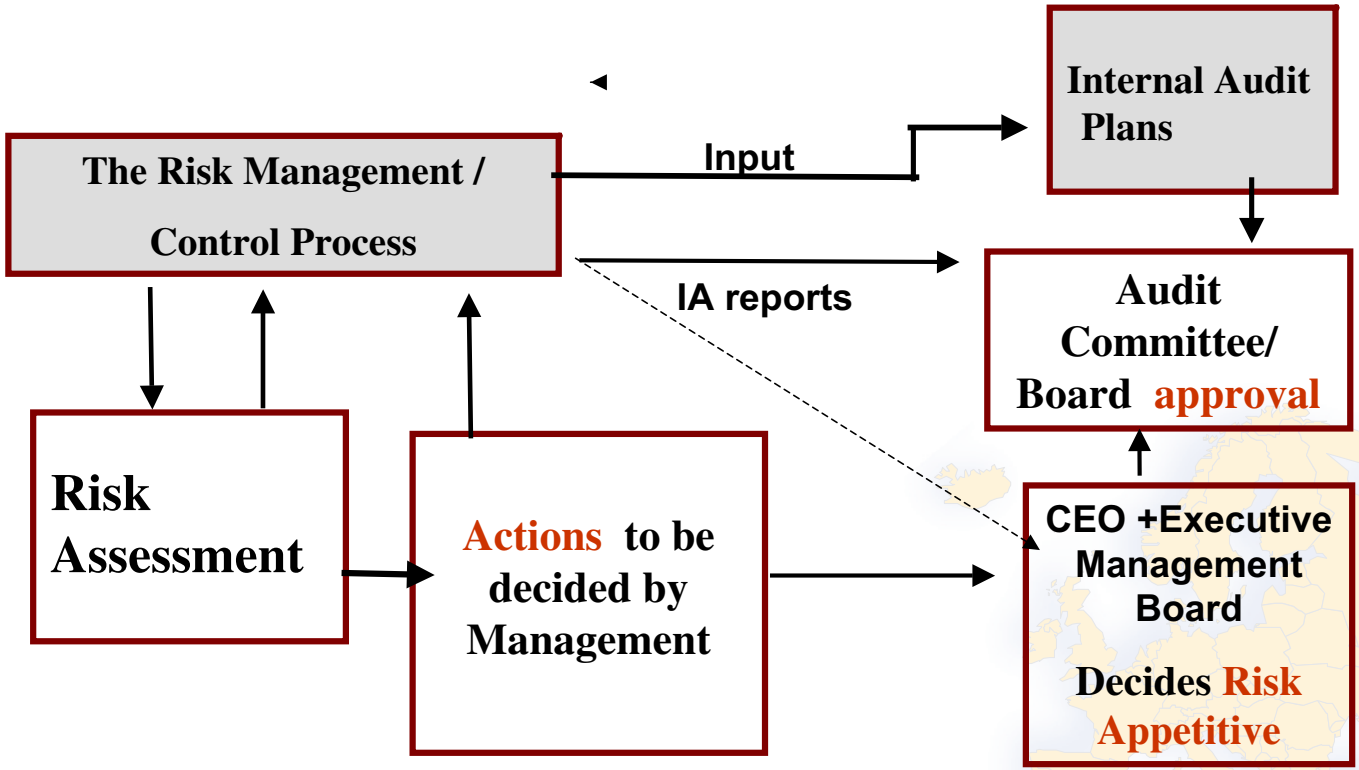
In Accordance with the standards

Internal Audit – strength

Systematic, disciplined approach

- Available tools e.g. COSO-ERM framework
- Used to think – risks
  - when performing plans /scope identification
  - when evaluating the control objectives

Quality of Audit – the only way to success



IA should examine, evaluate, report and recommend improvements (PPF)

Quality of Audit – the only way to success

Training
•Ensure that audit staff receives sufficient training
•Number of staff certified

Use of technology
• Does relevant technology support audit testing and analyses ?

Industry knowledge
•Have the staff sufficient knowledge of the industry, business operations and key functions ?

In accordance with the standards

Innovation & Capabilities
•Training
•Technology
•Industry knowledge

Quality of Audit – the only way to success

In accordance with the standards

Internal stakeholders
- Board/Audit Committee
- Senior Management
- Operating Management

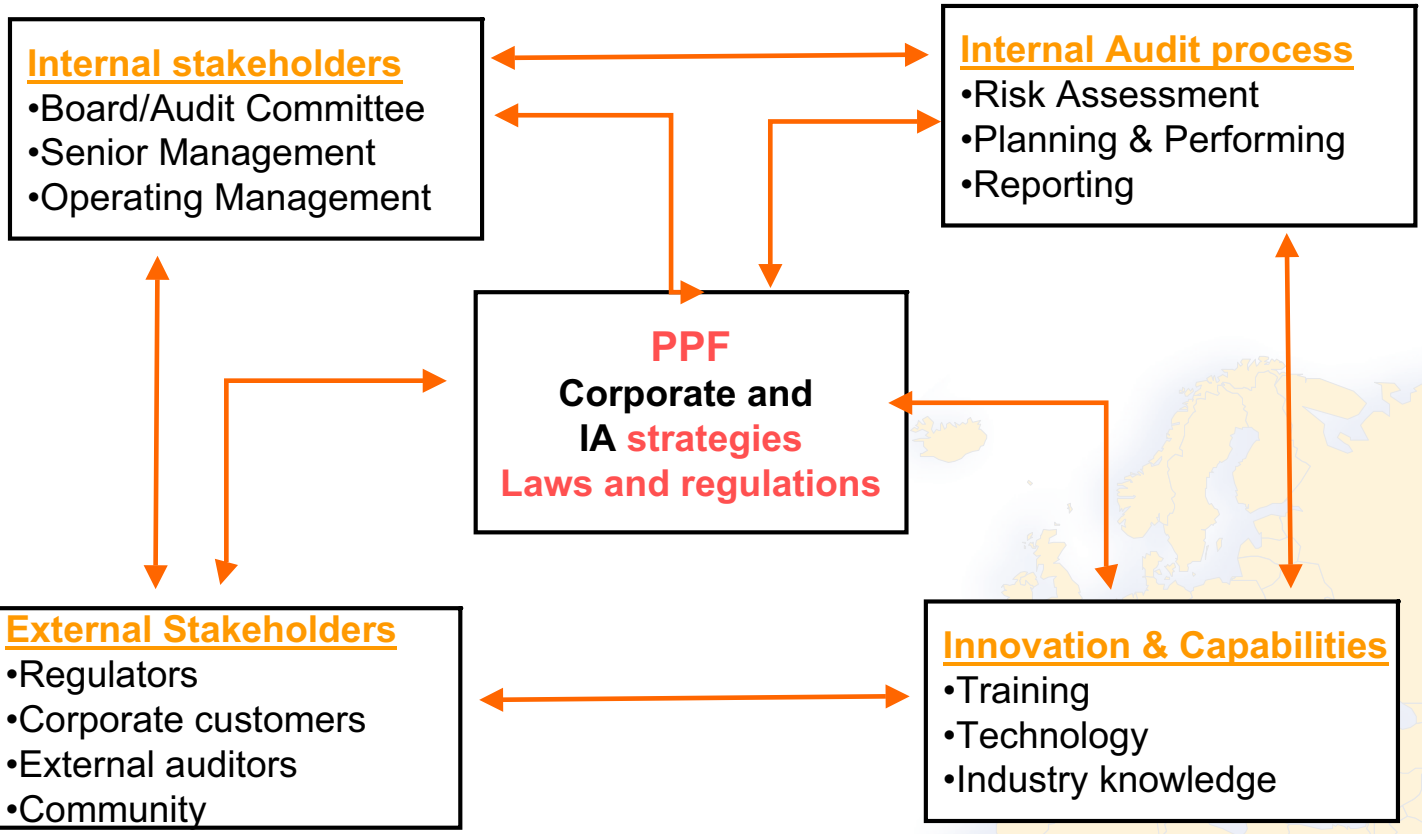
External Stakeholders
- Regulators
- Corporate customers
- External auditors
- Community

To identify all relevant stakeholders and what Service that are important to them

- Assess level of satisfaction
- Identify GAPs

Quality of Audit – the only way to success

In accordance with the standards

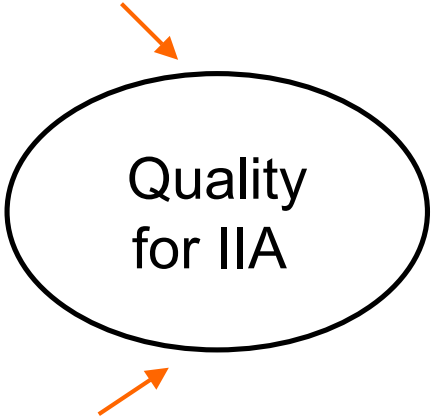


Quality of Audit – the only way to success

Quality of Audit – the only way to success

Quality components

Ensuring your practice is Continuous improvement oriented



Continued professional Development

Identify opportunities and offer ideas for improvements :

- New regulations, laws and common practice
- Contiguous site visits – communicate risks with management
- Use all available networks colleagues, university etc.
- Internal conferences on improvement and efficiency discussions – use knowledge on from new employed staff

Quality of Audit – the only way to success

Quality components

Adherence to the Code of Ethics

Principles for IA (PPF)

- Integrity
- Objectivity
- Confidentiality
- Competence

Quality of Audit – the only way to success

External Quality Assurance process

Preparation work

- Select QA team
- Send out and review the self-study
- Preliminary visit to the organization
- Go through customer and staff surveys

On site visit

- Review of IA activities (incl. improvement actions) and evaluate conformance to standards
- Interview selected members of the board (A.C.) Auditees etc.
- Consider relations to other monitoring functions

Reporting

- Provide a summary of issues and recommendations
- Holding a closing conference with CAE
- Draft report – obtain comments and response to the recommendations
- Follow up conference

Quality of Audit – the only way to success

Communicating the result of the external assessment

In accordance with the standards

Compliance or non compliance with the standard

Recommendations for improvement

To remember – the external assessment requires sound business judgment, integrity and professional care !!!!

Action Plan incl. implementation dates

From CAE

On going and Periodic Internal Assessment

Periodic Assessment

- *IA activity in accordance with its charter*
- *Level of audit effectiveness and efficiency*
- *Does the audit and consultant service add value to the organization*
- *Degree of IA activity's relating to Standards*

Provide recommendations for improvement

Prepare for an external review

On going monitoring of quality assurance

Quality of Audit – the only way to success

Self Assessment with Independent Validation

- Select QA team -
- Send out and review the self-study
- Preliminary visit to the organization
- Go through customer and staff surveys

In-house auditors ***scope adapted to circumstances***

- Review of IA activities (incl. improvement actions) and evaluate conformance to standards
- Interview selected members of the board (A.C.) Auditees etc.
- Consider relations to other monitoring functions

To be coordinated by Independent Validator who has to perform limited tests at least if IA *in accordance with Standards*

- Provide a summary of issues and recommendations
- Holding a closing conference with CAE
- Draft report – obtain comments and response to the recommendations
- Follow up conference

Reporting both by CAE and the Validator *to express if agree or disagree with the self assessment report*

You are good but you have to prove it !

The 2006 European Conference of Internal Audit

Thank You

Quality of Audit – the only way to success

Speaker : Elisabeth Styf (Member of the ECIIA Board)

B-1
The Role of Internal Audit in Corporate Ethics

Svein Andersen (NOR)
Former Head of Corporate Audit
Statoil ASA

The Ethical Challenge: The role of Internal Audit in Corporate Ethics

Svein Andersen, Former Senior Vice President Internal Audit
September 2006

STATOIL

Content

Introduction: The Statoil story

- **Building an organization to promote ethical values**
- **Incorporating ethical values in the organization**
- **Staying competitive while being ethical**

The Statoil story

Statoil was established as an instrument in 1972

- To secure national control of the energy resources
- To become a fully integrated operating oil company
- To develop a strong national support industry

Arm's length to the Minister of Petroleum and Energy

The Statoil story

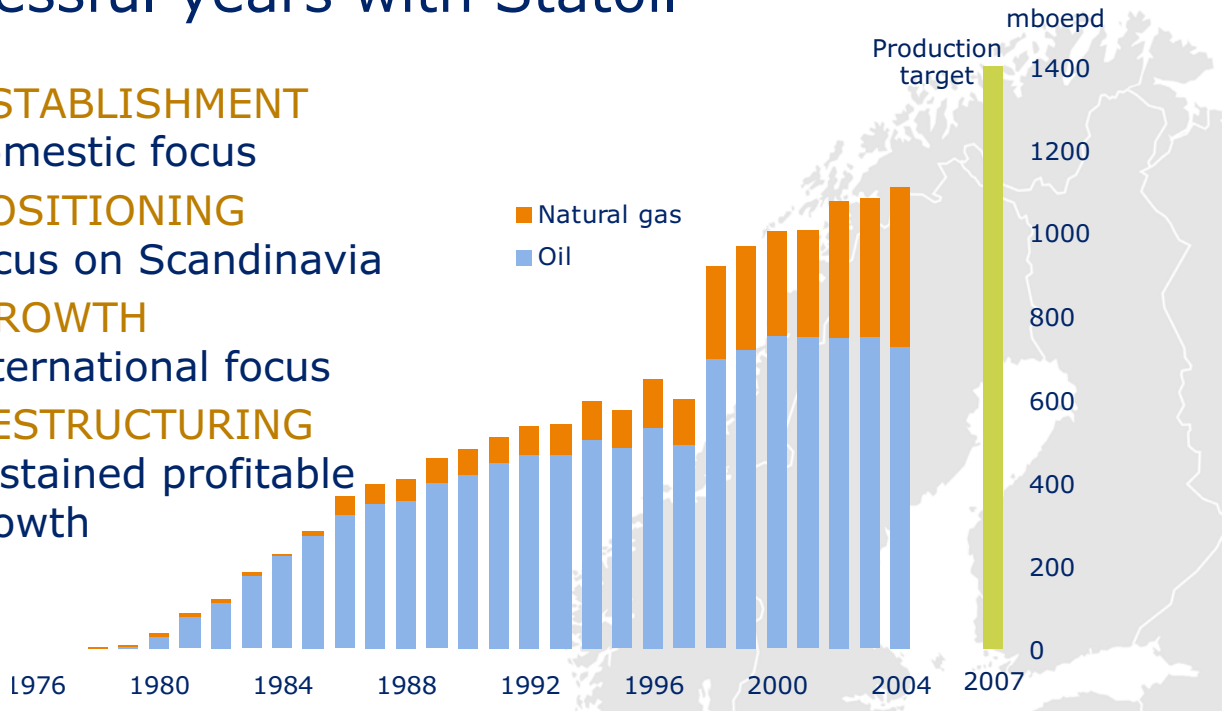
Statoil through changing environments

1972	1985	2001
Statoil established A national project	Gradually increasing Competitive exposure	Profitability and shareholder return
Designing a new industry	A competence company	Focus on performance
Planning & control	Commercialisation	Delivery

The Statoil story

31 successful years with Statoil

- 1970s: ESTABLISHMENT
  - domestic focus
- 1980s: POSITIONING
  - focus on Scandinavia
- 1990s: GROWTH
  - international focus
- 2001-: RESTRUCTURING
  - sustained profitable growth



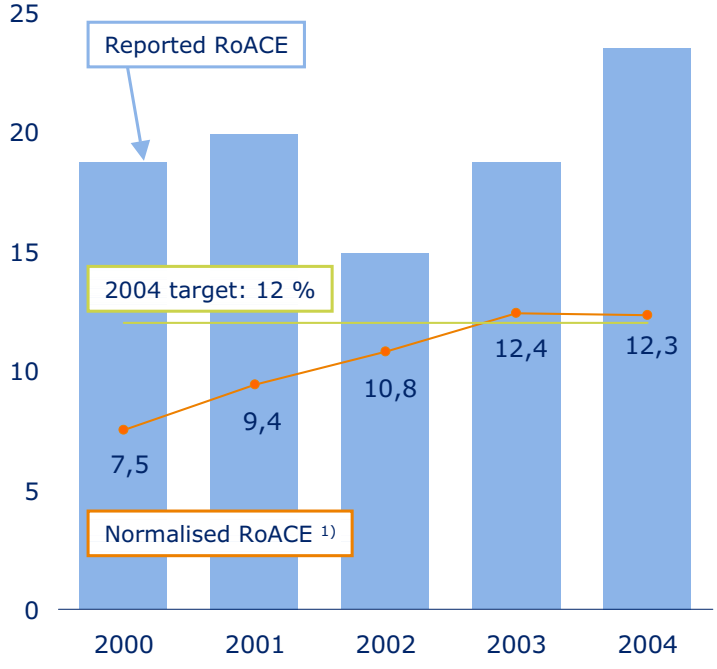
Adapting to changing environments

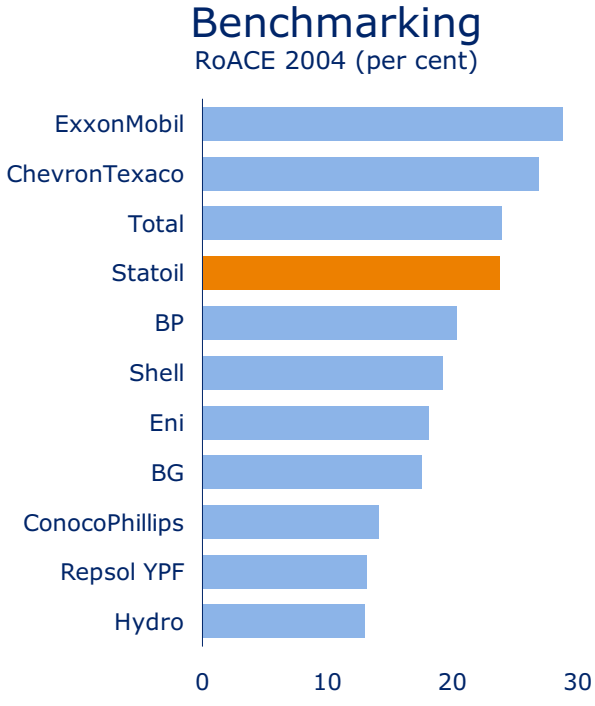
The Statoil story

Operations in 29 countries

The Statoil story

Strong financial performance



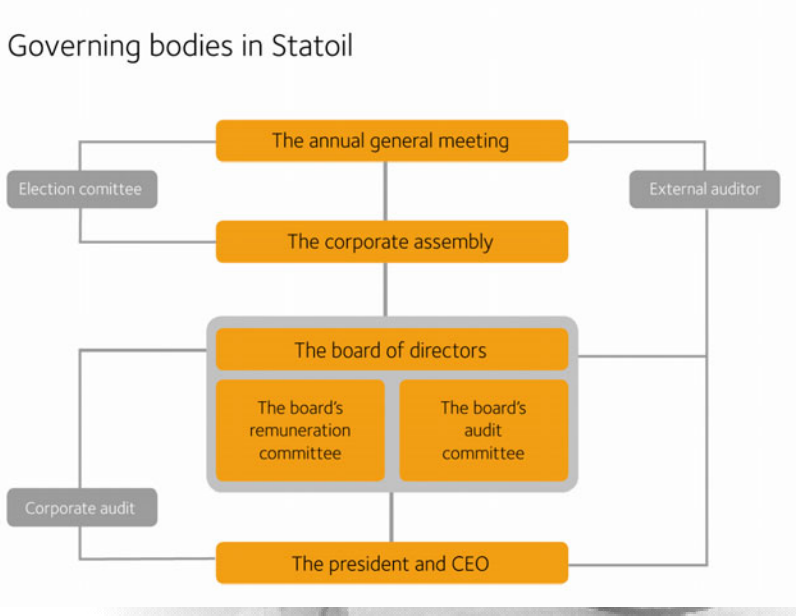


1) Normalised for oil and gas prices, downstream margins and exchange rates.

Building an organization to promote ethical values

Corporate Governance – principles and policies in place

- **The Board of Directors is elected by the Corporate Assembly at the AGM**
- **The Board of Directors are all non-executive**
- **Three employees sit on the Board of Directors**
- **The Ministry is not involved in day-by-day operations and decisions**
- **The CEO is appointed by the Board of Directors**

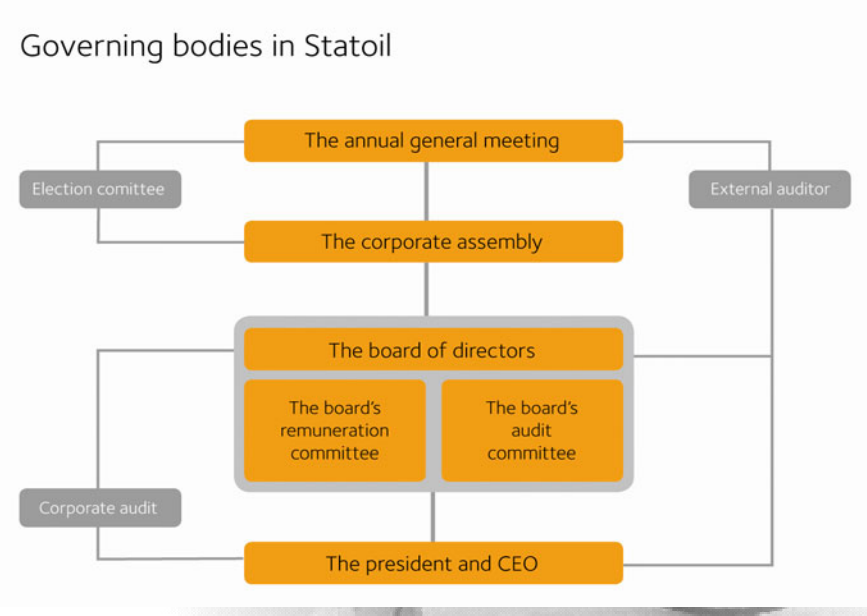


Building value through trust and performance

Building an organization to promote ethical values

The Board's Audit Committee (BAC)

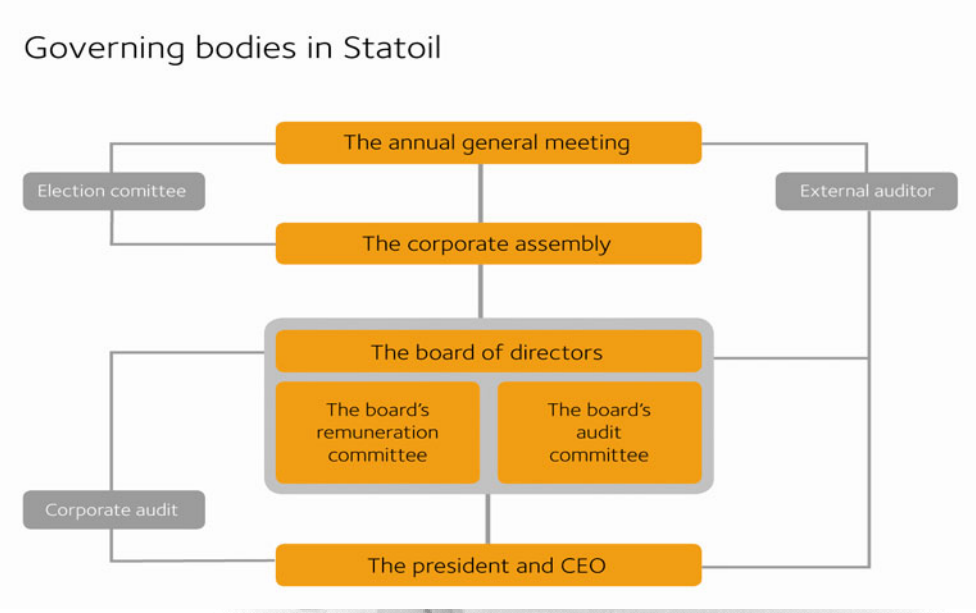
- **The BAC is a sub-committee of the board**
- **The BAC performs a thorough assessment of specific matters**
- **The BAC makes sure that the group has an independent, effective internal and external audit system**
- **The BAC supervises implementation of and compliance with the group's ethical rules**



Building an organization to promote ethical values

The relationship between the BAC and the External Auditor

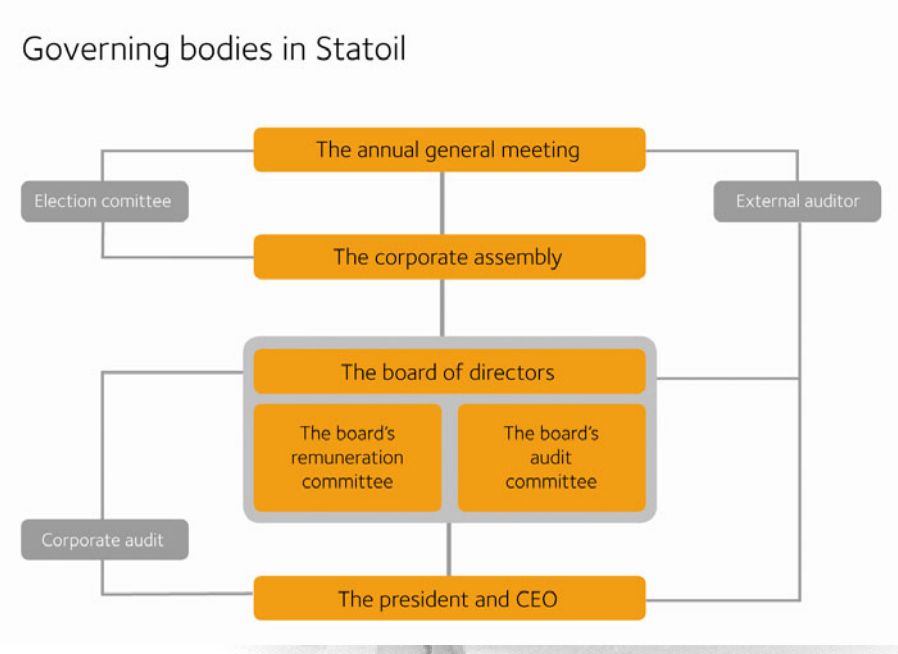
- **The BAC shall**
  - **ensure that the external auditor acts independently**
  - **review the plans and scope of auditing**
  - **review the reports to the board**
  - **hold regular meetings with external auditor**



Building an organization to promote ethical values

The relationship between the BAC and Corporate Audit

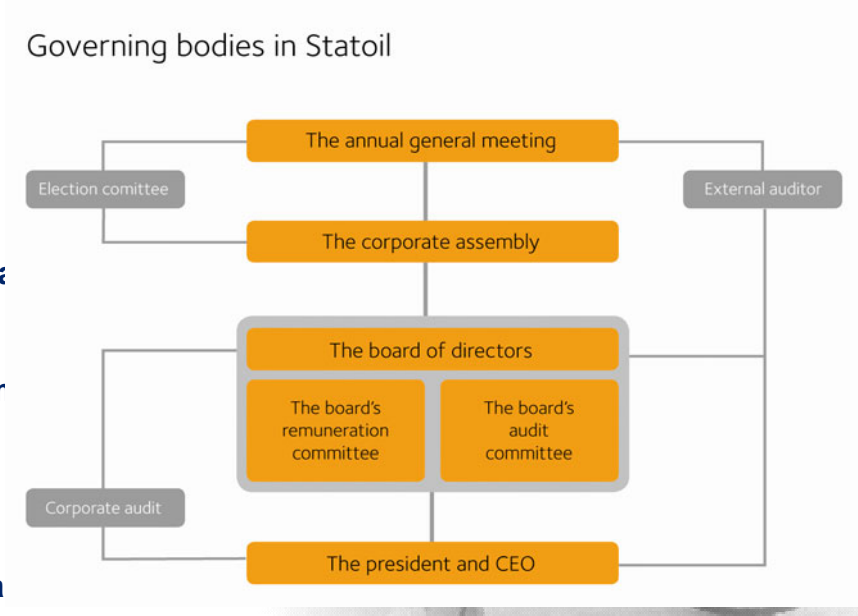
- **The BAC shall**
  - **ensure that Corporate audit acts independently**
  - **review the plans and scope of auditing based on risk assessment**
  - **review the quarterly reports to BAC related to internal control, ethical issues and fraud and important audits and deviation from governing documents**
  - **hold regular meetings with the general auditor**



Building an organization to promote ethical values

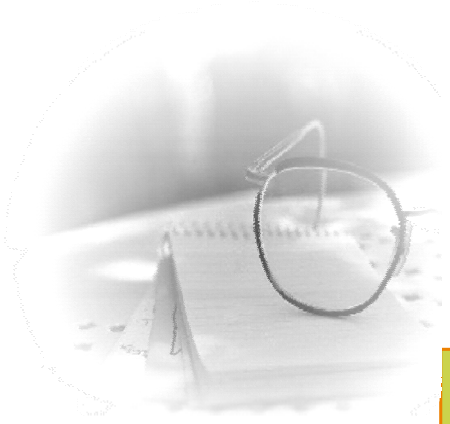
The Board's Audit Committee

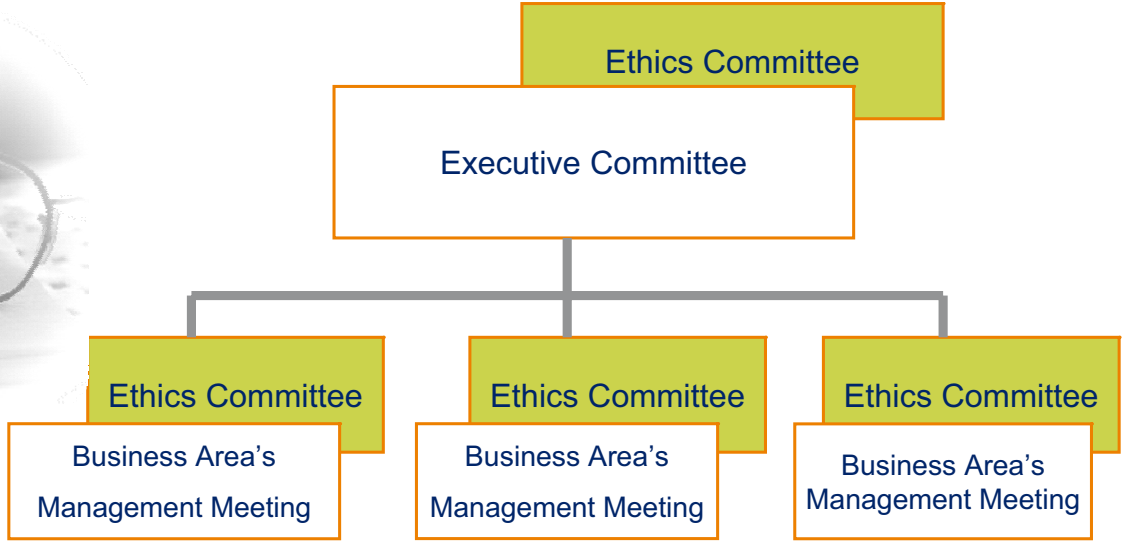
- **Overseeing implementation of and compliance with ethical standards**
- **Review compliance activities related anti-bribery legislation**
- **Overseeing implementation of progra for fraud detection and prevention**
- **Establishing a reporting system from EC's Ethics Committee**
- **At least six meetings per year**
- **Written report from Group Security a Corporate Audit at least quarterly**



Building an organization to promote ethical values

Ethics Committees





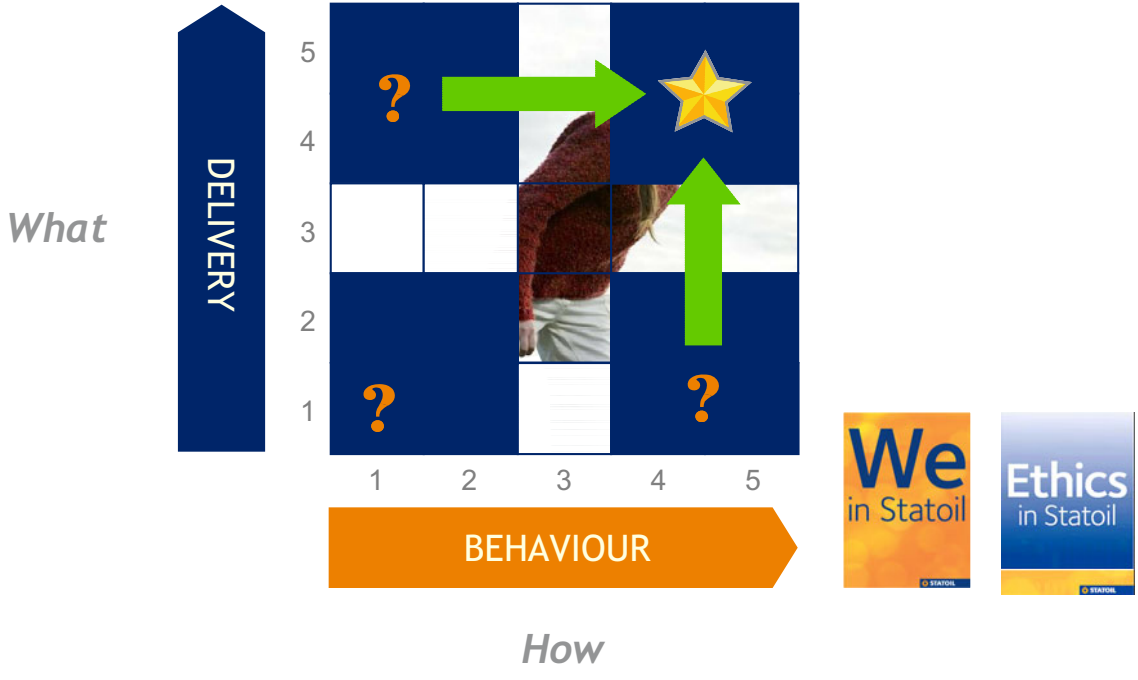
Ethics Committees are set up to ensure:

- **High-level attention to ethics in management groups**
- **Common understanding and practice in regard to ethical and reputational compliance**
- **That Statoil employees live up to the company's ethics guidelines and relevant rules**

Incorporating ethical values in the organization

Incorporating ethical values in the organization

Expectations to delivery and behaviour



Incorporating ethical values in the organization

Clear values and leadership approach




Our values

- Imaginative
- Hands-on
- Professional
- Truthful
- Caring

Our leadership

Our leaders are dedicated, stay close to the business and their people, and:

- Deliver results
- Drive change
- Develop and energise people
- Demonstrate passion for our values

Our leaders are clear about performance standards and individual accountability, and show personal humility




Incorporating ethical values in the organization

Ethics Policy

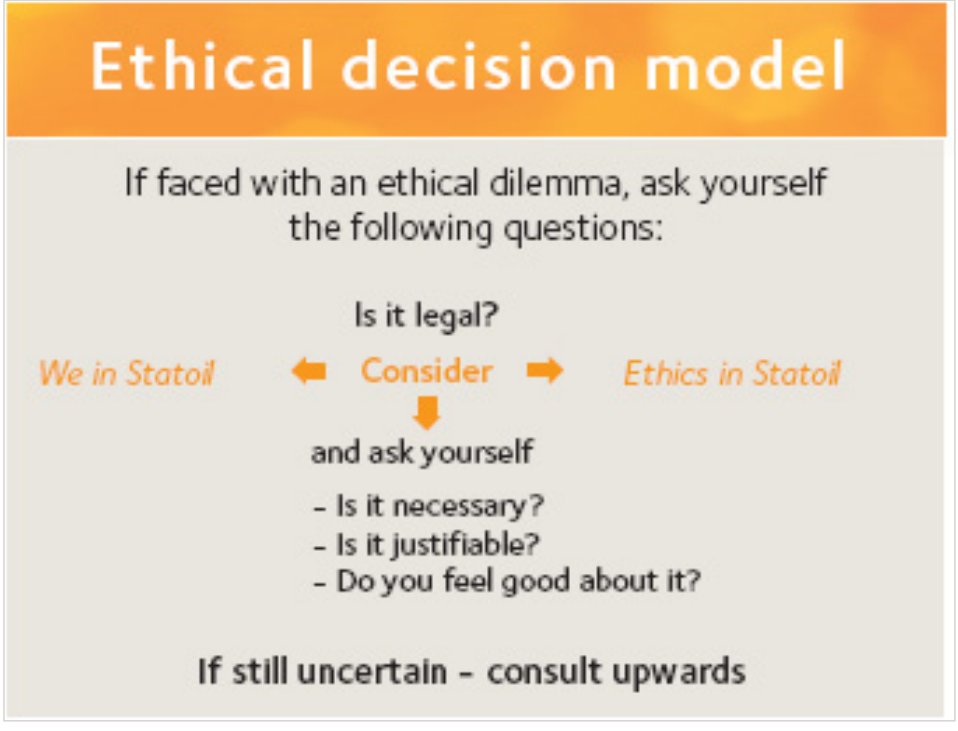
- Statoil's ethics rules and policies apply equally to everyone at Statoil:
  - Employees, board members, independent contractors, consultants, intermediaries, lobbyists and others who act on behalf of Statoil
- Managers are responsible for communicating the ethical guidelines
- Non-compliance with the ethical guidelines must be reported immediately

Incorporating ethical values in the organization

Ethics and Compliance Programs

- Goals
  - Achieve company business goals without violations of law, company values or ethical requirements
  - Provide benefits that outweigh costs
  - Create a culture that values compliance
- Challenge
  - Making ethics codes, training, ethics helpline a central part of everyday business life

Incorporating ethical values in the organization



Incorporating ethical values in the organization

Ethics Helpline

- Available in local languages of all Statoil employees
- Free phonecalls or use of internett
- Individuals may remain anonymous
- No sanctions in any form against individuals who reports in good faith and in a loyal manner

Incorporating ethical values in the organization
Awareness training

- Management training
  - Mandatory participation
  - Legal training and ethics dilemma discussions
- Training for especially exposed employees groups
  - In-depth training for employees in procurement and contract functions
- General awareness training
  - Red-flags awareness related to fraud and corruption




Incorporating ethical values in the organization

Anti-corruption compliance programme

Purpose

- Provides an overview of Statoil's efforts to combat corruption
- Enables the employees to identify and manage the operational risk that corruption and bribery pose to Statoil
- The document provides a brief overview of the main US and Norwegian anti-corruption legislation

Content

- *Ethics in Statoil*
- Legal framework – Norway and US
- Compliance coordinator network
- Risk analysis
- Contact with public officials
- Training
- Procurement procedures
- Integrity due diligence

Incorporating ethical values in the organization

Compliance coordinators

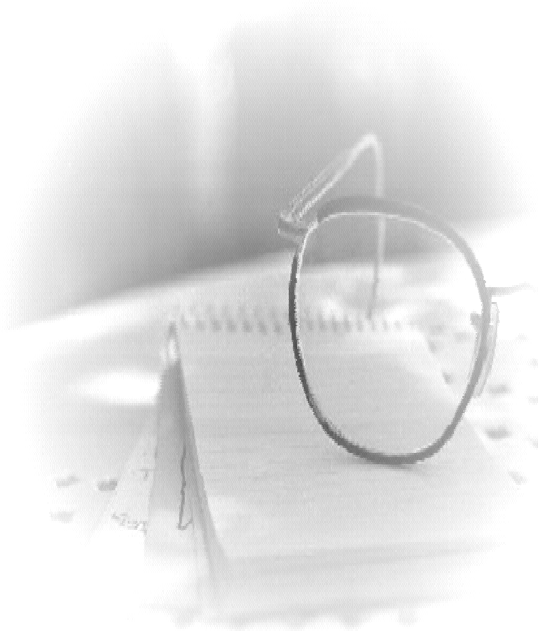
Responsibilities
• Follow-up on implementation of anti-corruption compliance programme • Ensure that necessary guidelines are established • Perform assessment of corruption risks • Coordinate anti-corruption training programmes • Report any violation of regulations to corporate compliance officer • Participate in the ethics committees • Keep up-to-date regarding investigations into alleged violations and corrective measures

Staying competitive while being ethical

- Tone at the top: Take a clear stand against unethical behaviour
  - Establish a good margin against behaviour which could be illegal or a breach of the ethical guidelines
  - Communicate the attitude with relevant authorities
- Openness
  - A culture with open discussions can prevent unethical behaviour
  - Sharing experiences with others
- Discussability
  - Anyone in any kind of doubt should talk to their colleagues and raise the matter with their superior
  - Sufficient time must be devoted to difficult decisions

Staying competitive while being ethical

- The future role of Corporate Audit
  - Evaluation of the effectiveness of the communications of expected ethical attitudes
  - Support the design of ethical awareness and training programs
  - Evaluate the formal and informal processes that could potentially undermine the ethical culture
  - Evaluate the state of the ethical climate in the organization



Rules to live by

Make sure your actions are comfortably within the law and our own ethical guidelines

Be open with regard to ethical issues

Spend sufficient time on difficult decisions

President and CEO Helge Lund

B-2
Whistleblower Procedures Best Practices

Thijs Smit (NED)
Director Internal Audit
SNS Reaal Group

Whistleblowing

Thijs Smit

Helsinki, September , 2006

Overview presentation

- Introduction
- What?
- Why?
- How?
- Conclusions

- Thijs Smit
- 28 years Internal Audit
- 15 years Chief Auditor several companies
- 8 years Boardmember IIA Netherlands
- 3 years President IIA Netherlands
- 3 years member PIC IIA Inc.

- IIA research
- CFE Recommendations
- External providers information
- Sarbanes Oxley Act
- Own experiences

Mechanism that enables employees and other stakeholders to report (financial) irregularities, concerns and other (workplace) issues and stay anonymous, whitout retaliation

- Technology
- Staff
- Procedures
- Communication

- Commitment company to integrity
- Provide additional way to raise concerns
- Effective internal control (monitor trends)
- Prevent surprises
- Comply with the law

SOX

- Title III section 301.4 complaints
- Title VIII section 806 protection
- Title XI section 1106 enforcement

- Technology
- Staff
- Procedure
- Communication

- Web form
- Messages service
- Complaints box
- Phone line

- Phone line
- Two way communication
- 24 hours 365 days
- Toll free
- One line for all issues
- Native language
- Possibility to stay anonymous

- Internal vs. external
- Skilled interviewer
- 24 hours 365 days

- Outside provider
- The network
  - 30% Fortune 500
  - GAP, SEARS, Home Depot
- Global Compliance Services
  - Starbucks, Tiffany

- Selection providers
- Develop shortlist
- Due diligence provider

- Call intake
- Multi-lingual interviewer (translators)
- Trained interviewers
- Technology used
- Customized complaint categories

- Automated escalation
- Automated reporting
- Link case management
- Customers
- Fee

- Receipt complaints
- Retention complaints
- Treatment complaints
- Anonymous submission
- Reporting

Receipt complaints

- Other channels than hotline
- More than financial irregularaties
- Actionable case
- Unique number case

Case management

- Unique number
- Provider and gatekeeper
- Gatekeeper and casemanagers

First treatment tip

- High risk situation
- Pre-determined list key staff
- Time sensitive situations

Dealing with the tip

- Depends on nature
- Depends on information available
- Never disclose tip

Reporting

- Database
- Status complaints
- Treatment tips
- Management reports
- Discovery trends

- Launch the program
- Keep hotline “Top of the mind”
- Effective communication is crucial

Launch the program

- Video executive management
- Posters
- Letter
- Wallet card
- Training

Keep it alive

- Procedures new employees
- Planning communication each year
- New campaign
- Keep reminding on annual basis

Intro | What | Why | How | Conclusions

- Lot of work
- Underestimated
- Effective control
- Monitor trends

Questions?

B-3
The Role of Internal Audit in Safeguarding Corporate Reputation

Mauro Di Gennaro (ITA)
Chief Audit Executive & Compliance Officer
FIAT SpA

FIAT GROUP

The Role of Internal Audit in Safeguarding Corporate Reputation

Mauro Di Gennaro (ITA), Chief Audit Executive & Compliance Officer,

FIAT SpA

Agenda

- FIAT GROUP OVERVIEW
- WHAT DOES INTERNAL REALLY MEAN?
- WHAT CAN INTERNAL AUDIT DO?
- INTERNAL AUDIT IN THE FIAT GROUP
- FIAT GROUP INTERNAL AUDIT FOR CORPORATE GOVERNANCE

FIAT GROUP OVERVIEW

(06/30/2006)
- Consolidated revenues € **26.2 B**
- Total Assets € **62.3 B**
- Employees **173,396**

Listed on the **NYSE** and the **Borsa Italiana** (Italian Stock Exchange)

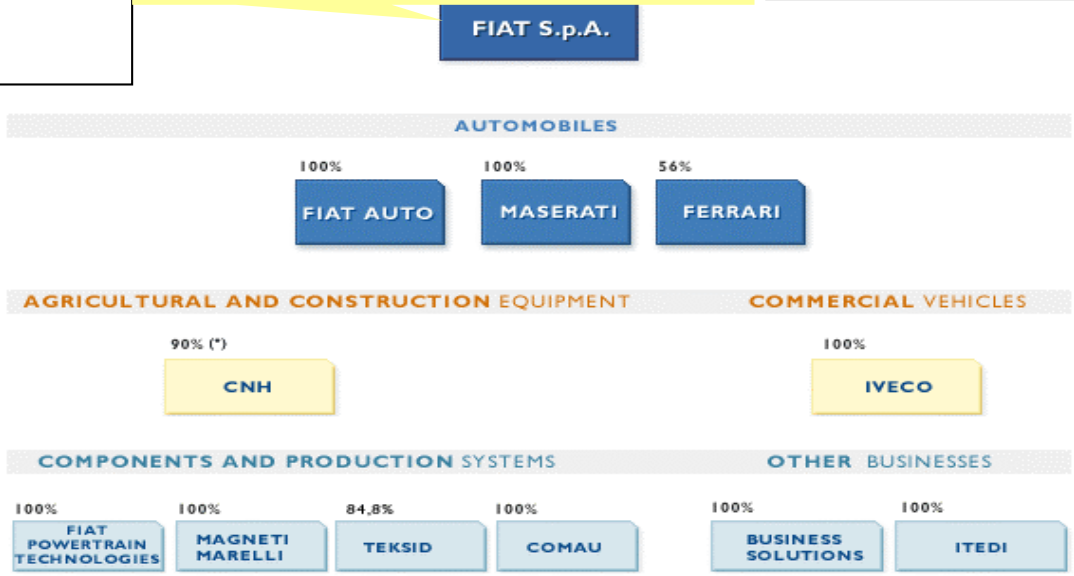
- Number of Companies **654** (*12/31/2005*)

- Sectors:

Cars, **F**errari, **M**aserati

Agricultural and construction equipment, **C**ommercial vehicles

Fiat Powertrain Technologies, **C**omponents, **M**etal components, **M**eans & production systems **S**ervices, **P**ublishing



http://www.fiatgroup.com

Corporate Service activities:

Fiat Revi Scrl provides activities and services to support the accounting systems, the applications of Internal control systems and procedures and to verify their goodness.

WHAT DOES **INTERNAL** REALLY MEAN?

- He is considered to be one of the persons responsible for a good or (bad) Corporate Governance. Following a corporate scandal one is likely to hear the usual question, "**where were the internal auditors**?"
- The Internal Auditor **plays an important role** in safeguarding the corporate reputation for at least two kinds of reason:
  - He contributes to built the corporate reputation **inside** the company:
    - To be a point of reference for the Stakeholders;
    - To support the Board of Directors with the right information;
    - To support Management in implementing their responsibilities referred to risk management, control and governance processes using a systematic and disciplined approach.

WHAT DOES **INTERNAL** REALLY MEAN?

= An effective function of Internal Audit must respect some premises:

- The **Chief Audit Executive** should **report** to a level within the organization that allows the Internal Audit activity to fulfill its responsibilities.
- The **purpose**, **authority**, and **responsibility** of the **Internal Audit activity** should be formally defined in a charter and approved by the board.
- A **risk-based audit plan** to determine the priorities of Internal Audit activities integrated with management evaluation should be reviewed and approved by the Audit Committee.

WHAT DOES **INTERNAL** REALLY MEAN?

- Audit activities should be in **compliance** with **International Standards**, **Best Practices** and **local requirements**.
- Internal Auditing **skills** and **competencies** should be **consistent** with Internal Audit's **responsibilities**.
- A "**Quality assurance Program**" should be implemented in order to provide assurance to all stakeholders as to the quality of the activity and value added to improve the organization within the ambit of Corporate Governance.

WHAT CAN INTERNAL AUDIT DO ?

= **Perform** assessments to provide assurance that governance structures and processes are properly designed and are operating effectively.

= **Provide** advice on potential improvements to the governance structure and processes.

= **Act** as catalysts for change.

WHAT CAN INTERNAL AUDIT DO?

FIAT GROUP

= Perform specific activities related to Corporate Governance processes, in which Internal Audit could be involved in:

- Auditing the design and implementation of the key elements of a sound Corporate Governance Program.
- Supporting the Management in the Risk Management process and strategies and review the results.
- Ethics Policies and Code of Conduct (appropriatenes, communication and acceptance).
- Supporting Management in the Corporate Compliance Program definition.
- Fraud prevention/detection.
- The Sustainability process.

WHAT CAN INTERNAL AUDIT DO?

- Audit the design and implementation of the key elements of a sound Corporate Governance Program:
  - Needs identified: - legal, regulatory, ethics business and technical.
  - Risks identified: - strategic operational financial performance market/ business environment.
  - Control objectives established and communicated to address risks.
  - Performance measurements implemented to ensure the organization is practicing sound governance.

WHAT CAN INTERNAL AUDIT DO?

- Support the Management in the Risk Management process and strategies and review the results:
  - Risk management processes should be implemented at a board level and throughout the organization.
  - Different types of risk should be identified.
  - Adequate strategies should be established to address key risks.
  - Although many elements of the governance are generally driven from the top, a top down review should ensure that designed processes are adequate and embedded effectively throughout the organization.

WHAT CAN INTERNAL AUDIT DO?

- Ethics Policies and Code of Conduct (appropriateness, communication and acceptance).
  - Ethics policies and Codes of Conducts are used by the organizations to govern acceptable employee behaviour and represent a key part of the organization's governance structure. Internal Auditor can asses weather the organization's policies and codes include appropriate subjects and guidance.
  - To be effective ethics policies and codes of conducts need to be communicated clearly to, and understood and accepted by , employees.
  - IA can asses whether the communication is occurring and whether the information is understood.

WHAT CAN INTERNAL AUDIT DO?

- Support the Management in the Corporate Compliance Program definition to ensure compliance with all laws, rules, regulation and policies to which the company is subject:
  - workplace discrimination/harassment/respect,
  - anti trust,
  - conflict of interest (Legislative Decree no. 231/2001, white-collar crimes),
  - document management and confidentiality,
  - customer privacy, product liability,
  - intellectual property and company asset protection,
  - Sarbanes - Oxley Act and other national laws,
  - insider trading restrictions, environmental, health and safety regulations,
  - financial integrity,
  - whistleblower/misconduct reporting.

CORPORATE GOVERNANCE PROCESSES IN THE FIAT GROUP

GUIDELINES FOR THE INTERNAL CONTROL SYSTEM IN FIAT GROUP

- The **Internal Control System** is an **essential element** of the Corporate Governance System of Fiat S.p.A. and of its subsidiaries and **plays a key role** in identifying, minimizing and managing risks that are significant for the Fiat Group, contributing to the **safeguarding of stockholders' investments** and the **Company's assets**.

- The **responsibilities** on Internal Control System are allocated to:
  - Board of Directors
  - Audit Committee
  - Executive Directors
  - Internal Control Compliance Officer
  - Internal Audit Function
  - All employees

FIAT CORPORATE GOVERNANCE STRATEGIES

= The Fiat Group adopted and abides by the Corporate Governance Code of Italian listed companies, which is mentioned as a model in the regulations issued by Borsa Italiana (Italian Stock Exchange) on Corporate Governance.

Corporate Governance

- **Members of the Board of Directors, of the Board of Statutory Auditors, and of the Committees established by the Board of Directors** *(14,9 Kb)*
- **Annual Report on Corporate Governance (March 2006)** *(84,9 Kb)*

Annexes to the Annual Report on Corporate Governance

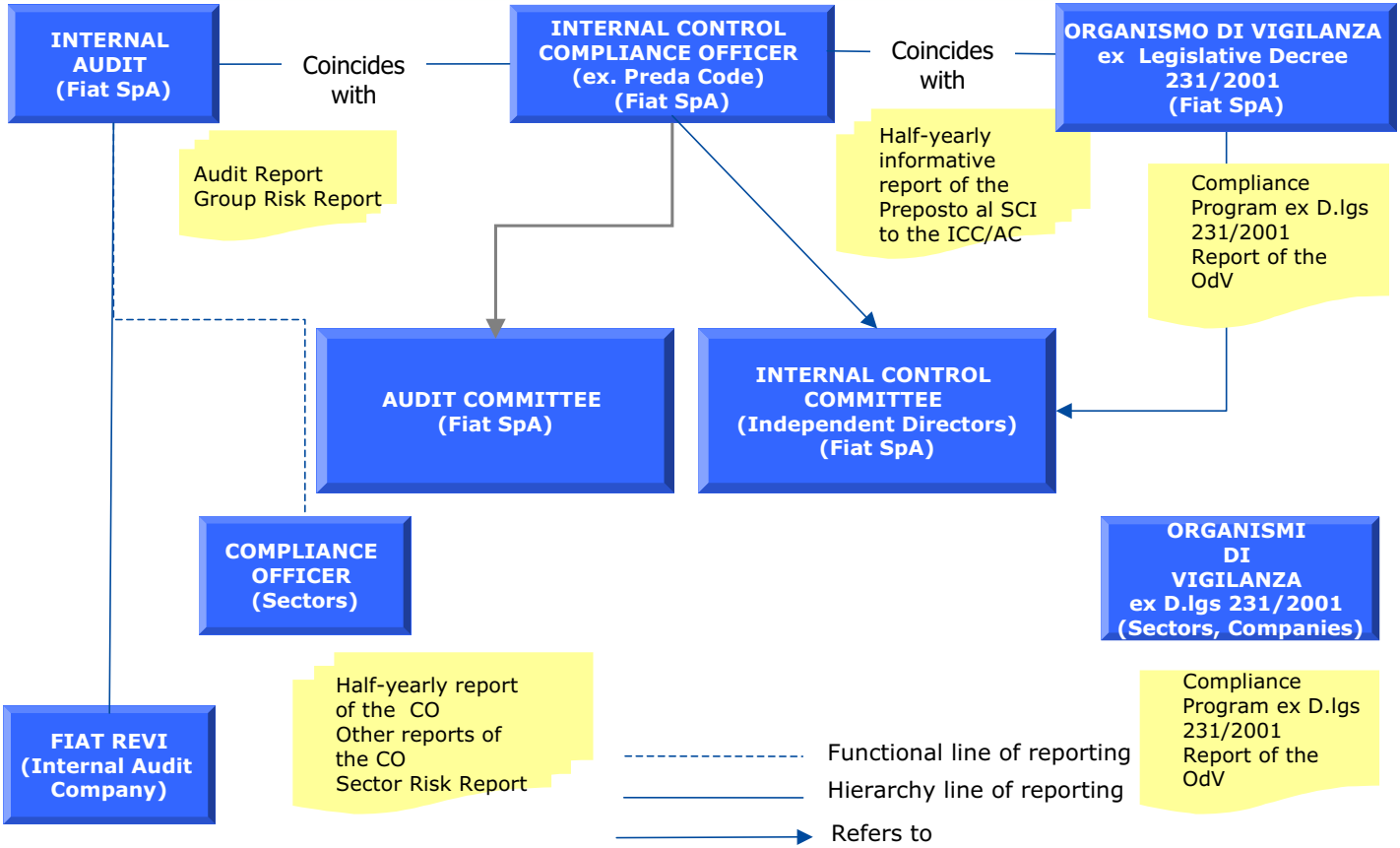
- 1 - Fiat Group Code of Conduct *(72,1 Kb)*
- 2 - Excerpt from the Compliance Program pursuant to Legislative Decree no. 231/2001 *(115,8 Kb)*
- 3 - Guidelines for the Internal Control System *(39,8 Kb)*
- 4 - Procedure for the Engagement of Auditing Firms *(41,7 Kb)*
- 5 - Whistleblowings Management *(64,2 Kb)*
- 6 - Charter of the Internal Control Committee *(29,7 Kb)*
- 7 - Charter of the Nominating and Compensation Committee *(28,6 Kb)*
- 8 - Guidelines for Significant Transactions and Transactions with Related Parties *(40,9 Kb)*
- 9 - Internal Dealing Regulation (in force until March 31, 2006) *(37,6 Kb)*
- 10 - Fiat S.p.A. Articles of Association *(51,9 Kb)*
- 11 - Regulations for Stockholders Meetings *(34,0 Kb)*
- **List of Relevant Persons (Internal Dealing)** *(18,8 Kb)*

→ **Italian Corporate Governance Requirement**

→ **Italian law further to OCSE Convention on combating bribery of foreign public officials in international business transactions**

http://www.fiatgroup.com

FIAT GROUP – INTERNAL CONTROL SYSTEM



CORPORATE GOVERNANCE - FIAT INTERNAL AUDIT

= In regard to the Corporate Governance Process, **Fiat Internal Audit** is involved in the following **activities**:

- Design and implementation of key elements of Corporate Governance Process.
- Enterprise Risk Management (ERM).
- Ethics Policies (Code of Conduct).
- Corporate Compliance Program:
  - Whistelblowing.
  - Sarbanes Oxley Act.
  - The Legislative Decree no. 231/2001.
  - Anti Fraud Program.
- Sustainability Report.

- The Internal Audit function is involved in the analysis of key elements of Corporate Governance, as stated in its responsibilities.
  - Internal Audit is **responsible** for:
    - Operating in compliance with set objectives.
    - Assisting the Group in maintaining the validity of the Internal Control System through assessment of its effectiveness and efficiency and by promoting continuous improvement.
    - Assisting the Group in identifying and assessing the greatest exposure to risk and contribute to improvements in the risk identification, reduction and management systems.
    - Implementing specifically planned oversight activities to verify any weaknesses of the Internal Control System and identify any failings and the need for improvement of the internal control processes.
    - Verifying that the rules and procedures constituting the terms of reference of the control processes are actually applied and that all those involved.

CORPORATE GOVERNANCE - *Enterprise Risk Management*

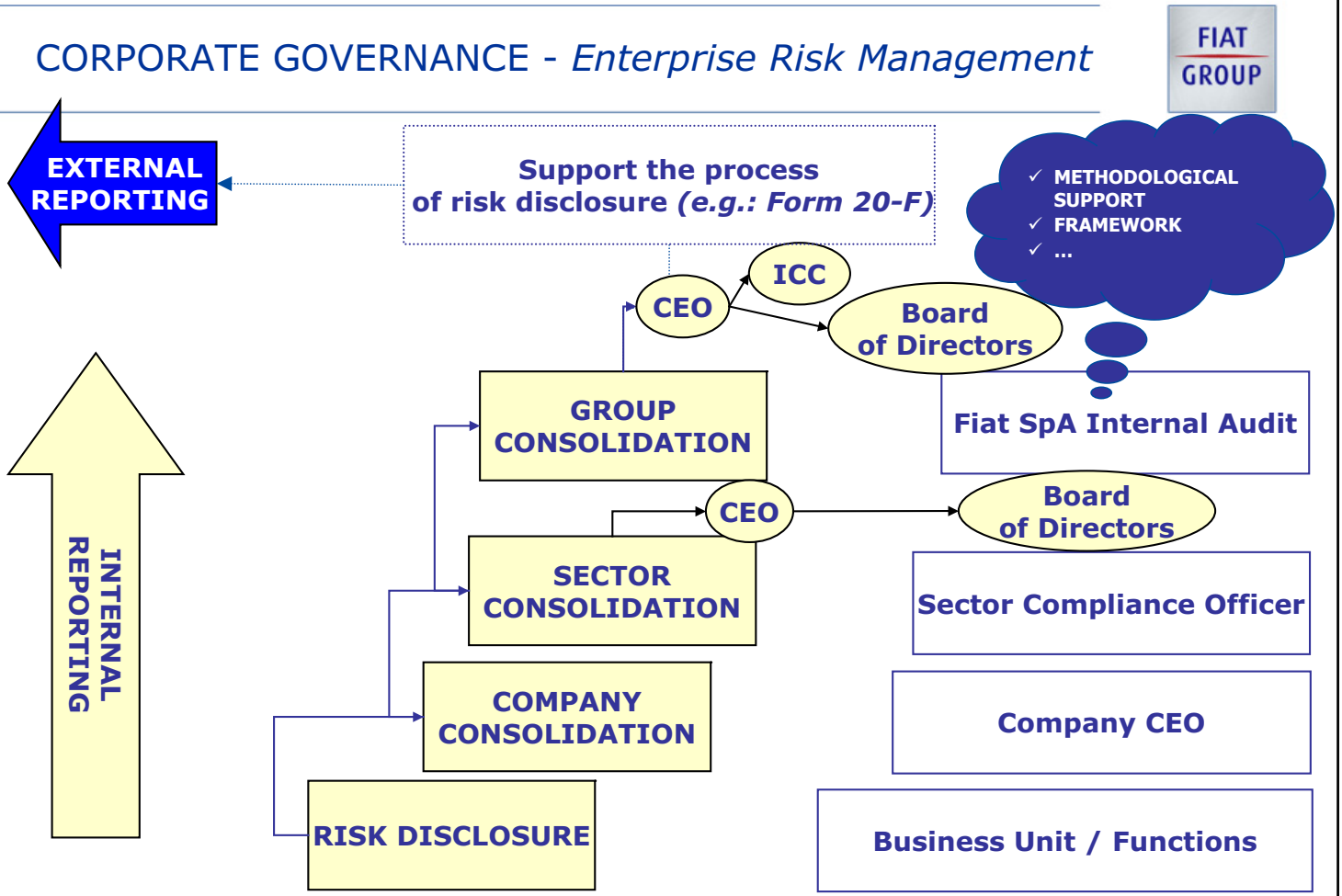
= Implementation of Guidelines for Internal Control Systems to manage risks, as stated in the **Fiat SpA Announcement**:

- *The significant (critical) risks for the Company and for the Group are submitted to the CEO and to the board of directors for analysis.*
- *Senior Management sends a bi-yearly report to the CEO and to the Head of Internal Audit, which contains: significant Risks; Corrective measure to prevent, reduce and manage risks.*

*… the Head of Internal Audit prepares the "**Group Risk Report**" for the CEO*

= The duty of the individual Sector **Compliance Officer** are to: Support and assist management in identifying and assessing the Sector's main areas of exposure to risk (e.g., operational, financial, contractual, information security, or other risks), and to contribute to improving the risk management systems.

CORPORATE GOVERNANCE - *Enterprise Risk Management*



CORPORATE GOVERNANCE - *Enterprise Risk Management*

FIAT GROUP

= In the Fiat Group, there is an **ERM process** which operates with the aim of **identifying** the **principal risks** faced by the company with regard to the effectiveness and efficiency of its operations, the reliability of financial reporting, the compliance with laws and regulations and the safeguarding of company assets.

EXAMPLE OF FIAT RISK MODEL

NATURE	PROCESS	CLUSTER	RISK DRIVER	EVALUATION ELEMENTS
STRATEGIC	**SALES**	**MARKET**	**Competition**	Major changes related to competitors, which consequently threaten the company's margins and profitability. Systematic benchmarking of competitors
			Changes in customers' expectations/needs and changes in demand	Changes in customer expectations and/or in demand not perceived by the company and/or not translated into products, which consequently reduce sales and related revenues
			Product offering (price, discount, promotion)	Factors to be considered in defining product offering: price competitiveness, margin to be achieved, discounts level, effectiveness of targeted promotions, etc…
			Clients dynamics*	Dependence on major customers (including dealers) towards which the company has either contractual weaknesses or the customers are in difficult business/financial situation and they are difficult to replace. Credit exposure management (credit line, client rating, supply restrictions, guarantees / hedging mechanism)

* includes identification of potential risks related to fraud

CORPORATE GOVERNANCE - *Code of Conduct*

- **Internal Audit** has been involved in the **definition** of the Code of Conduct (responsibility of Human Resources, Legal Affair, Communication).
- The **diffusion** of the Code of Conduct within the company is the responsibility of **Human Resources**.
- **Internal Audit** verifies the **application** of the Code of Conduct through:
  - Business Ethics Audit.
  - Fraud Audit.
  - Investigations following signaling of violations of the Code.
- In Fiat, **Internal Audit** has contributed to the definition of the Whistleblowing Management Procedure, concerning **violations** of the Code of Conduct.

CORPORATE COMPLIANCE PROGRAM - *Whistleblowing Management Procedure by Internal Audit*

FIAT GROUP

PROCESSES

HIGHLIGHTS OF THE PROCEDURE

- **responsibilities** of the Internal Control Compliance Officer, the Sector Compliance Officers, the Whistleblowing Committee
- **information** for the Board of Auditors and the Internal Control Committee and for the Internal Control Compliance Officer/the Sector Compliance Officers for whistleblowings received by the CEOs and Management
- **safeguarding the anonymity** of whistleblowers in good faith, to protect them from any form of reprisal, discrimination or penalization
- **disciplinary System** which ensures the effectiveness of the Program, by establishing rules to punish all intentional misbehaviour by Employees, Directors, CEOs, members of the Board of Auditors, according to statutory regulations
- Implementation and **dissemination to employees** and third parties

☞ The document is available on the Fiat Group web site http://www.fiatgroup.com

CORPORATE COMPLIANCE PROGRAM –
Sarbanes – Oxley Act

= **Section 302**:
- Documentation of Fiat Group disclosure controls and procedures
- Creation a Disclosure Committee
- Definition of cascade certification process

= **Section 404**:
- A Management Assessment Process, based upon a reporting process and a "cascade" certification will be based on the following principles:

- **Each Sector** is individually **responsible** for its own ICFR (according to the general principles defined at Corporate level).
- **Each Sector** (by the CEO/CFO) will ensure its own **compliance** to SOX section 404.
- The "**cascade**" process shall involve Service Providers. The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting.
- Internal Audit is requested to provide a **positive assurance** over ICFR

- Introduced the concept of various criminal liabilities of legal entities and related monetary sanction.
- Sanctions of civil nature but with "criminal-like" consequences because of their high impact.
- The company is liable for crimes committed by high level senior officers if the result of their crimes is a company profits.

- The criminal offence categories are:
  - Criminal offences committed against the **Public Administration**.
  - Criminal offences relating to **forgery of currency**, **credit cards** and **duty stamps**.
  - **Social crimes** (e.g. false social communications).
  - Offences relating to **terrorism** and the **subversion of democratic order** (including the financing thereof).
  - Offences relating to **prostitution** and **child pornography**, as well as the **trade of people** and their **enslavement**.
- The **sanctions** are:
  - Monetary sanctions.
  - Confiscation of profits.
  - Publication of judgment.
  - Disqualifications and injunctions envisaged.

COMPANY EXONERATION FROM LIABILITY

= The law requires:

- The implementation of "**Compliance Programs**" (Modello di Organizzazione Gestione e Controllo) to prevent the committing of criminal offences and to exonerate the Company from liability.
- The appointment of the "**Organismo di Vigilanza**" with the duty of monitoring the Compliance Programs.
- In Fiat Group, that the "Organismo di Vigilanza" agrees with the CAE and manages two lines of **report**:
  - The first line is on a continuous basis directly to the Chief Executive Officer.
  - The second line consists of reports submitted on at least a semi-annual basis to the Audit Committee and the Board of Statutory Auditors.

FRAMEWORK

= The Program integrates the following, already existing, instruments:

- Corporate Governance Group principles.
- Internal Dealing Regulation and Relevant Persons.
- Guidelines for significant transactions and transactions with related parties.
- Internal rules concerning administrative, accounting, financial, reporting system of the Group.
- Code of Conduct.
- Internal Control System (policy, procedures, rules, organization, etc).
- Disciplinary system for employees (CCNL).

- Internal Audit is generally involved in the design phase of the process of Corporate Social responsibility. In order not to prejudice its objectivity, such involvement should ensure **only** a **methodological support**.

- The duties of Internal Audit include **also** the **verification** of Corporate Social responsibility.

- Internal Audit should **not be involved in** the implementation of a Corporate Social Responsibility process which involves **managerial responsibility**.

CONCLUSIONS

- More awareness by management about the responsability of the internal control system, governance processes and risk management....

- … new Internal Audit role (changing mindsets and skills).

- and future developments as to the role of the function within the ambit of the Corporate Governance processes:
  - Board structure, objectives and dynamics.
  - Board committee functions.
  - Management evaluation and compensation.
  - Recruitment processes for senior management and board members.

B-4
Valuating Sustainability Behaviour

Susanne Stormer (DEN)
Director, Accountability and TBL Leadership
Novo Nordisk A/S

Valuating Sustainability Behaviour

Susanne Stormer
Director, Accountability and TBL Leadership

ECIIA, Helsinki
7 September 2006

novo nordisk®

Key points

1. **Accountability**
   – buzz or biz?
2. **Sustainability**
   – a different approach
3. **Navigability**
   – staying the course
4. **Profitability**
   – the value of values

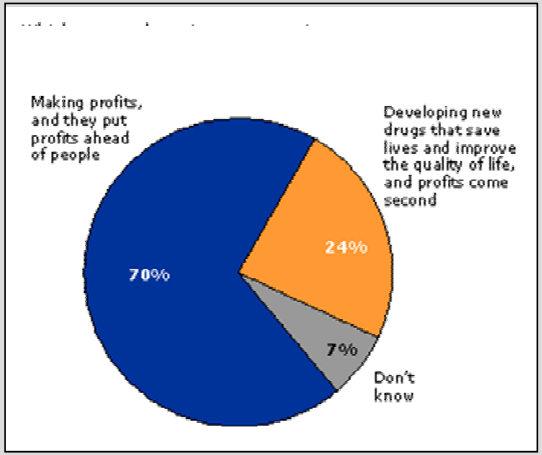
1

Accountability – buzz or biz?

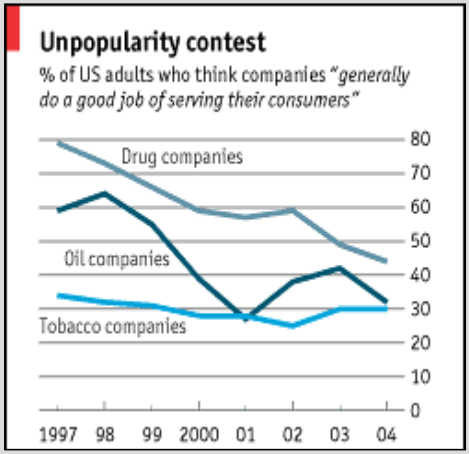
'Accountability to all company stakeholders – employees, communities, investors, civil society – through engagement, disclosure and constructive responses is a precondition to business success. Accountability fosters trust, and trust, arguably a company's single most valuable asset, takes years to build and only days to lose.'

Business for Social Responsibility, 2006

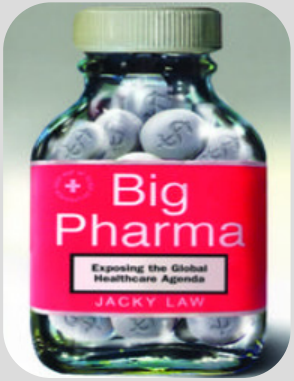
A case in point: The pharma industry – profitable, trusted and valued?



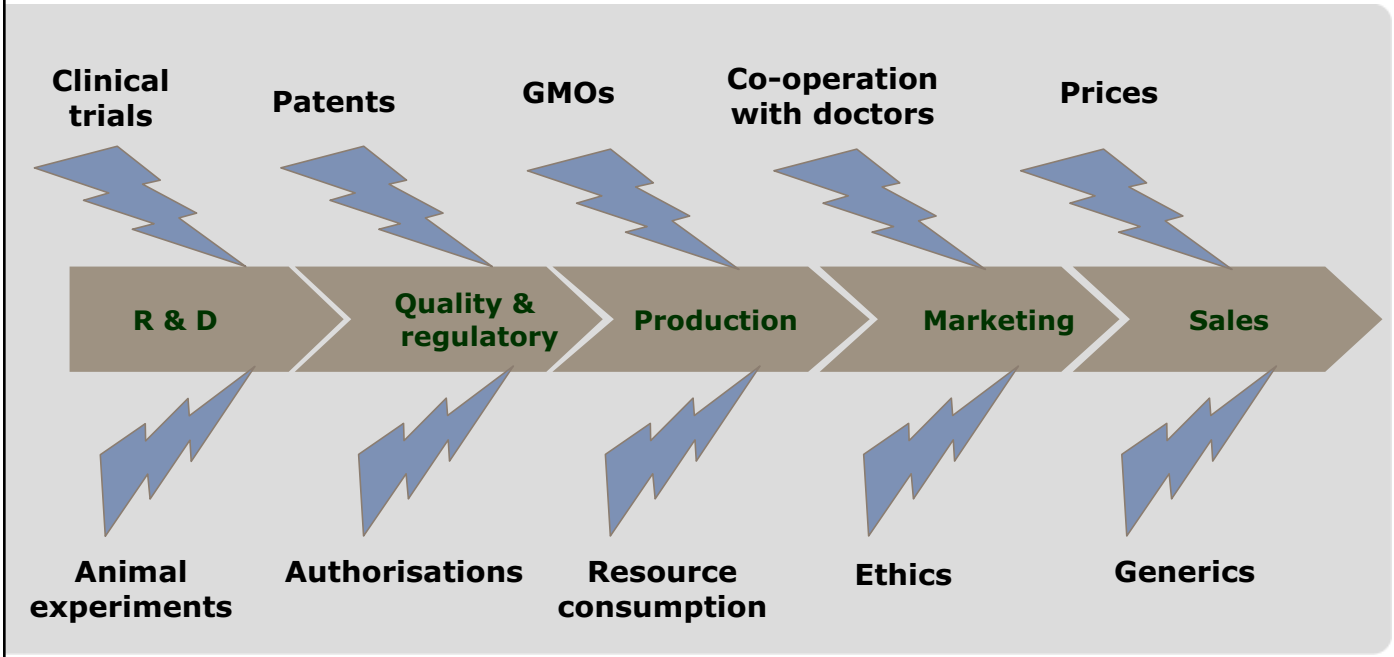
Source: Kaiser Family Foundation
Health Poll Report Survey 2005



Source: Harris Interactive



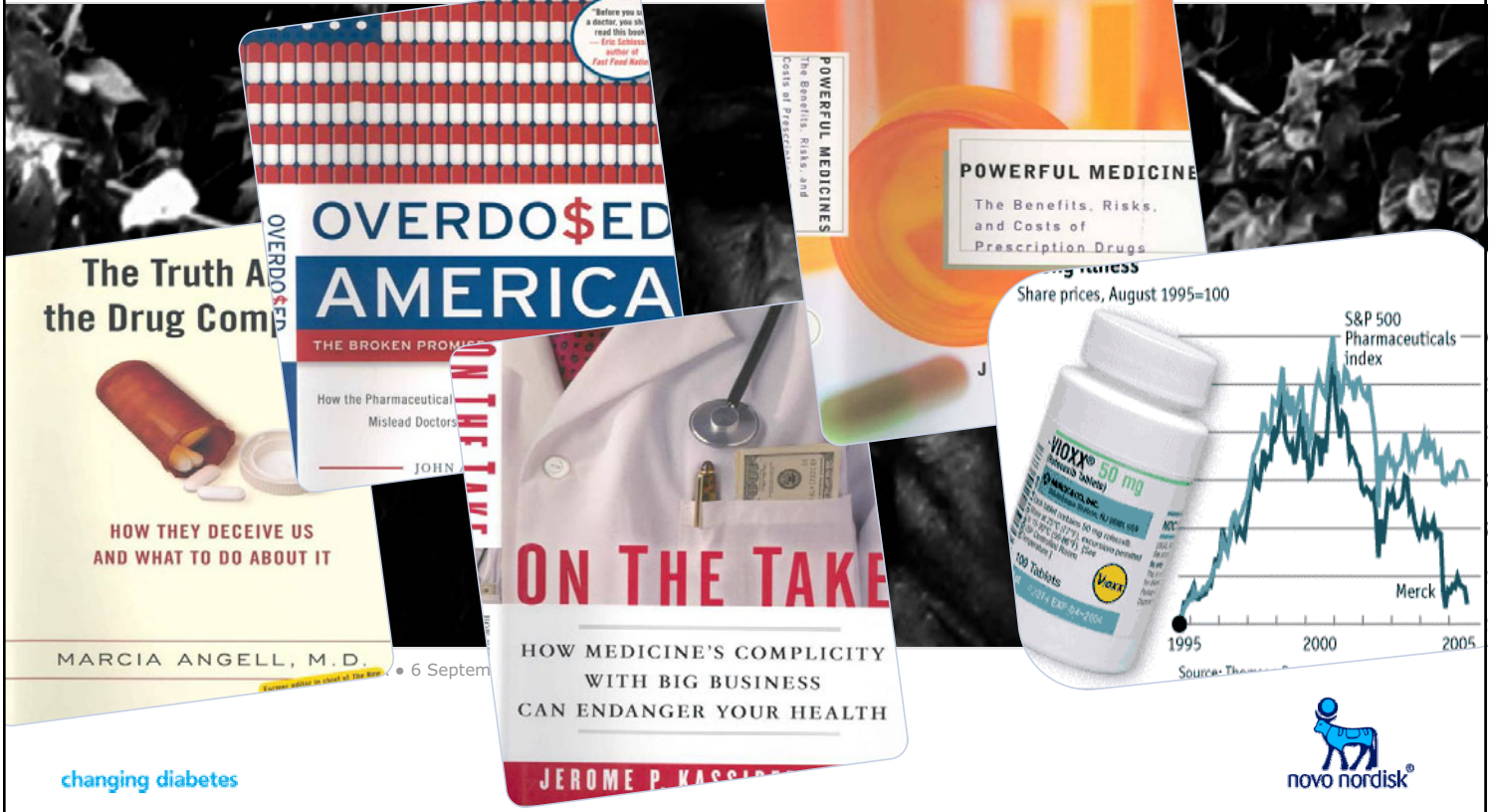
Industry practices are under public scrutiny – throughout the value chain



changing diabetes

novo nordisk®

"So - what does the 800 pound gorilla do? Anything it wants..."



• 6 Septem

changing diabetes

novo nordisk®

Sustainability - a different approach

2

Novo Nordisk at a glance: A focused healthcare company

- Approx 23,000 people
- Sales in 2005: 33.7 billion DKK
- Diabetes care and biopharmaceuticals
- Foundation owns 70% of shares

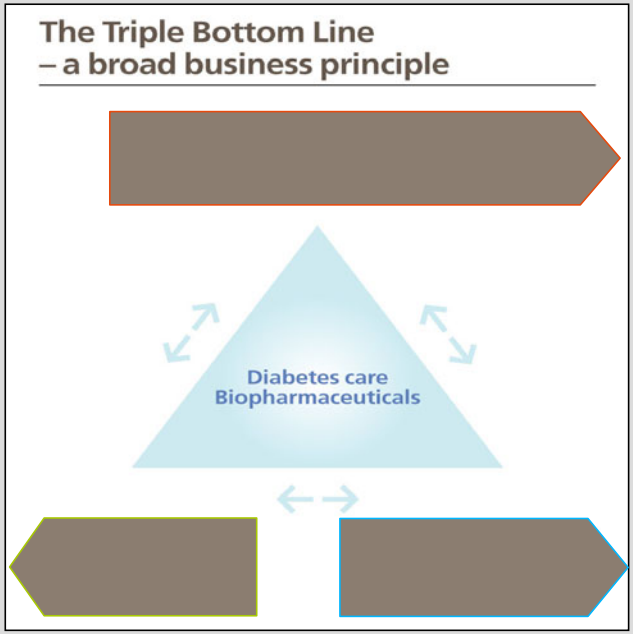
- Active in 179 countries
- Affiliates in 78 countries
- Headquartered in Denmark

changing diabetes

novo nordisk®

The Novo Nordisk Way of Management

The Triple Bottom Line business principle



Business ethics

Access to diabetes care

Climate change

changing diabetes

novo nordisk®

We will be the world's leading diabetes care company

Our aspiration is to defeat diabetes by finding better methods of diabetes prevention, detection and treatment.

We will work actively to promote collaboration between all parties in the health care system in order to achieve our common goals.

Diabetes now seen as a bigger killer than Aids

By Frances Williams in Geneva

New estimates by the World Health Organisation put the worldwide total of deaths from diabetes at 3.2m a year, three times higher than previously thought and higher than the Aids death toll.

The number of people with diabetes is expected to more than double from 171m in 2000 to 366m by 2030, the vast bulk of the increase in developing countries, according to a report by WHO and the International Diabetes Federation, which are launching a campaign against the disease.

Type II diabetes, which accounts for more than 90 per cent of cases, is linked to obesity. Sufferers are at high risk of heart disease, blindness, amputation and kidney failure and their care puts heavy pressure on health systems.

Robert Beaglehole, director of WHO's chronic disease department, said diabetes was "a growing and massive silent epidemic that has the potential to cripple health services in all parts of the world".

Diabetes is already a leading cause of death in many developing countries and a high proportion of sufferers are in their middle years, unlike in rich nations where it mainly afflicts the over-65s.

On average, one in 10 deaths is adults aged 35-64 is attributable to diabetes but in countries with high diabetes prevalence, notably in the Pacific and the Middle East, the figure rises to one in four.

The incidence among younger age groups is also high in the Indian subcontinent and North America, and the number of people with diabetes is predicted to rise to nearly seven by 2030 from 32m today.

■ WHO experts said yesterday that diseases transmitted from animals to humans (zoonoses), such as bird flu, monkeypox and "mad cow" disease, posed an ever greater threat to public health, due mainly to changes in animal husbandry and international movement of both people and animals.

"The current upward trend is likely to continue," said François Meslin, WHO's co-ordinator for zoonoses control, after a three-day meeting on detection and prevention of outbreaks.

Though it was not possible to predict when and where the next new disease would emerge, existing diseases were expected to spread. "The Europeans are expecting the West Nile virus very soon," he said.

www.who.int/diabetes

We will offer products and services in other areas where we can make a difference

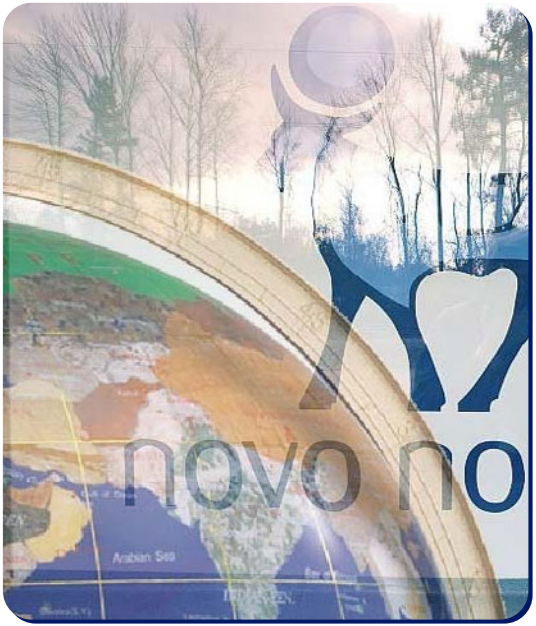
Our research will lead to the discovery of new, innovative products also outside diabetes.

We will develop and market such products ourselves whenever we can do it as well as or better than others.

We will achieve competitive business results

Our focus is our strength.

We will stay independent and form alliances whenever they serve our business purpose and the cause we stand for.



A job here is never just a job

We are committed to being there for our customers whenever they need us.

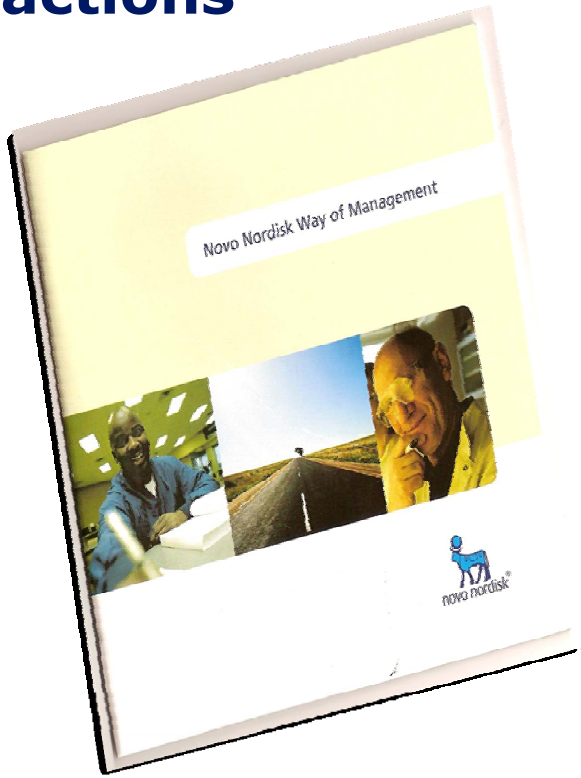
We will be innovative and effective in everything we do.

We will attract and retain the best people by making our company a challenging place to work.

changing diabetes

novo nordisk®

Our values are expressed in all our actions



Decency is what counts.

Every day we strive to find the right balance between compassion and competitiveness, the short and the long term, self and commitment to colleagues and society, work and family life.

Accounting for performance

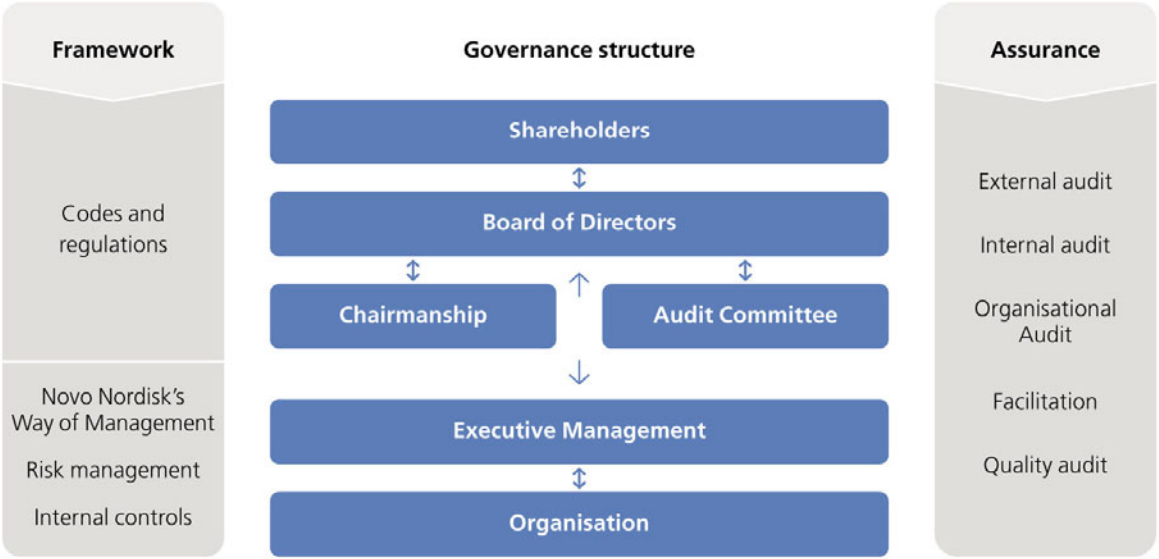
Suanne Stormer, Novo Nordisk • ECIIA • 6 September 2006

changing diabetes

Navigability – staying the course

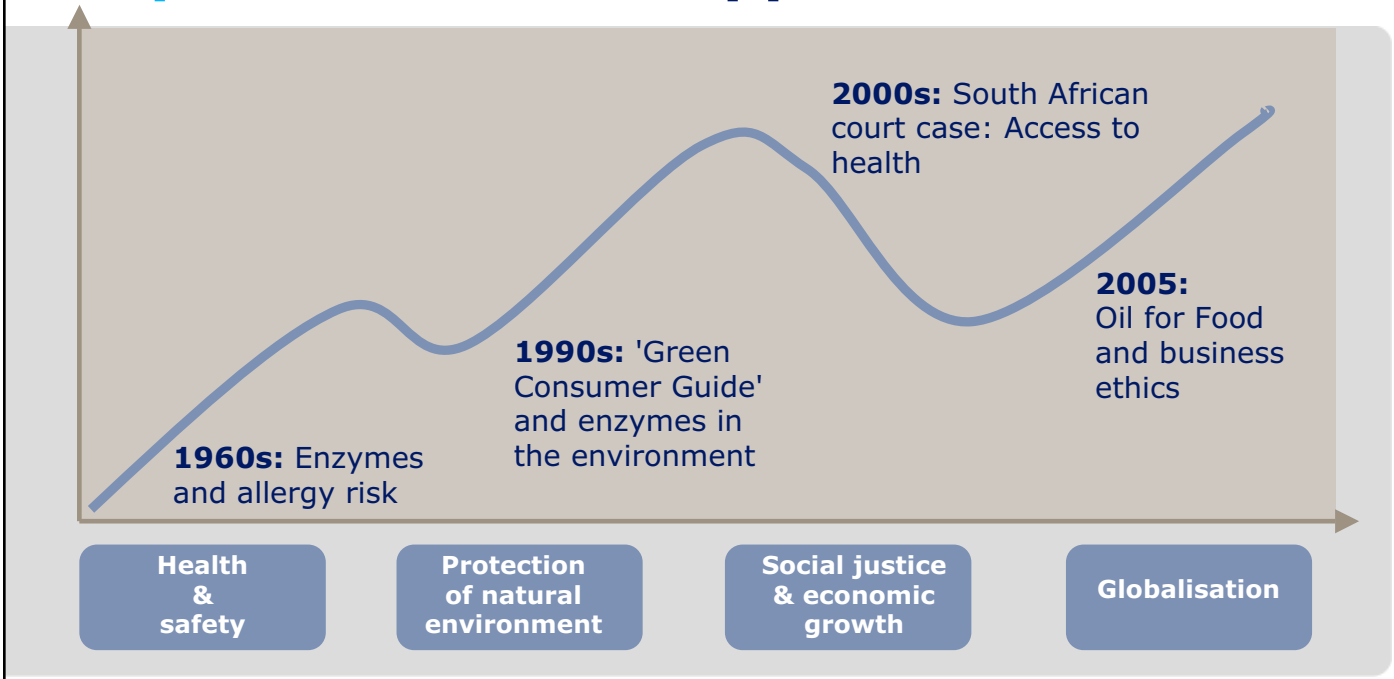
3

The corporate governance model sets the direction



The Novo Nordisk corporate governance model sets the direction and is the framework under which the company is managed.

Defining moments have shaped our Triple Bottom Line approach



Embedding the TBL approach – a learning process

Business ethics policy

Business ethics
Conflict of interest, bribery, facilitation payment, donations, interactions with suppliers

Product promotion
Interactions with public officials and healthcare professionals

Contracts
legal compliance, contracts and fees, accounting, documentation

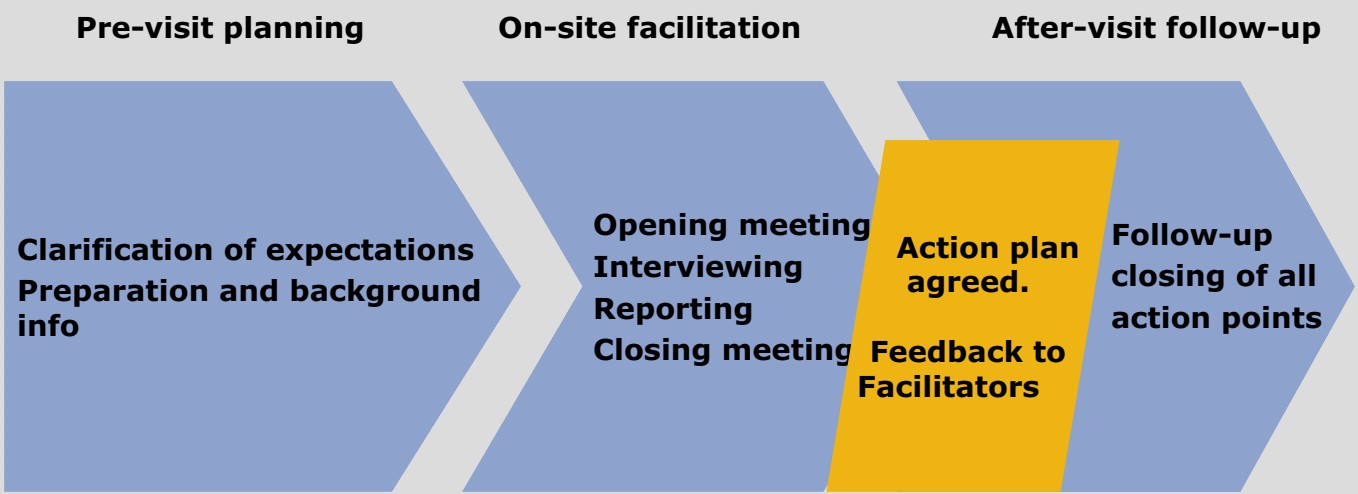
"In Novo Nordisk we will conduct our business according to a high ethical standard, living our values and protecting Novo Nordisk's reputation:

- Adhere to the principles of the UN Convention against Corruption
- Conduct business with integrity, honesty and professionalism
- Work against bribery in any form."

Training ▷ **Advice** ▷ **Raising concern** ▷ **Audit** ▷ **Balanced Scorecard**

Facilitation – follow up on values in action

An unbiased and systematic analysis of compliance with the Novo Nordisk Way of Management.



Reporting – driver of performance

- Vision and goals
- Targets
- Compliance and beyond

- Data collection and analysis
- Assurance

- Stakeholder engagement
- Reporting

- Challenging performance
- Reviewing practices
- Revisiting targets

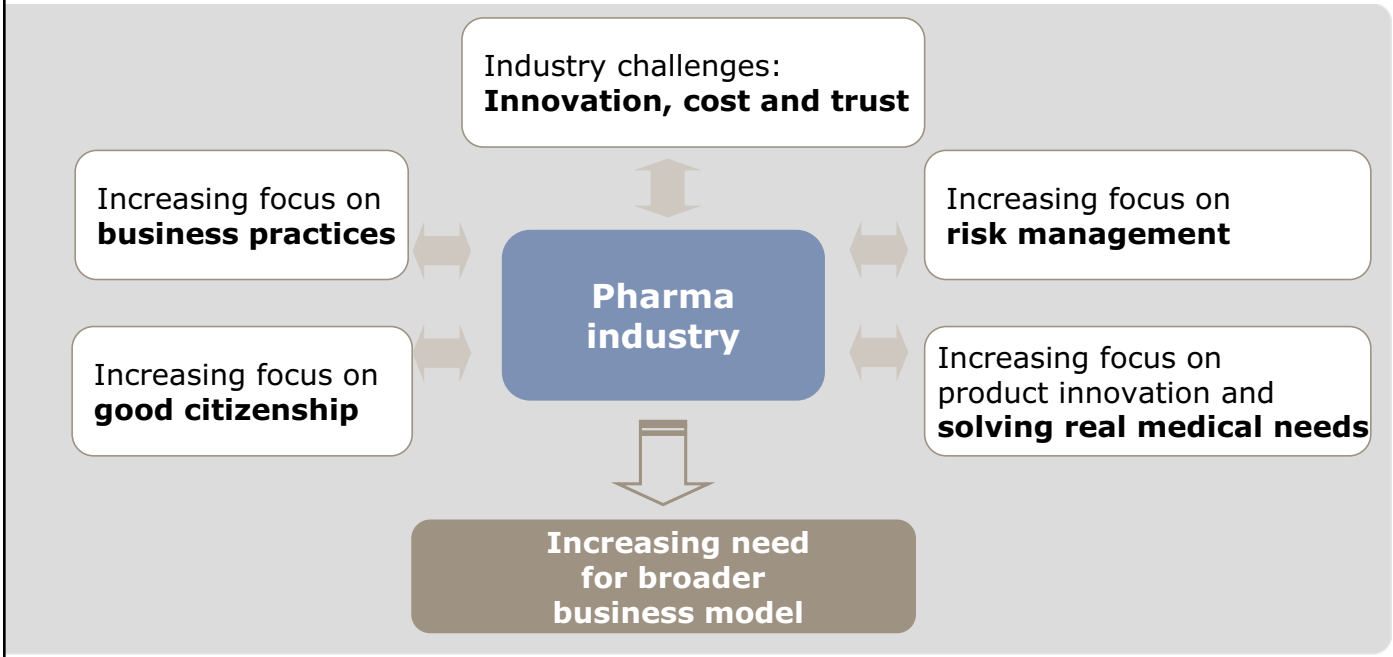
Dealing with dilemmas

- Two worlds:
  Financial and non-financial
- Mandatory vs. voluntary standards and practices
- Targets vs. goals
- Performance vs. impact
- Past vs. future
- Audience vs. readership
- Cohesive and coherent
- Comprehensive and concise
- Seamless integration

4

Profitability - the value of values

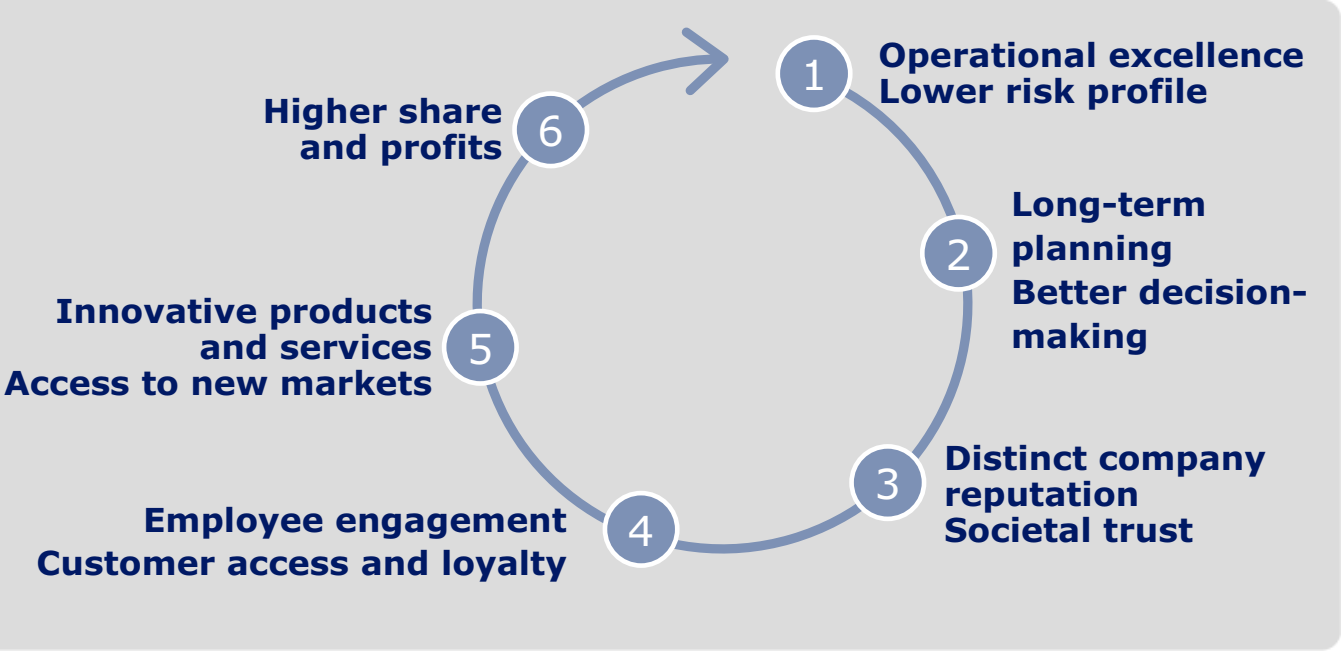
Business challenges for the pharma industry



From risk to innovation

Corporate Responsibility as risk management	Corporate Responsibility as driver of innovation
Defensive rationale: **'Business as usual'** • Risk management driven • Compliance orientated • Managed through metrics • Accountability organised • Western markets shape business model • CR separate from core business	Proactive rationale: **'Future market position'** • Driven by business opportunities • Stakeholder orientated • Managed through partnerships • Global market growth shapes business models • CR seamlessly integrated into corporate mainstream

A sustainable business model



Thank you!

ssr@novonordisk.com

novo nordisk®

C-1
Auditing the EU Budget: the various actors involved

Walter Deffaa (GER)
Director-General, Internal Audit Service
European Commission

EUROPEAN COMMISSION

IAS

Internal Audit Service

ECIIA Annual Conference 2006

–Auditing the EU Budget: The Various Actors Involved –

Dr. Walter Deffaa,
Director-General, Internal Audit Service, European Commission,

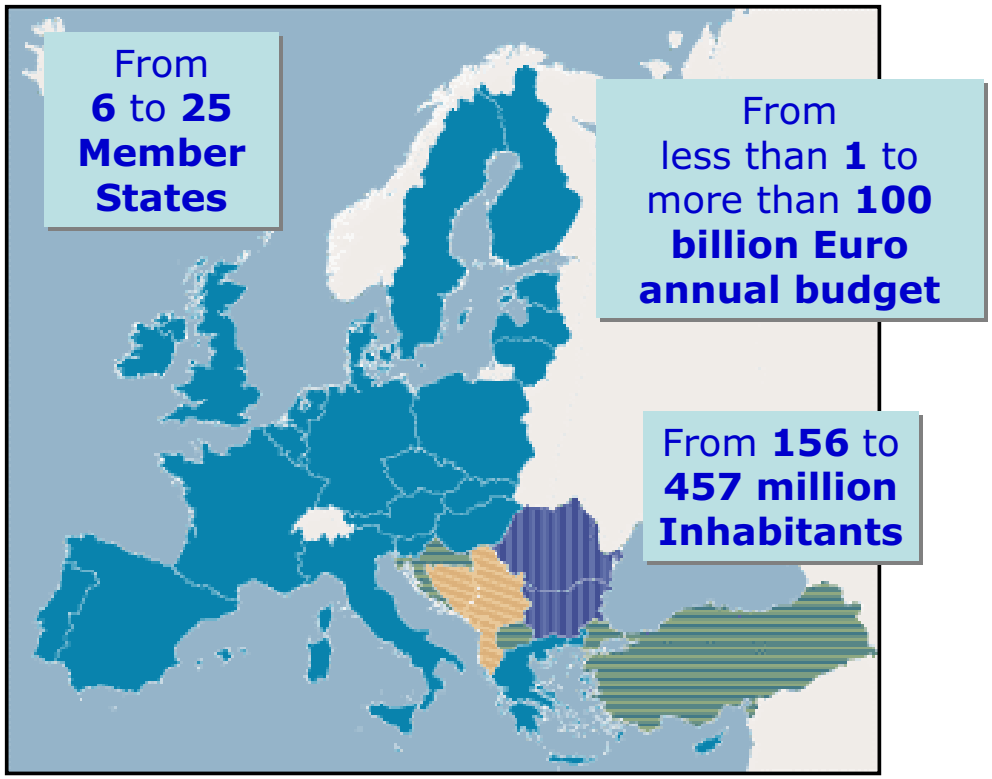
Helsinki, 7 September 2006

Presentation Overview

Content

The European Union

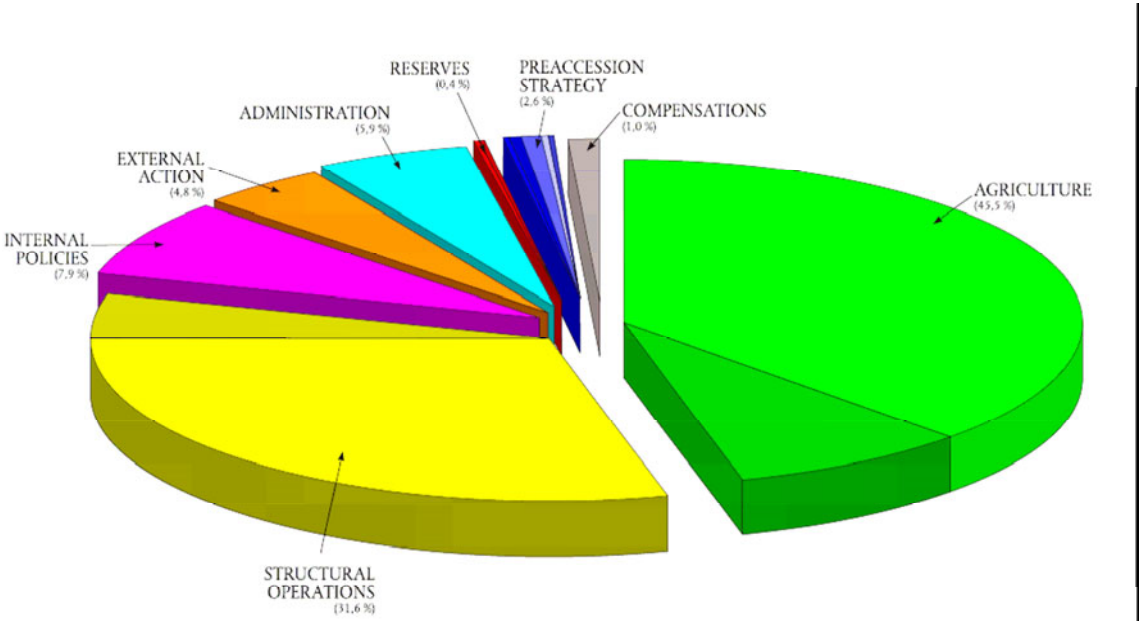
Content



The EU Budget 2006

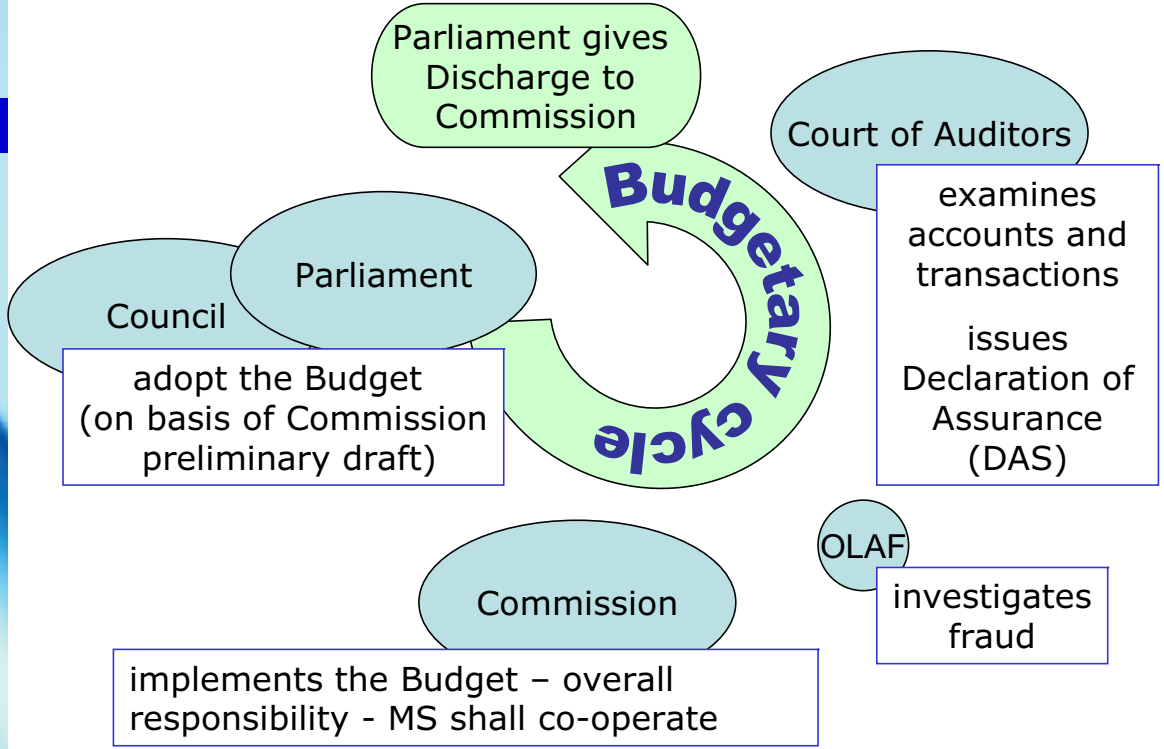
Content

The European Commission has **overall budget implementation responsibility** (EC Treaty, Art 274).



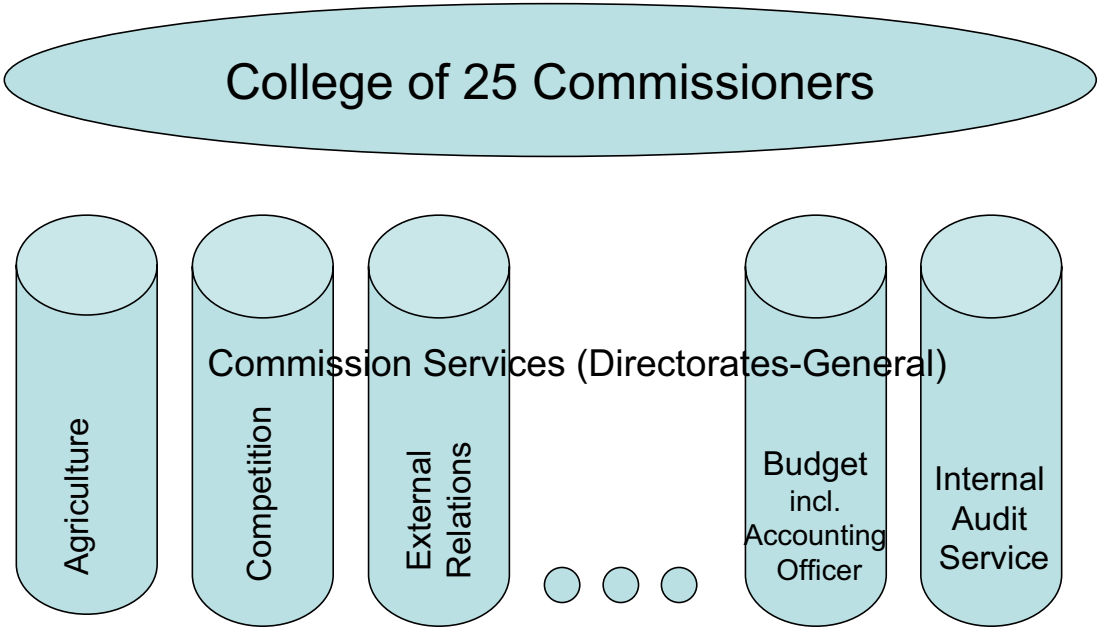
The EU Budget – Main Actors

Content



The European Commission

Content



Overview EU Management & Control Structure I

Content

Centralised Management by the Commission (or with national partners) - mainly Administration and "Internal Policies" of trans-national character, +/- 14% of the budget.

Shared Management with Member States responsible for operational and financial management - mainly Agriculture and Structural Policies, +/- 80% of the budget.

De-centralised Management, third countries are responsible for operational and financial management with Commission involvement - mainly "External Policies", some 4,5% of the budget.

Joint Management, EU funds pooled and managed by international organisations - external Policies, some 1,5%.

Overview EU Management & Control Structure II

Content

Complex management and control system for EU funds: varying degree of involvement of external actors and different accountability arrangements – **Delegation Risk**.

Recognition of **inherent risk** in public sector activity.

Public concern but also growing **understanding** among actors and stakeholders about **limitations to assurance**.

accountability / assurance issue:

debate on necessary (re-) design of management and control systems and degree of assurance possible.

Overview EU Management & Control Structure III

Content

Example Agriculture and Structural Funds – **Shared Management**

Irregularities and Fraud - reported by Member States

Field	Number of irregularities reported	Total financial impact (in € million)
EAGGF Guarantee	3 193	102
Structural Funds and Cohesion Fund	3 570	601

Compared to total payments (in million EUR):
48.466
32.763

Source: Commission report on the Fight against Fraud for 2005, COM(2006)378 and Provisional Annual Accounts 2005, http://ec.europa.eu/budget/

Recovery and Corrections -

Example Agriculture Guarantee Fund: Member States recover over 50%

Example Structural Funds: Commission 2004/5 corrections of some EUR 1.4 billion on 2000-2006 programmes

Management and Control - Reform Developments

Content

Professionalisation – Responsibilisation Accountability

- Comprehensive **Administrative Reform** programme since 2000
- **Accounting** / accounting system reform programme since 2003
- Common **Risk management** methodology adopted in 2005

Action Plan « Roadmap towards an **Integrated Internal Control Framework** » 2006 – with Member States to manage risk of error in underlying transactions:

- agree on tolerable level of risk,
- apply single audit elements (control/audit reliance),
- obtain reasonable assurance

Management and Control - Commission Reform

Content

Director General

Full Responsibility:
- Internal Control System (24 Internal Control Standards, including ex-ante and ex-post controls)

Accountability:
- Annual Activity Report + Annual Assurance Declaration
- Provide reasonable assurance on four control objectives (effectiveness, efficiency of operations – compliance with laws and regulations – safeguarding of assets – reliability of financial reporting)

Accrual Accounting

Increased authority / responsibility of Accounting Officer

Internal Audit

- DG-level Internal Audit Capabilities (IACs)
- Commission-level Internal Audit Service (IAS)
- Audit Progress Committee (APC)

Control and Audit Actors – Overview

Content

Control actors Commission:
- DG operational management
- DG control units (incl. contracted audit services)
- Central control oversight and support functions (Accounting Officer, Central Financial Service)

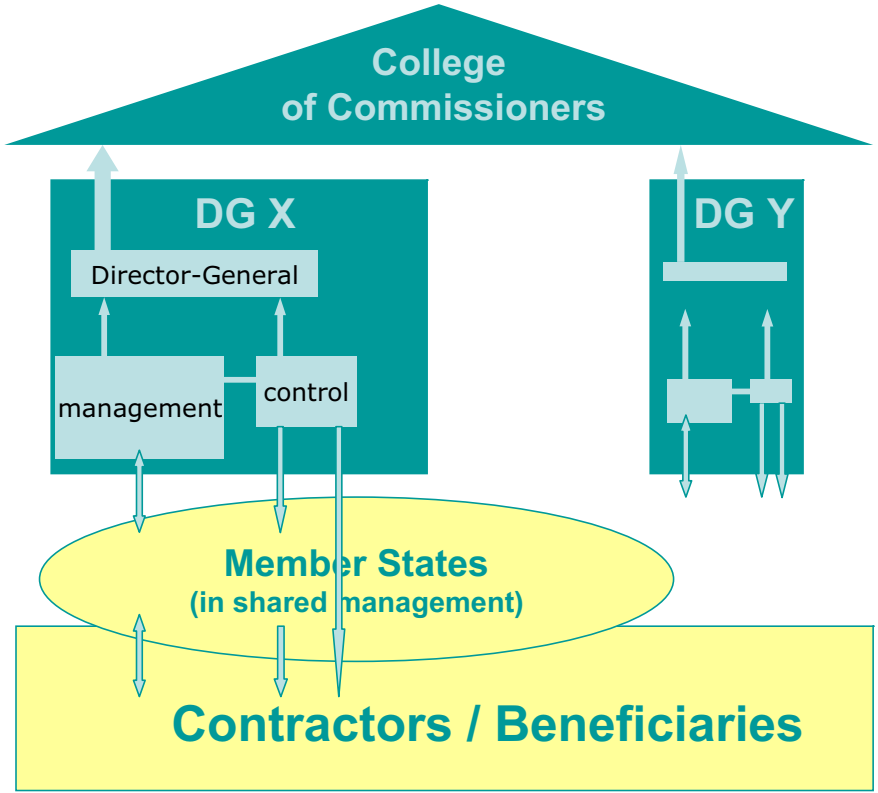
Control actors Member States (shared management)**:**
- Operational level management and control bodies
- Central level management and control functions

Internal Audit
- DG-level Internal Audit Capabilities (IACs)
- Commission-level Internal Audit Service (IAS)
- Audit Progress Committee (APC)

External Audit
- European Court of Auditors

Control and Audit Architecture – Operational Control

Content

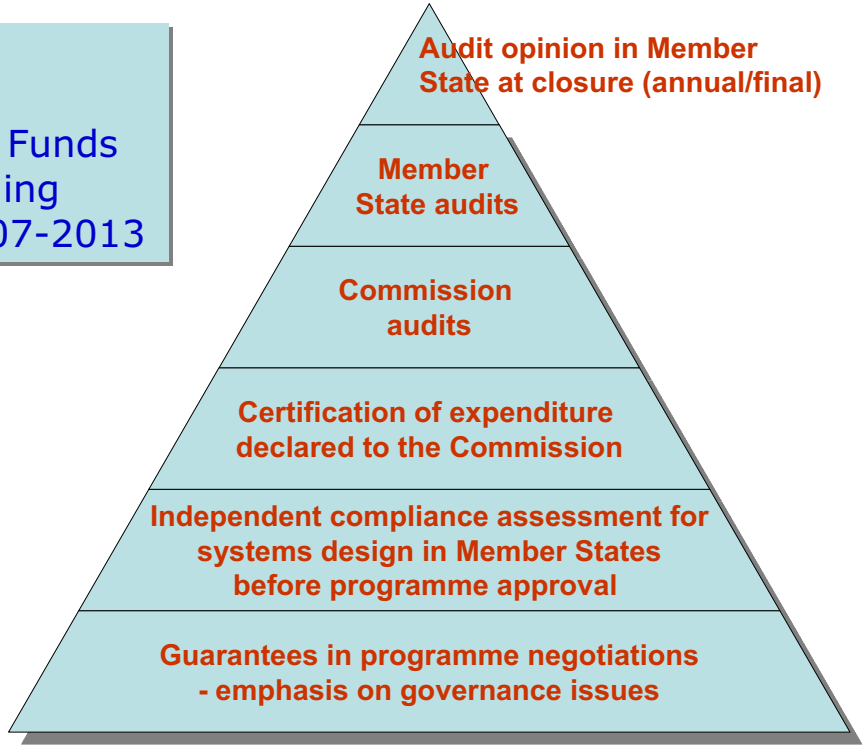


Control and Audit Architecture – Operational Control

Content

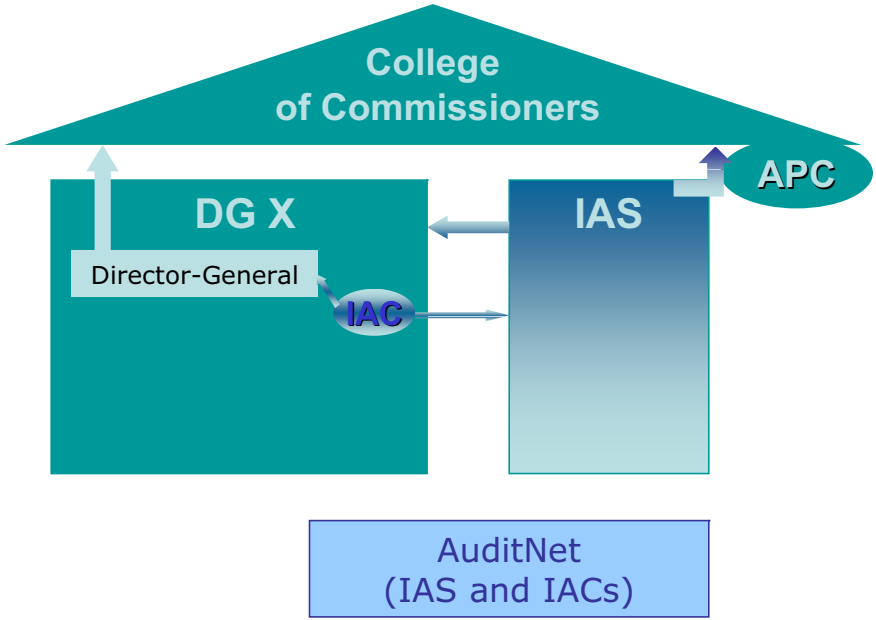
Example:

Structural Funds Programming Period 2007-2013



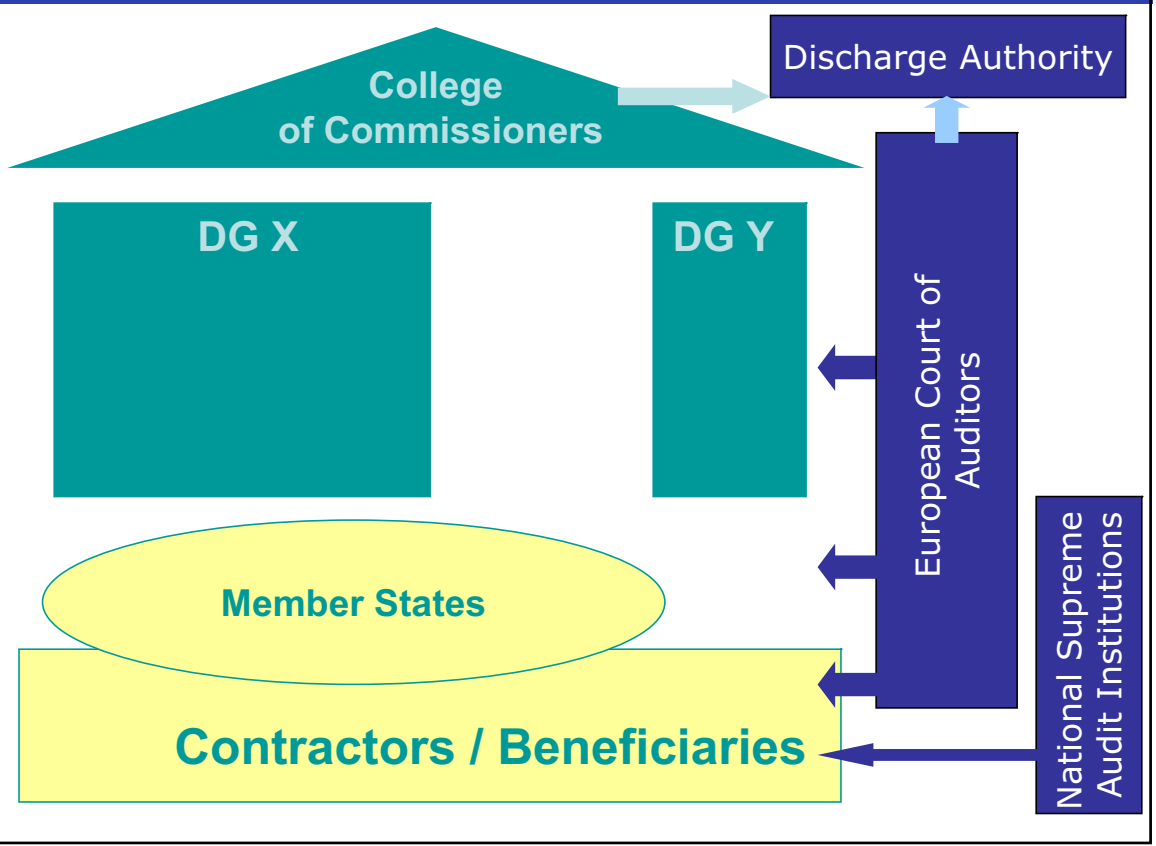
Control and Audit Architecture - Internal Audit

Content



Control and Audit Architecture - External Audit

Content



Résumé

Content

European Commission: From sole policy and law making to extensive programme management responsibilities.

From « It is becoming difficult to find anyone who has even the slightest sense of responsibility » to a clear accountability framework.

Complex architecture for budget implementation.

Better integrated management and control framework for new shared management programming generation 2007 – 2013.

Outlook - Challenges for the Future

Content

Transparency.

Simplification.

Align cost and benefits of controls.

Strategic perspective:
Positive declaration of assurance from European Court of auditors.

C-2
Financial and Compliance Auditing of EU sponsored projects

Ágnes Dobó (HUN)
Senior Expert
Ministry of Finance, Hungary

FINANCIAL AND COMPLIANCE AUDITING OF EU SPONSORED PROJECTS

Ágnes DOBÓ
Senior expert
Ministry of Finance, Hungary

Main topics

- Requirements and basic principles of auditing EU Structural and Cohesion Funds
- Players in Hungary
- Experience in auditing EU projects, typical findings (system audits and sample based project audits)
- Future challenges

Legal requirements

- Most important EU Regulations
  - Financial Regulation (1605/2002)
  - Regulations concerning Structural Funds (1260/1999, 438/2001, 448/2001, 1685/2000 and 438/2004)
  - Regulations concerning Cohesion Fund (1164/1994, 1264/1999, 1265/1999, 1386/2002)
  + Methodological guidance issued by the Commission

Legal requirements

- Hungarian legislation (most important ones)
  - General legislation on the management and control of public funds:
    - Act XXXVIII of 1992 on Public Finances
    - Act LXV of 1990 on Local Governments
    - Gov. Decree 217/1998 on the operation of public finances
    - Gov. Decree 193/2003 on the internal audit of public budgetary organisations
    - Gov. Decree 70/2004 on the Government Control Office

  + Methodological guidelines and manuals issued by the Ministry of Finance

Legal requirements

- Hungarian legislation (most important ones)
  - Special regulation on the management and control of Structural and Cohesion Funds:
    - Gov. Decree 360/2004 on financial management, accounting, control and audit of Structural and Cohesion Funds and EQUAL
    - Gov. Decree 1/2004 on the Hungarian institutions responsible for the use of support from the EU Structural and Cohesion Funds
    - Joint Decree 14/2004 on the general rules of the use of Structural and Cohesion Funds
    - Gov. Decree 124/2003 on the establishment of the monitoring system of programmes carried out with the financial support of the EU

Basic principles

- Without prejudice to the Commission's responsibility for implementing the general budget of the European Communities, Member States shall take responsibility in the first instance for the financial control of assistance
- Management and control systems shall ensure that Community funds are being used efficiently and correctly (in accordance with the principles of sound financial management)
- Preventing, detecting and correcting irregularities shall be ensured and any amounts lost as a result of an irregularity detected shall be recovered

Control and audit tasks concerning Structural and Cohesion Funds

- Financial management and control system (FM/C)
  - at every level of the system
  - separation of functions
  - „four eyes principle”
  - audit trail
  - Art. 4 verifications – on-the-spot checks
  - retention of documents

Control and audit tasks concerning Structural and Cohesion Funds

Certification of expenditure

The objective is to certify that the statement of expenditure includes only expenditure

- that has been actually effected within the eligibility period laid down in the decision in the form of expenditure by final beneficiaries,
- can be supported by receipted invoices or accounting documents of equivalent probative value,
- that has been incurred in operations that were selected for funding under the particular assistance with the selection criteria and procedures
- and have been subject to Community rules throughout the period during which the expenditure was incurred,
- from measures which all state aid has been formally approved by the Commission.

Control and audit tasks concerning Structural and Cohesion Funds

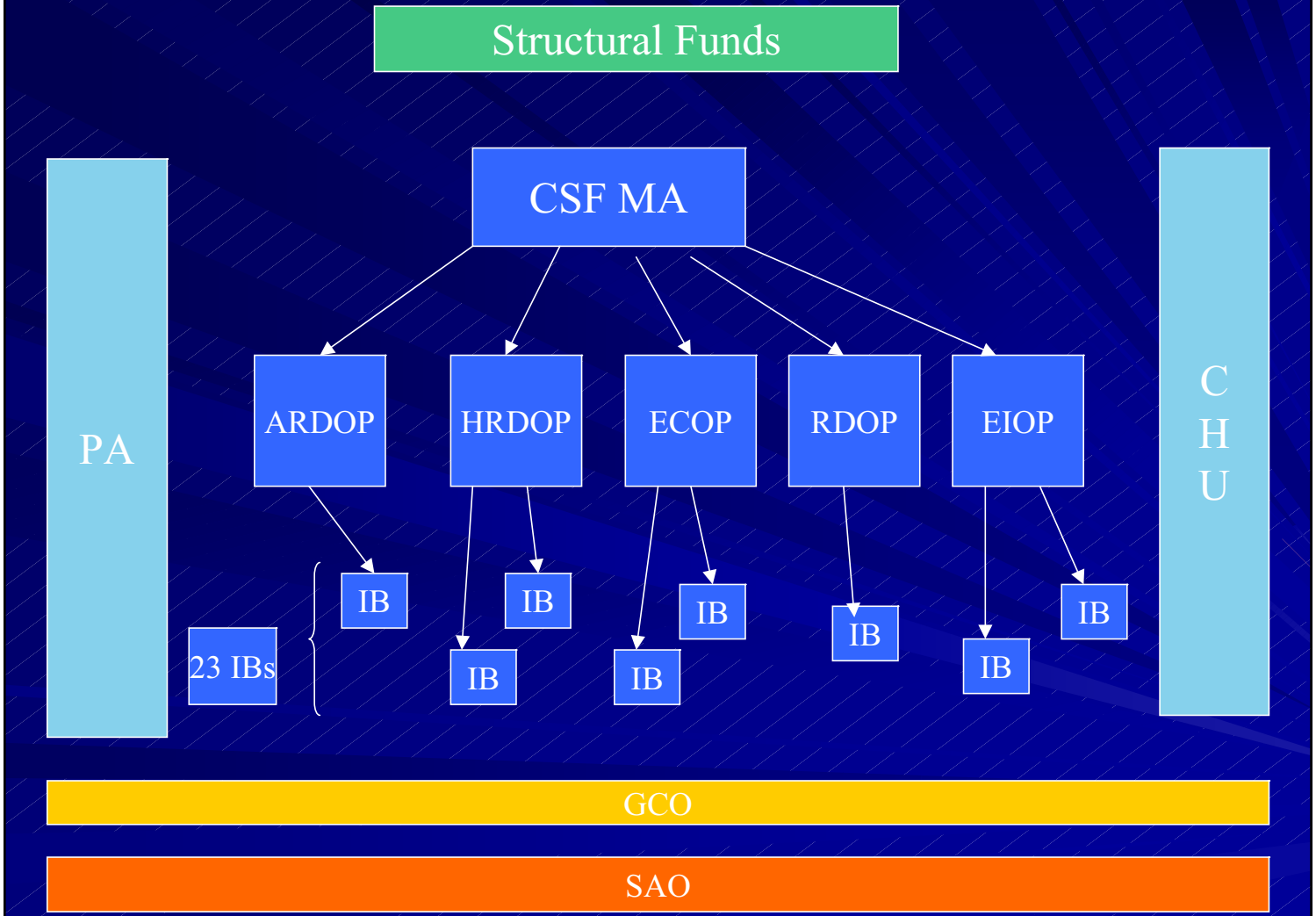
- Internal audit
  - Shall be ensured at all organisation involved
  - According to internationally accepted auditing standards
  - System audits for the whole system carried out by the Government Control Office
  - CSF Managing Authority is also authorised to audit the whole system, and the Paying Authority as regards financial management and control systems

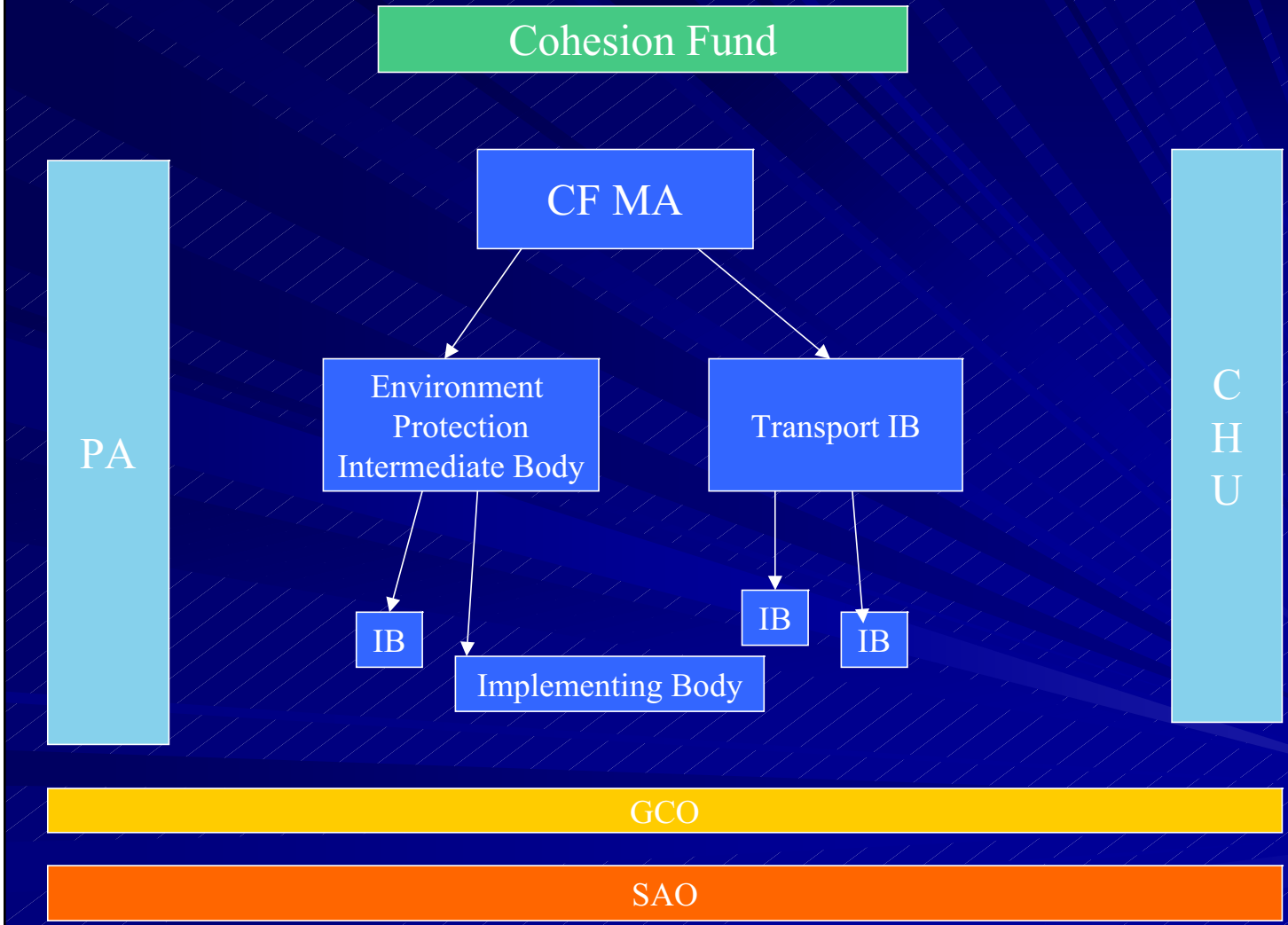
Control and audit tasks concerning Structural and Cohesion Funds

- 5-15% checks
  - Special requirements regarding sampling (risk based sample combined with some elements of representative sampling)
  - Structural Funds: at least 5% of total eligible expenditure
  - Cohesion Funds: at least 15% of total eligible expenditure
  - Done by the Government Control Office

Control and audit tasks concerning Structural and Cohesion Funds

- Declaration at winding-up of the assistance
  - The goal is to obtain reasonable assurance that the certified statement of expenditure is correct and the underlying transactions are legal and regular
  - Based on the examination of the management and control systems, of the findings of checks already carried out and, when necessary, of a further sample check of transactions
  - Done by the Government Control Office


Structural Funds
CSF MA
PA
CHU
ARDOP
HRDOP
ECOP
RDOP
EIOP
IB
23 IBs
GCO
SAO


Cohesion Fund
CF MA
PA
Environment Protection Intermediate Body
Transport IB
C H U
IB
IB
IB
Implementing Body
GCO
SAO

Experience in auditing EU projects

- Audits done based on the audit strategy and scheduled according to the annual work plan
- Audit plan for each assignment
- Preparation – field work – draft report – conciliation – final report (findings and recommendations) – follow-up of recommendations
- Relation between system audits and sample based project audits

Experience in auditing EU projects

- Main findings of system audits:
  - Systems in place generally comply with the requirements (however, there is room for improvement)
  - Changing national legislation has effect on procedures – moving systems
  - Problems regarding human resources
  - Financial management and control systems to be strengthened and rationalized (deficiencies and overlaps, delays, documentation problems)
  - Shortcomings in the development of supporting IT system (EMIR)

Experience in auditing EU projects

- Sample based project audits

  Selection criteria:

  - To check an appropriate mix of types and sizes of operations
  - Any risk factors which have been identified by national or Community checks shall be taken into account
  - To check the main intermediate bodies and final beneficiaries at least once before the winding-up of each assistance

  Checks shall be spread evenly over the period

  Special attention to systematic problems

Experience in auditing EU projects

- Typical findings of sample based project audits:
  - Significant delays in the system (project selection, contracting, payment, etc.)
  - Information and communication requirements not fully complied
  - Lack of documentation or incomplete records on controls carried out
  - Horizontal policies not checked appropriately during verification (FM/C)
  - Property changes and changing beneficiaries

Experience in auditing EU projects

- Typical findings of sample based project audits (cont.):
  - Delays in project implementation and exceeding costs previously planned
  - Incomplete accounting records
  - Lack of splitting expenditure between implementation of EU sponsored project and investment supporting objectives of prior activity
  - Dilemma on what to be considered as different technical characteristics

Future challenges

- Amended EU regulation for the new programming period (2007-2013):
  - Audit Authority to be designated, concentration of audit tasks
  - System (compliance) audit at the beginning of the programming period
  - Annual opinion issued by the Audit Authority
  - Eligibility rules (and approach) changed
- Development of an Integrated Internal Control Framework at EU level

Thank you for your kind attention!

Ágnes Dobó
Senior expert
Directorate for Budget and Fiscal Policies, Unit for EU affairs
Ministry of Finance of Hungary
Phone: + 36-1-327-5663
Fax: + 36-1-327-5949
E-mail: agnes.dobo@pm.gov.hu

C-3
Roles of Internal Audit in Enterprise Risk Management

Peter Brady (IRL)
Audit Manager
Electricity Supply Board (ESB), Ireland

The 2006 European Conference of Internal Audit

Helsinki - September 6th-8th

Track C-3:

Roles of Internal Audit in Enterprise Risk Management

Peter Brady (IRL)
Audit Manager
Electricity Supply Board (ESB), Ireland

Group Internal Audit

PRESENTATION OUTLINE

- Personal and Company Orientation
- Historical Perspective on the Role of Internal Audit in Risk Management
- Roles of Internal Audit in ERM today
- Future Perspectives on Internal Audit

Group Internal Audit

PERSONAL ORIENTATION

Professional

- Information Technology
- Training & Development
- Consulting
- Internal Audit
- Management Representative ISO 9001:2000 for Internal Audit Quality Management System

Academic

- BA in Mathematics & Mathematical Physics
- MSc(Mgmt)

Group Internal Audit

ESB ORIENTATION

ESB Head Office
Dublin Ireland

ESB

- **Irish power utility**
- **Established 1927**
- **90k new customers connected**
- **5GW capacity**
- **Turnover €2.8bn (2005)**
- **Asset value €6.8bn**

ESB International

- **Wholly owned subsidiary**
- **Engineer, operator, investor**
- **Established 1973**
- **1,500 employees**
- **€470m turnover**

Group Internal Audit

PERSPECTIVE ON ESBI SELECTED PROJECTS: 2000 - 2005

Consultancy

Construction

Operations

Investment

Group Internal Audit

HISTORICAL PERSPECTIVE ON THE ROLE OF INTERNAL AUDIT IN RISK MANAGEMENT

Group Internal Audit

TRADITIONAL RISK MANAGEMENT PERSPECTIVE

The process of planning, organising, leading and controlling the activities of an organisation in order to minimise the adverse effects of accidental losses on that organisation at a reasonable cost

EARLY 1990s
RISK PERCEPTION IN ESB

- Was Functionally Biased
- HILP Model Used by Engineers
- Analysis Technically Good
- Range & Scope Limited
- Overall Approach Ad Hoc

Group Internal Audit

EARLY 1990s
PERCEPTIONS CHANGED BY:

- Reorganisation - Manager Responsible for Everything
- All Areas had own P&L Account, Asset Register, Business Plan, Targets, etc.
- Removal of Monopoly Status
- Increased Business Complexity

EARLY 1990s
INTERNAL AUDIT INVOLVEMENT

- Identify Control / Governance Requirements
- Communicate to Top Management
- Agree Approach
- Facilitate Implementation Including Provision of Risk Management IT System
- Monitor and Report Outcome

Group Internal Audit

EARLY 1990s
KEY SUCCESS FACTORS

- Line Management Ownership
- Managers' Responsibilities Clear
- Audit seen as Facilitating not Dictating
- Governance Statements Reinforced Need for a Formal Risk Management Process
- Top Management Support

EARLY 1990s
LEARNING POINT FOR ROLE OF INTERNAL AUDIT

- If Risk Management Does Not Exist in an Organisation:
  - Bring this to Management's Attention along with Suggestions for Establishing such a Process
  - If Requested, Play a Proactive Role in Assisting with the Initial Establishment of a Risk Management Process for the Organisation

ROLES OF INTERNAL AUDIT IN ENTERPRISE RISK MANAGEMENT TODAY

Group Internal Audit

EARLY 2000s
PRESSURES FOR ERM IN ESB

EARLY 2000s
THE NEED TO CHANGE

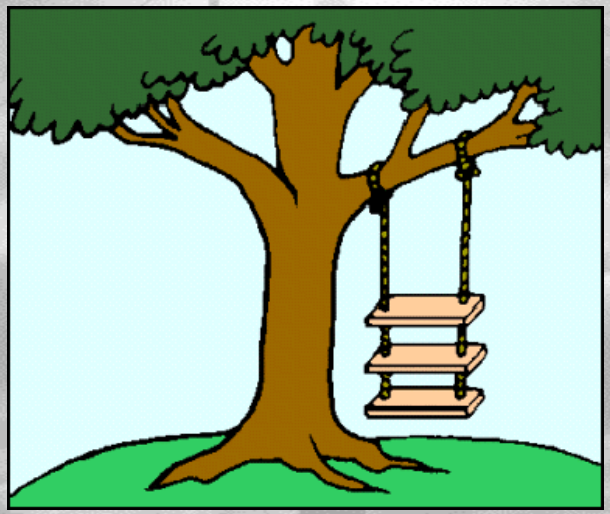
- External Consultant Brings an Objective Perspective on Risk Management in ESB
- Risk Management not Appropriately Resourced at Group Level
- Internal Audit Carrying Dual Management/Assurance Role
- CFO supports the need for ERM

TRANSITION FROM OLD RISK MANAGEMENT ROLE TO NEW ROLE IN ERM

- Established Risk Coordination Function at Group Level
- Group Risk Coordination Establishing ERM systems that Satisfy Best Practice as Appropriate to ESB
- Appointment of Chief Risk Officer Presents Opportunity to Transition Fully to New Role
- Getting the Message Right about Roles in ERM including Internal Audit is So Important!

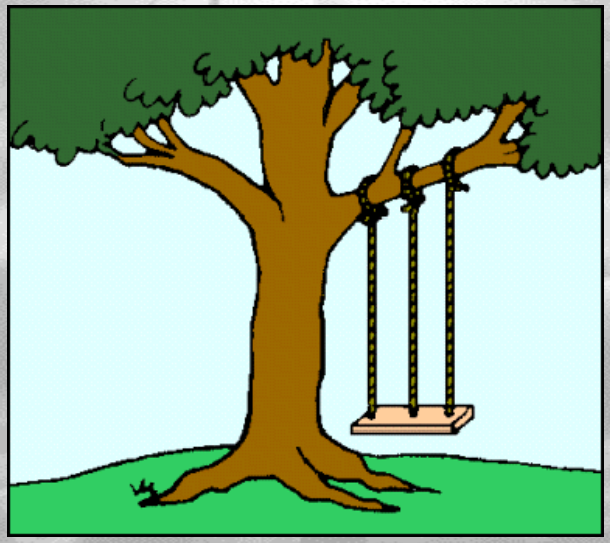
Group Internal Audit

AS SENIOR MANAGEMENT REQUESTED IT



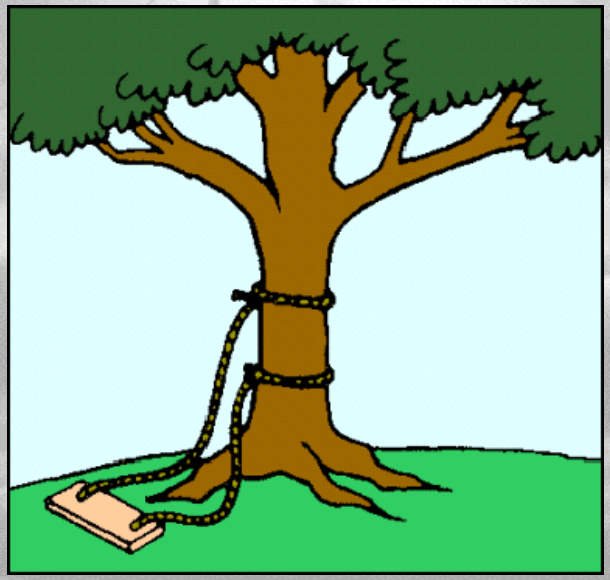
Group Internal Audit

AS BUSINESS LINE MANAGERS PERCEIVED IT



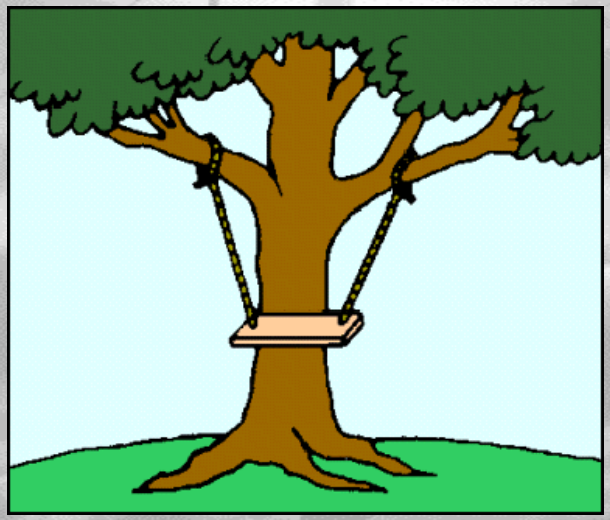
Group Internal Audit

AS CHIEF RISK OFFICER DESIGNED IT



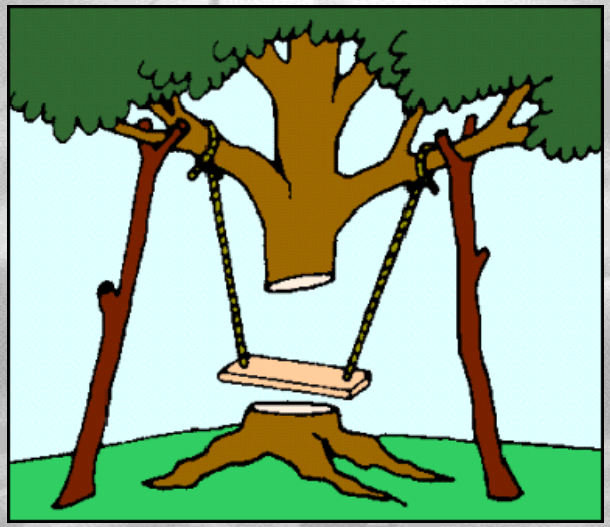
Group Internal Audit

WHAT INTERNAL AUDITORS TESTED



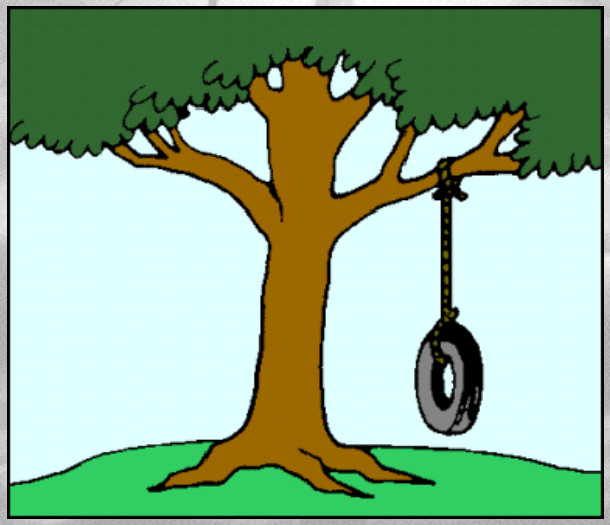
Group Internal Audit

AS BUSINESS INSTALLED IT



Group Internal Audit

WHAT THE BOARD WANTED



Group Internal Audit

INTERNAL AUDIT ROLES IN ERM

RESEARCH SUGGESTS THAT ERM ADOPTION IS POSITIVELY RELATED TO:

- Presence of a Chief Risk Officer
- Board of Director Independence
- CEO and CFO Support for ERM
- Size of the Entity
- Nature of Industry – banking, insurance, education

Source: *Journal of Accounting and Public Policy,* November/December 2005

Group Internal Audit

SOME NEW EQUATIONS!

Value = f(I,R,S,T)

Role of Internal Audit in ERM = f(T, M, C)

where

T=time and

M=maturity of risk management process

C=internal audit capability

FUTURE PERSPECTIVES ON INTERNAL AUDIT

Group Internal Audit

EMERGING GLOBAL PARADIGM

There are knowns,

known unknowns,

and unknown unknowns

– Author Unknown

Group Internal Audit

RISK MANAGEMENT THINKING HAS EVOLVED

Old Thinking

- Little risk management strategy
- Risk management limited to certain areas
- Risk analysis typically in silos
- Risks not owned
- Inspect, detect, react
- Correlation among risks not understood

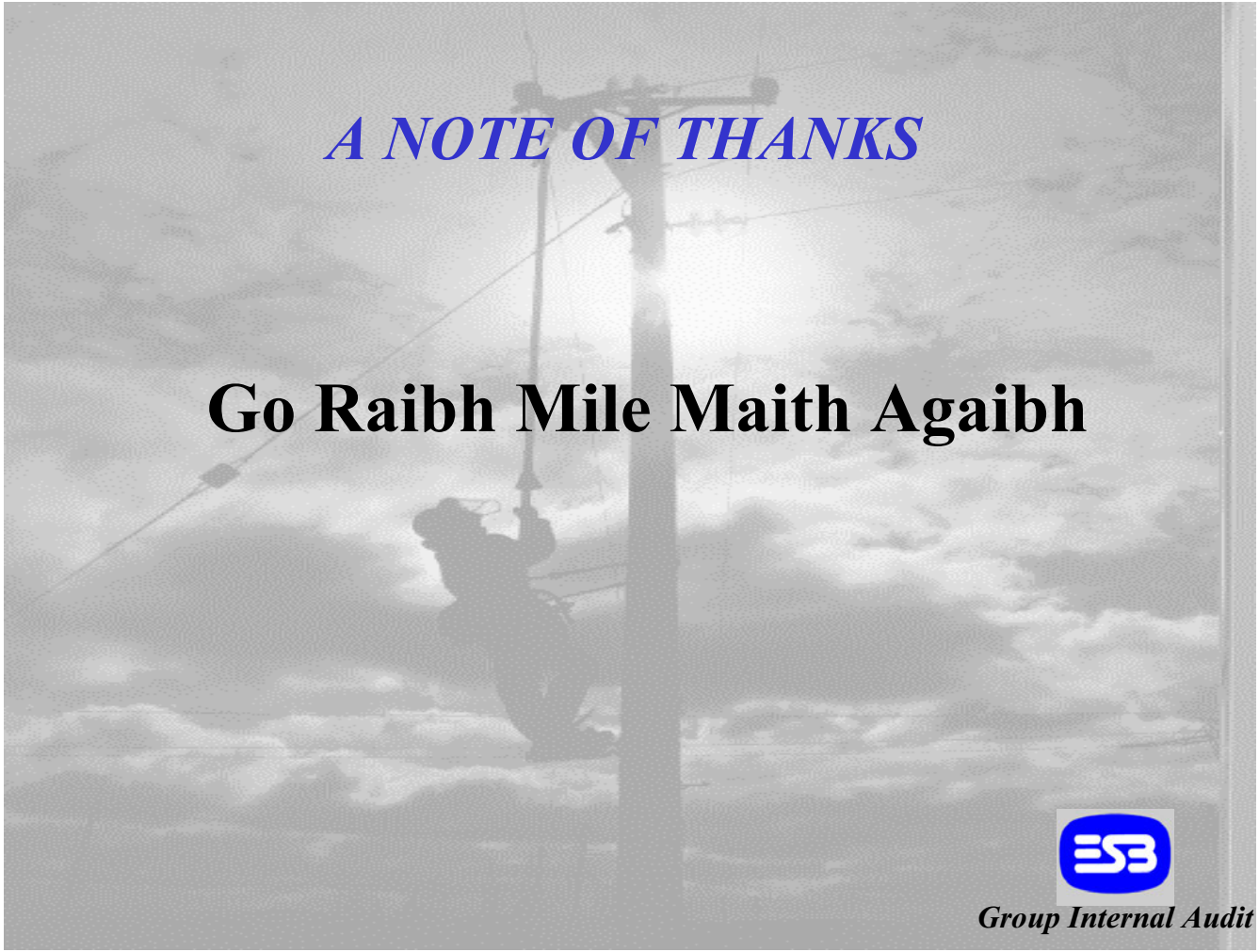
New Thinking

- Risk strategy linked to business strategy
- Risk culture created throughout the enterprise
- Risk management is a continuous, systematic process integrated within the enterprise's culture
- Risk management responsibilities clearly defined
- Risk is quantified, aggregated and studied for interrelationships
- Risk is a key consideration for decision making

CHANGING & CHALLENGING ROLES OF INTERNAL AUDIT

- The “Old” Auditor
- Living Up to Our Auditing Standards
- Heart of Corporate Governance
- Heart of Where Value is Created
- What an Opportunity!

Group Internal Audit



A NOTE OF THANKS

Go Raibh Mile Maith Agaibh

Group Internal Audit

QUESTIONS?

Why oh Why!

Group Internal Audit

C-4
Corporate Governance in the Public Sector

Gerald D. Cox (GBR)
Head of Internal Audit Partnership
South West Audit Partners

Corporate Governance in the Public Sector

Gerry Cox
Head of Internal Audit
SWAP

A Definition:

"Corporate governance generally refers to the processes by which organizations are directed, controlled, and held to account."

Australian National Audit Office

Another Definition:

"The framework of accountability to users, stakeholders and the wider community, within which organisations take decisions, and lead and control their functions, to achieve their objectives."

Audit Commission for England and Wales

Public v. Private

Private:

- Accountable to shareholders
- Motivated by profit
- Regulated – by law or compliance
- Audit Committees
- Non-executive directors
- Competitors
- Efficient and ruthless
- Corporate governance principles established

Public v. Private

Public:

- Accountable to citizens?
- Motivated by service – making a difference
- Considerable regime of inspection
- Audit Committees?
- Politicians and bureaucrats
- Sole supplier of service – the citizen has no choice
- Inefficient and weak
- Corporate governance a new concept

Characteristics – Hard & Soft

- Leadership and vision
- Culture – based on openness and honesty
- Accountable – systems of internal control
- Focus on citizen need
- Ethical and moral – transparent in everything
- Effective decision making

A Framework

- Clear constitution
- Independent scrutiny function
- Clear rules and regulations
- Direct accountability to citizens?
- Audit Committee
- Effective risk management & internal control
- Effective internal and external audit
- Key decisions made in public

Key Risks – The Audit Challenge

- Inadequate risk management
- Poor financial management
- Questionable standards of conduct
- Ineffective internal audit
- Patchy adoption of audit committees
- Inadequate performance management
- Poor project management
- Lack of accountability and clarity
- Poor leadership

The Four Pillars

- The Board – Council, Executive Management etc.
- Audit Committee, Scrutiny function etc.
- External Audit
- **Internal Audit**

The Role of Internal Audit

- Provide independent, unbiased assessment of the governance structure an the operating effectiveness of specific governance activities.
- Acting as an advisor or advocate, being a catalyst for improvement in governance structure and practices.

Effective Public Sector Internal Audit

- Organisational independence
- A formal mandate or charter
- Unrestricted access
- Properly resourced
- Competent leadership and staff – CIA
- Stakeholder support
- Work to Professional Standards - IIA

The Role of Internal Audit

- Oversight –
  - Are they doing what they are supposed to?
  - Are they complying with laws and regulations?
  - Are managers managing risk?
  - Is policy being properly/effectively implemented?
  - Detection and prevention of fraud and corruption.

The Role of Internal Audit

- Insight –
  - Are programs and policies working?
  - Share best practices.
  - Cross-cutting reviews as well as service reviews.
  - Adding value by improving systems and practices.

Role of Internal Audit

- Foresight –
  - Identifying trends before problems arise.
  - Identifying risks that have yet to materialise.
  - Help the organisation to set its risk appetite taking into account all known current and future risks.

Role of Internal Audit

- Serve as check on abuse of power.
- Focus on the needs of the citizen.
- Ensure the citizen gets ‘best value’.
- Evaluate performance against stated aims.
- Provide whistle-blower support – hotline.
- Help management see the ‘big picture’.
- Audit the corporate governance regime.

“Good governance is more than making sure that things do not go wrong or fixing them if they do. Good governance adds value; it ensures effectiveness in ever changing circumstances…..”

"……It achieves more than meeting performance targets; it balances the need for compliance with the benefits of being creative about what the organisation does and how it does it."

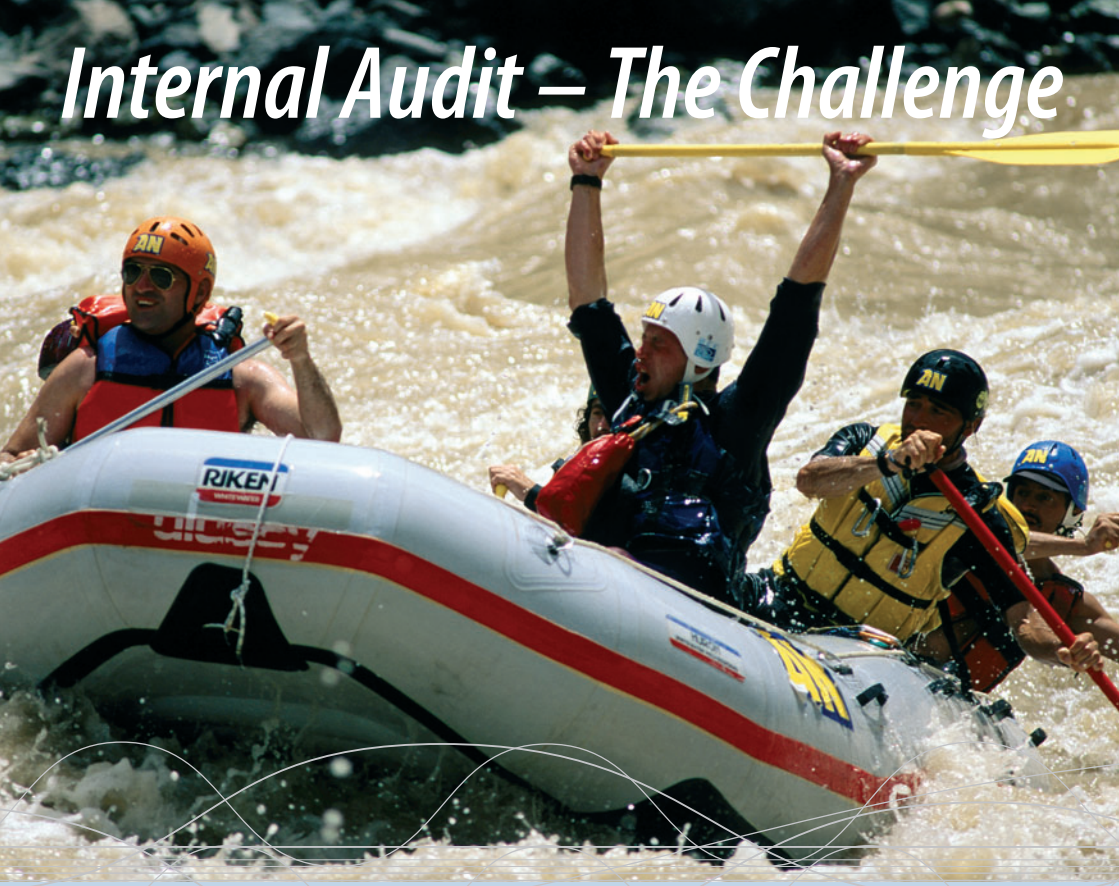
Audit Commission for England & Wales

Finally….

Internal Audit protects the interests of the citizen.

They are our ultimate client!

Internal Audit – The Challenge



Handouts

Day 2, 8th of September

The 2006 European Conference of Internal Audit

6–8 September, 2006

Hilton Helsinki Kalastajatorppa

ECIIA

European Confederation of Institutes of Internal Auditing

General Session 3
Auditing Standards Principle or Rule based?

Flemming Ruud (NOR)
Professor of Auditing, University of Zurich

University of Zurich
Institute for Accounting and Control

Auditing Standards
Principle or rule based?

ECIIA International Conference
Helsinki, Finland, 8 September 2006

T. F. Ruud, PhD, CPA (Norway)
Professor of External and Internal Auditing, University of Zurich
Adjunct Professor of Internal and External Auditing, University St. Gallen
and the Norwegian School of Management, Oslo
Email: flemming.ruud@irc.unizh.ch

Rules and principles – briefly defined

Principles

- A moral rule or a strong belief that influences your actions
- A law, a rule or a theory that something is based on (= the most basic rules)
- A belief that is accepted as a reason for acting or thinking in a particular way

Rules

- A statement of what may, must or must not be done in a particular situation - or when playing a game
- A statement of what you are advised to do in a particular situation

(Source: Oxford Dictionary)

Principles v Rules in business

- …*in corporate governance,* ***it is the principles that matter, not the rules****. "I spent a lifetime working in the accounting business where we had rules coming out of our ears and it didn't get us very far.*

Lord Colin Sharman, chairman of Aegis Corporation

Principles v Rules in business

- *The better approach lies in instilling fundamental principles, not rules, that focus on the spirit, not just the letter, of good corporate governance.*
- *Actions must be based upon the long term interests rather than the short-term expedient solutions that we find ourselves with…. This requires us to manage our businesses with integrity, cultivating long-term relationships with customers that are based on trust.*

James Schiro, CEO of Zurich Financial Services Group

Principles v Rules in business

- *I am not appealing against every new, generally applicable form of rule outside or within the formal law, but simply for* ***a sense of proportion.***
- ***Do new rules produced in response to one-off events actually help matters and effectively prevent abuses of power****?*
- *The question of how a board of directors organizes itself should be* ***resolved pragmatically rather than dogmatically****. One thing that recent events in the United States has demonstrated is that an* ***excessively complex, formalistic approach tends to heighten rather than reduce the risk of abuse****.*

Peter Brabeck-Letmathe, CEO, Nestle

Principles v Rules in business

- *In a debate with many trends, but no clear direction, the focus – **wrongly - has increasingly been on detailed rules rather than principles, and on control rather than responsibility**.*
- *Only **sound, rock-solid principles** in accounting, corporate and global governance will be able to respond to the major challenges of growing complexity, increasing turbulence and rapid change in the business world. **Rules remain necessary for predictability and enforcement**, but further details in rules will be counter-productive; excessive reliance on ever more detailed rules instead of principles is even one of the causes of the recent business failures and scandals.*

Peter Brabeck-Letmathe, CEO, Nestle

Contributing Factors – Developments

- Legal structure
  - Code-law (Roman law) versus Case-law
    - US-Generally Accepted Accounting Principles (GAAP) v
    - International Financial Reporting Standards (IFRS)
      - X standards cover Y% of issues
  - Company acts
  - Development in external audits, audit process, reporting
  - Corporate Governance initiatives
- History
  - The conqueror decides and writes the history – Wars
- Culture
- Incidents
- Societal development
- Cost of regulation – Principles or Rules?
- Desires and needs – Cookbook mentality?

Institute of Internal Auditors - Code of Ethics

The Code of Ethics contains principles and rules:

- **Principles** that are relevant to the profession and practice of internal auditing.
- **Rules of Conduct** that describe behaviour norms expected of internal auditors. These rules **are an aid** to interpreting the Principles into practical applications and are **intended to guide** the ethical conduct of internal auditors.

Principles and Rules – IIA Code of Ethics

Integrity

The integrity of internal auditors estab
for reliance on their judgment.

Objectivity

Internal auditors exhibit the highes
gathering, evaluating, and communica
process being examined. Internal audi
the relevant circumstances and are
interests or by others in forming judgr

Confidentiality

Internal auditors respect the value
receive and do not disclose inforr
unless there is a legal or professional

Competency

Internal auditors apply the knowledg
performance of internal auditing servi

1. Integrity (Rule of conduct)

Internal auditors:

1.1. Shall perform their work with honesty, diligence, and responsibility.

1.2. Shall observe the law and make disclosures expected by the law and the profession.

1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.

1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

„Moses tried it, and he failed. Sarbanes and Oxley tried it, and they will fail. We cannot legislate against dishonesty."

„Lawyers can make rules as much as they like, but good corporate lawyers will get around rules".

(Mervyn King, in: Barrier, M. (2003). „Principles, Not Rules", Internal Auditor, 08/03, p. 73)

The IIA-Standards

The purpose of the *Standards* is to:

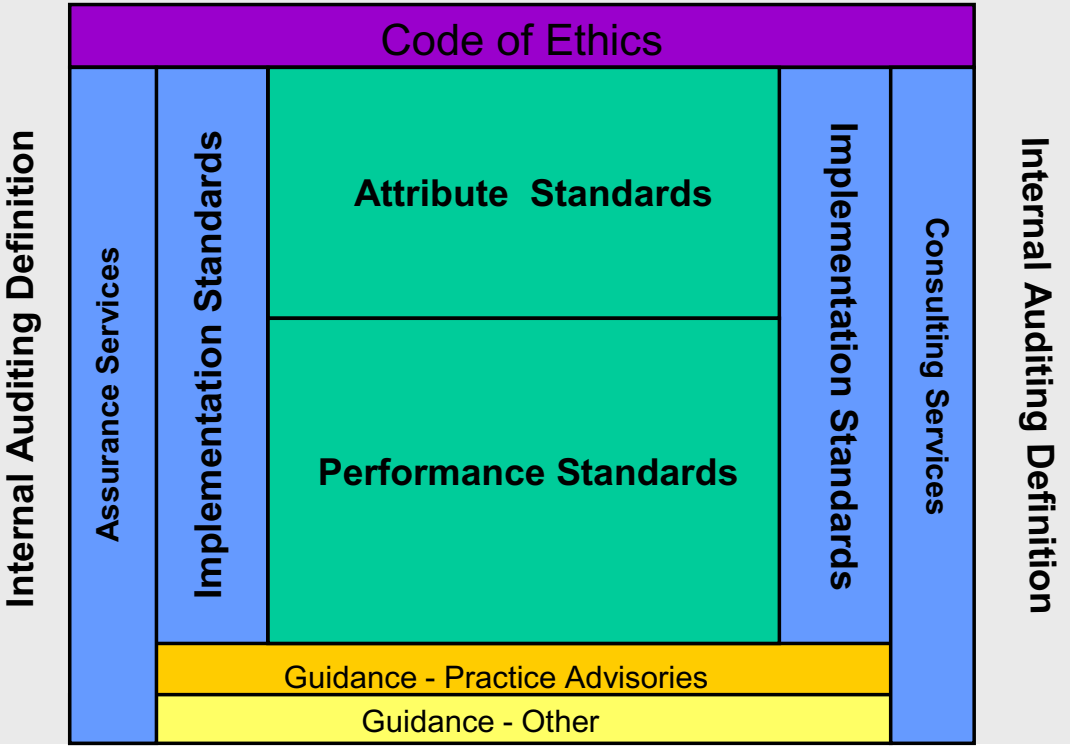
1. **Delineate basic principles** that represent the practice of internal auditing as it should be.
2. Provide a **framework** for performing and promoting a broad range of value-added internal audit activities.
3. Establish the basis for the ***evaluation*** of internal audit performance.
4. Foster improved organizational processes and operations.

→ Although mandatory and comprehensive, the Standards are primarily designed as principles, not rules

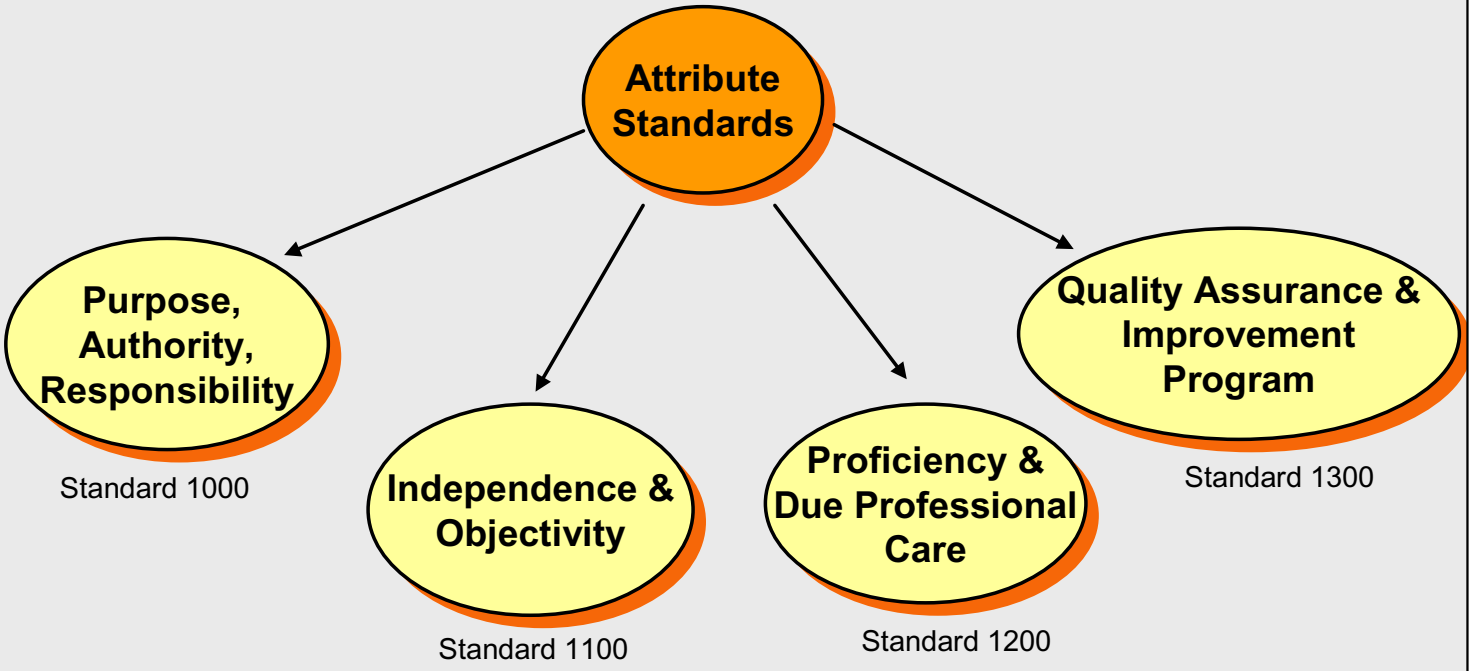
→ The Practice Advisories, which are only recommended for implementation, have more character of rules

→ Recent IIA Development: Practice Advisories are flourishing

The Professional Practices Framework



The Attribute Standards



The Performance Standards

2000 – Managing the Internal Audit Activity - The chief audit executive should effectively manage the internal audit activity to ensure it adds value to the organization.

2100 – Nature of Work - The internal audit activity evaluates and contributes to the improvement of risk management, control and governance systems.

2200 – Engagement Planning - Internal auditors should develop and record a plan for each engagement.

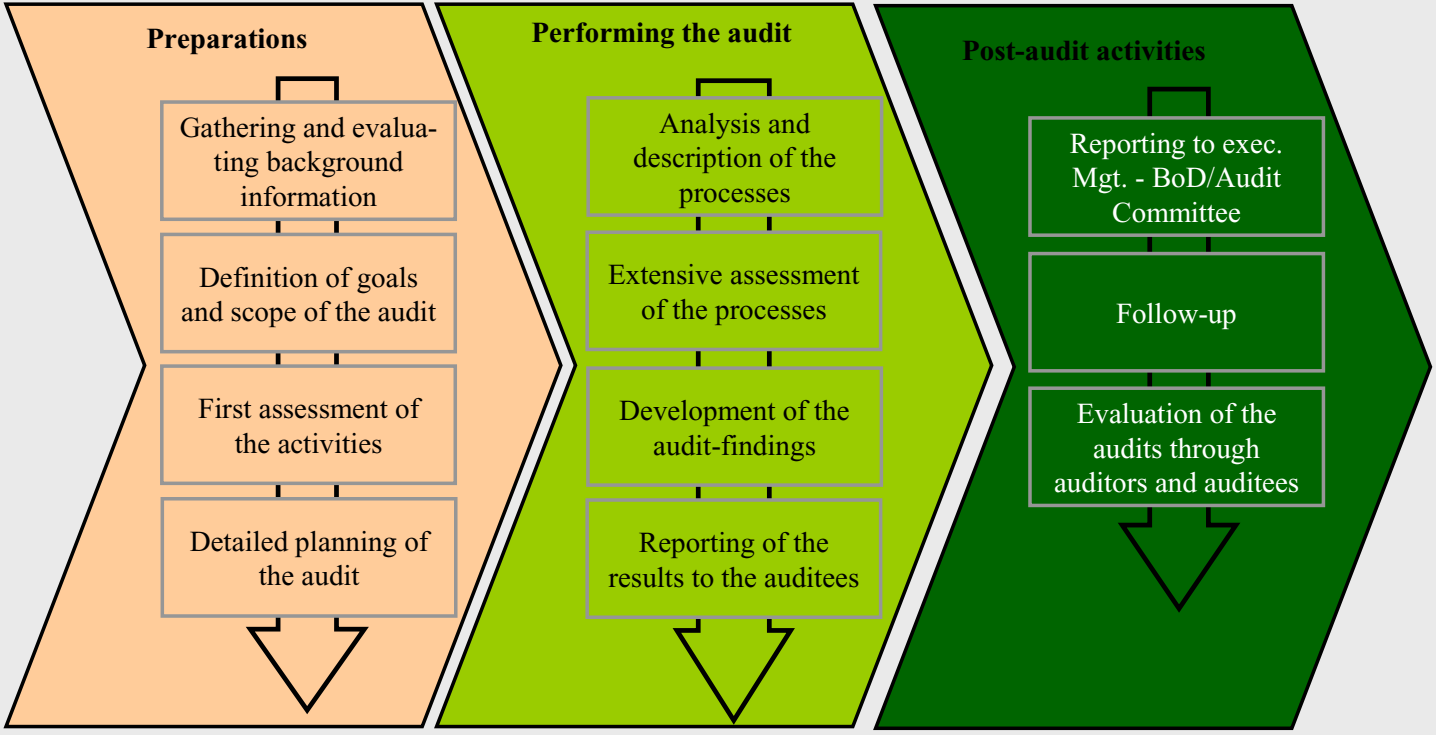
2300 – Performing the Engagement - Internal auditors should identify, analyze, evaluate, and record sufficient information to achieve the engagement's objectives.

2400 – Communicating Results - Internal auditors should communicate the engagement results promptly.

2500 - Monitoring Progress – The chief audit executive should establish and maintain a system to monitor the disposition of results communicated to management.

2600 - Management's Acceptance of Risks – When the chief audit executive believes that senior management has accepted a level of residual risk that is unacceptable to the organization, the chief audit executive should discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive and senior management should report the matter to the board for resolution.

Internal Audit Process – Performing the audit

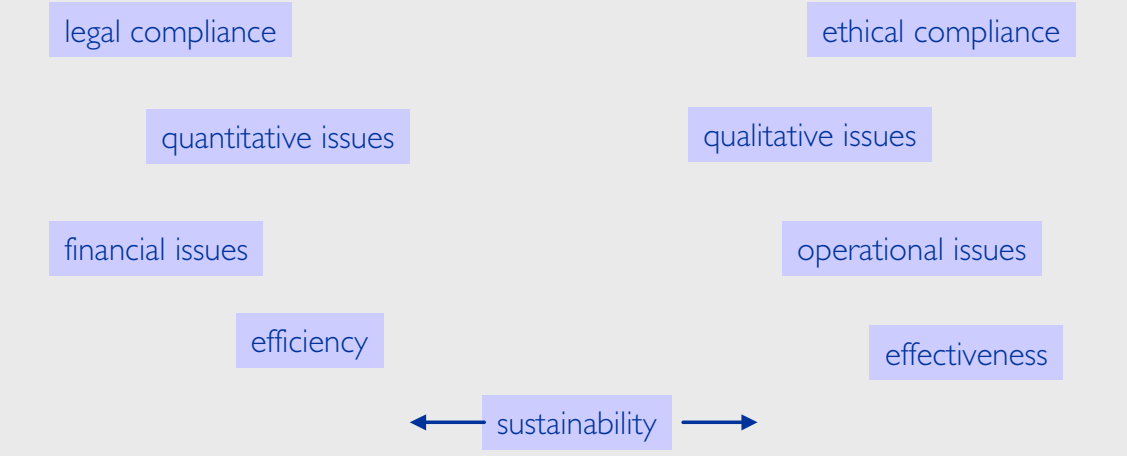


Everyday Life – Example children

Everyday Life - Example German Autobahn

Everyday Life – Example Ten Commandments

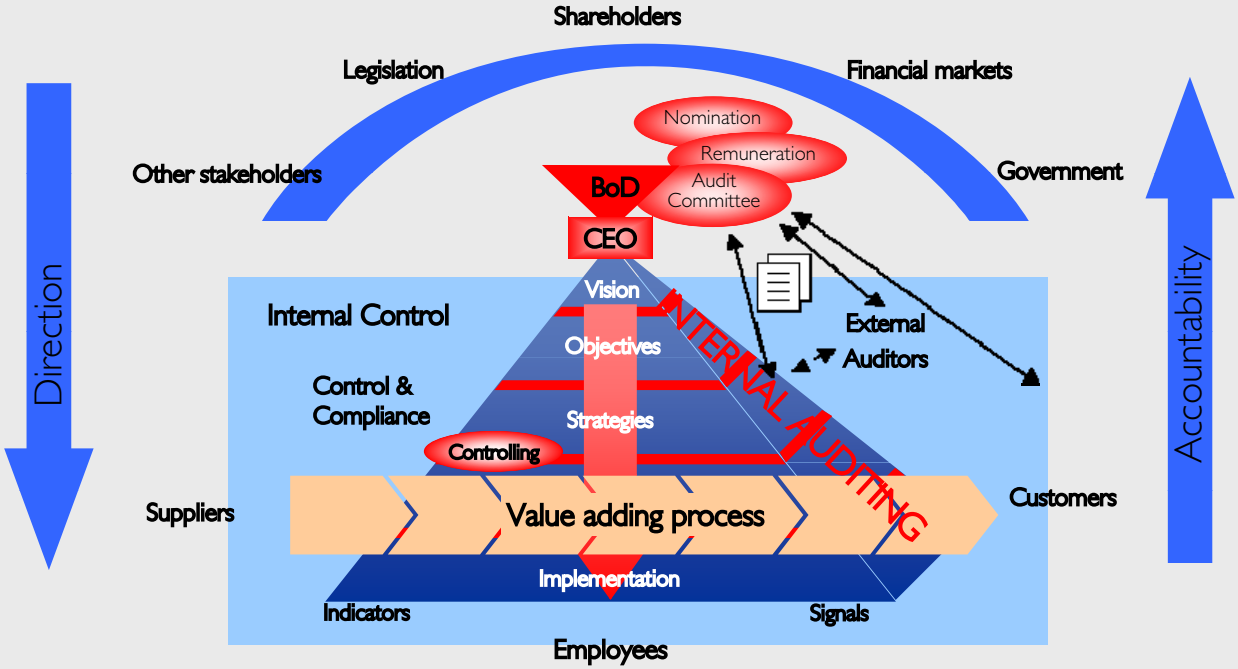
Rule – principle continuum?



Competence, Knowledge, Experience, Understanding,

Professional Judgement…

Organizational Governance – A model for Internal Auditing



Does internal auditing need to be more rule-based?

What speaks *in favour* of more rules for the internal audit profession

- Precision – and complexity – added to internal auditing
- Efficiency potentials due to standardization
- No need to justify the internal audit activity to third parties, provided that it adheres to the defined rules
- More objective third-party evaluation of the performance of internal auditing possible, as it can be compared to defined, pre-defined rules
- Reduction of a potential expectation gap
- Increased credibility of internal auditing in countries that have a ruled-based culture

What speaks *against* more rules for the internal audit profession

- Principles can be adopted (by means of interpretation) to a dynamic environment and to different basic conditions, whereas rules provide less space for evolution and adoption → *always a principle you can stick to*
- High commitment and incentive to obey principles, whereas people try to get around rules
- Rules are often too complex, non-transparent, detailed and, as a matter of principle, incomplete and vulnerable to loopholes – question of system
- Restrictive rules do not allow a better set-up of a process, structure or system
- Lawyers go after non-compliance – litigation

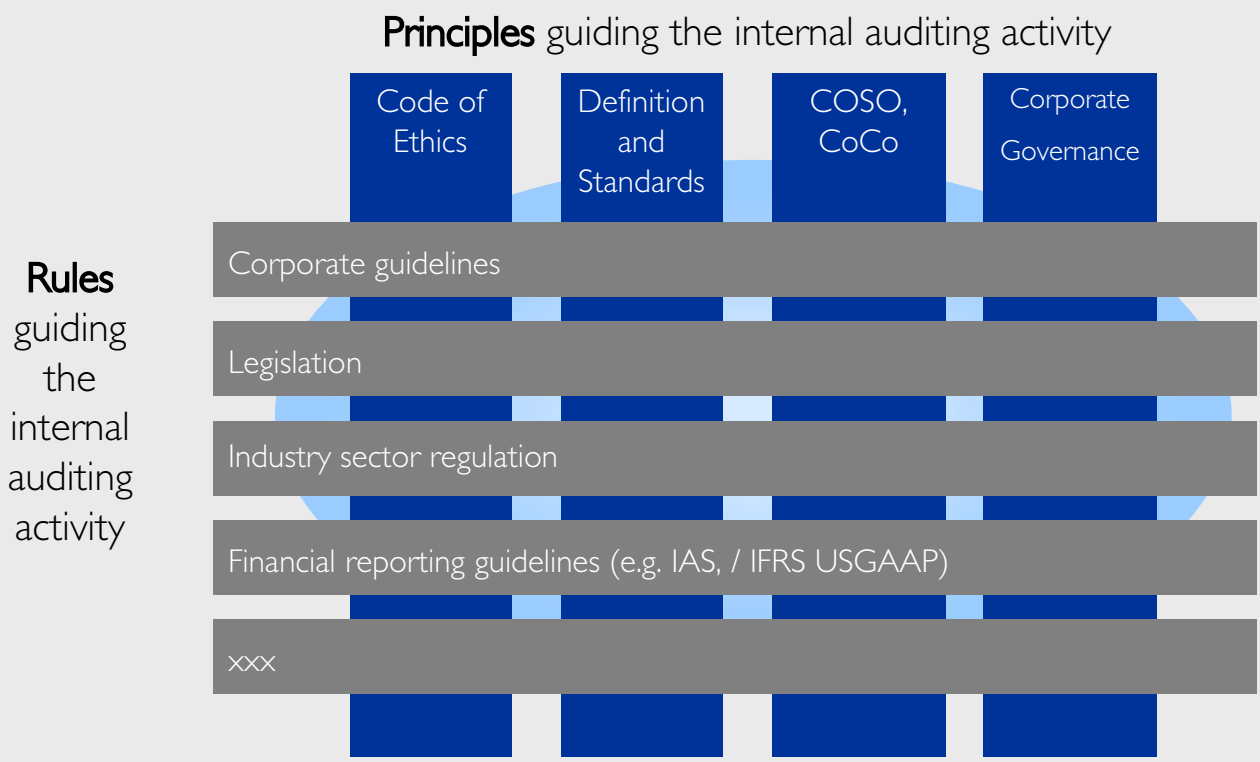
What speaks *against* more rules for the internal audit profession (cont'd)

- Too many rules bind internal auditors (= restrictions)
- Other potential assurance or consulting providers are free in delivering their services → competitive disadvantage
- Rules are particularly interesting for issues that have predictable characteristics
- Int. Audit deals far less with predictable "standard" issues
- Poor rules can have a negative impact on the performance, e.g., because they are not challenging enough or because they limit the 'radius' of action
- Internal auditors are professionals that are committed to the Code of Ethics and that are trained in critical thinking, they should be allowed a certain degree of autonomy
- Professionalism

„I think principles are more effective than rules, simply because it's easier to get around a rule than to get around a principle."

(Mervyn King, in: Barrier, M. (2003). „Principles, Not Rules", Internal Auditor, 08/03, p. 71)

Interacting dimensions



D-1
Audit Committee, management, internal and external auditors; self-fulfilment or interactive business support

Tom Palmberg (FIN)
Chairman of the Finnish Association of Professional Board Members

Audit Committee, management, internal and external auditors
–
self-fulfilment or interactive business support

Tom Palmberg
Chairman,
The Finnish Association of Professional Board Members

ECIIA Conference 2006
-
8 september 2006
Hilton Hotel, Helsinki

Structure of presentation

A *broad* perspective

A *board* perspective

DECEMBER 30, 2002 / JANUARY 6, 2003

SPECIAL DOUBLE ISSUE

PERSONS OF THE YEAR

TIME

The Whistleblowers

CYNTHIA COOPER
OF WORLDCOM

COLEEN ROWLEY
OF THE FBI

SHERRON WATKINS
OF ENRON

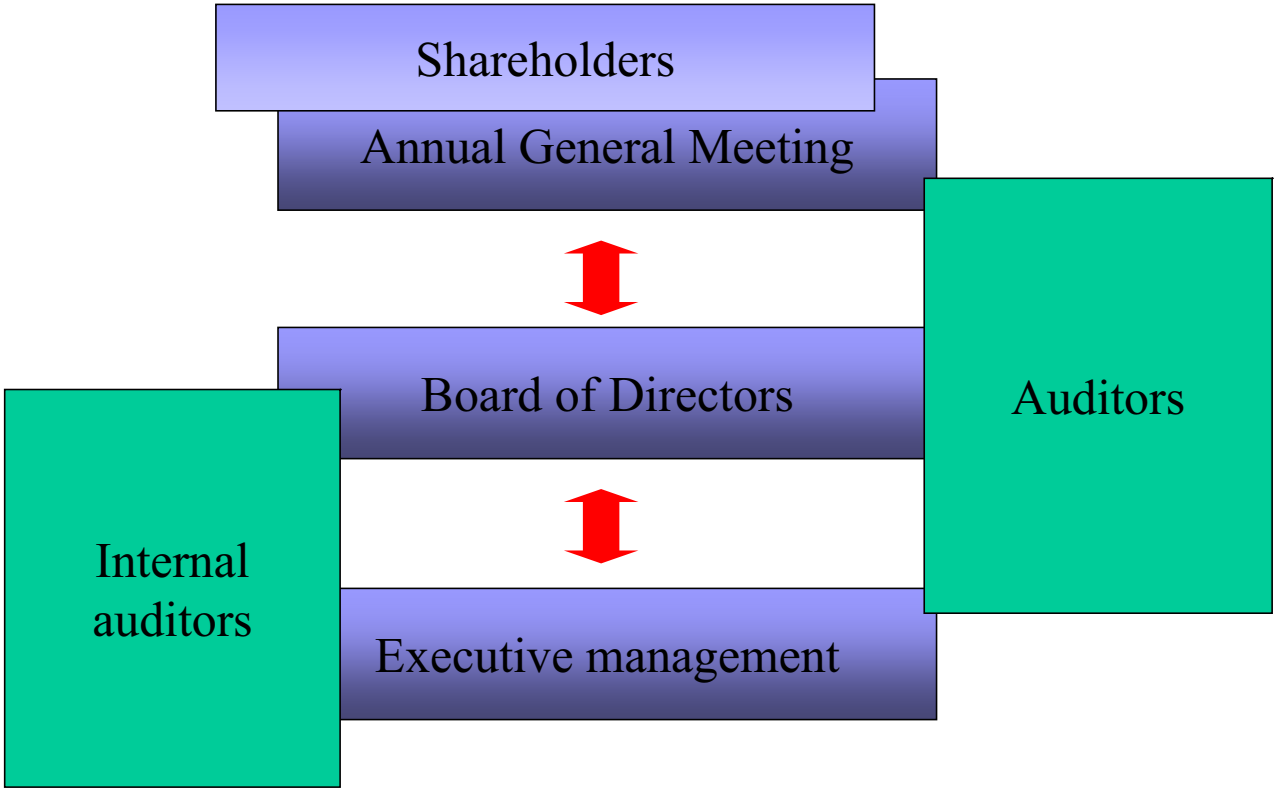
www.time.com AOL Keyword: TIME

The Corporate Governance regulatory environment

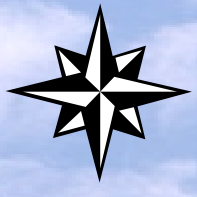
Country	Form of regulation	Background	Initiated by
United States	Legislation, Sarbanes - Oxley	Corporate scandals	The US Government
Sweden	National Code	Corporate scandals	The Swedish Government´s Code of Conduct Commission
United Kingdom	Combined Code	Improper conduct	The UK Government
Finland	National Code	Aspirations to increase transparency and to specify CG roles	Business Organisations (OMX, Chamber of Commerce, CFI)

Should Internal Audit become an integral part of corporate competitiveness?

Roles in Corporate Governance

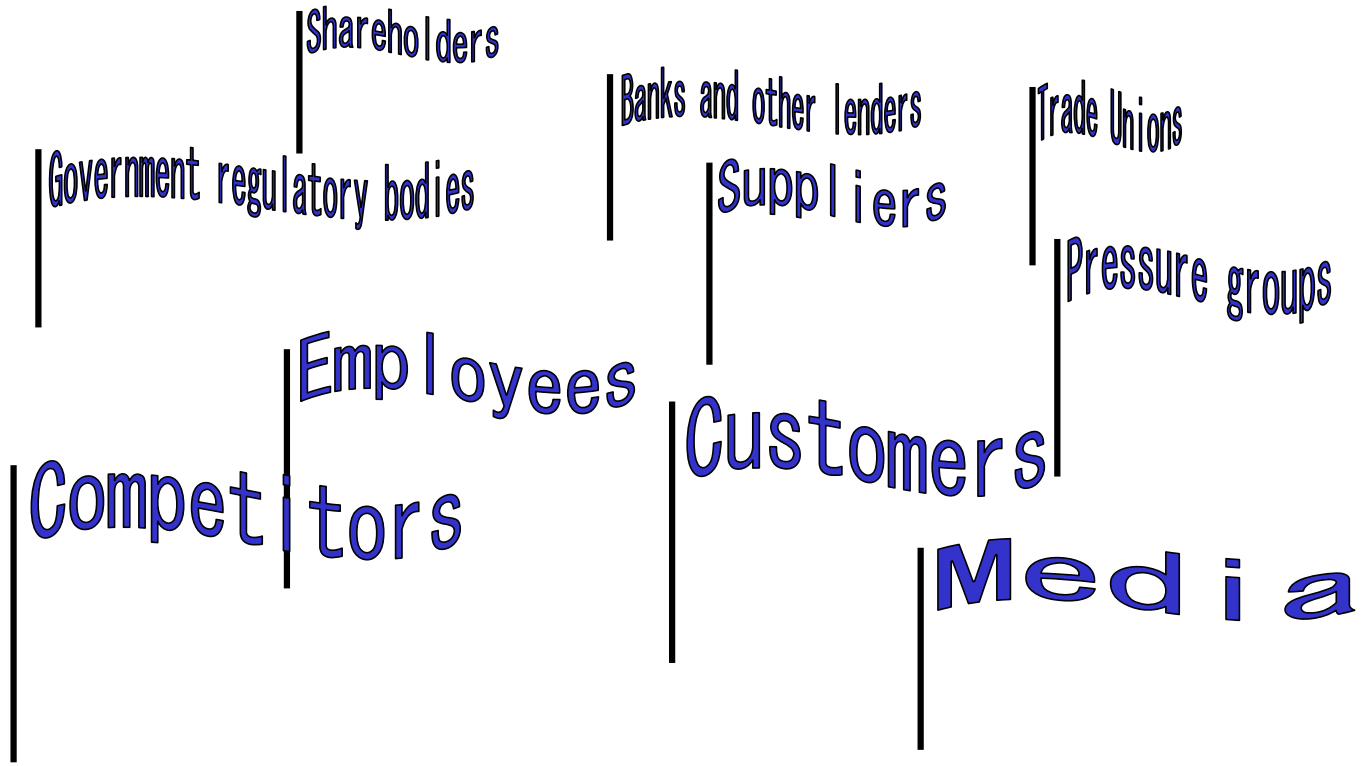


Corporate governance



means
the process and structure
used to
direct and manage the business
of the corporation with the objective of
enhancing shareholder value,
which includes
ensuring the financial viability of the business.
The process and structure define the
division of power and established mechanisms
for achieving
accountability
among
shareholders, the board of directors and management.
The direction and management of the business
should take into account the impact on
other stakeholders
such as
employees, customers, suppliers and communities

UNITED STAKES



Shareholders rights

A financial return,

normally in the form of a proportion of the company`s distributable profits

A right to transfer

their interest to another person

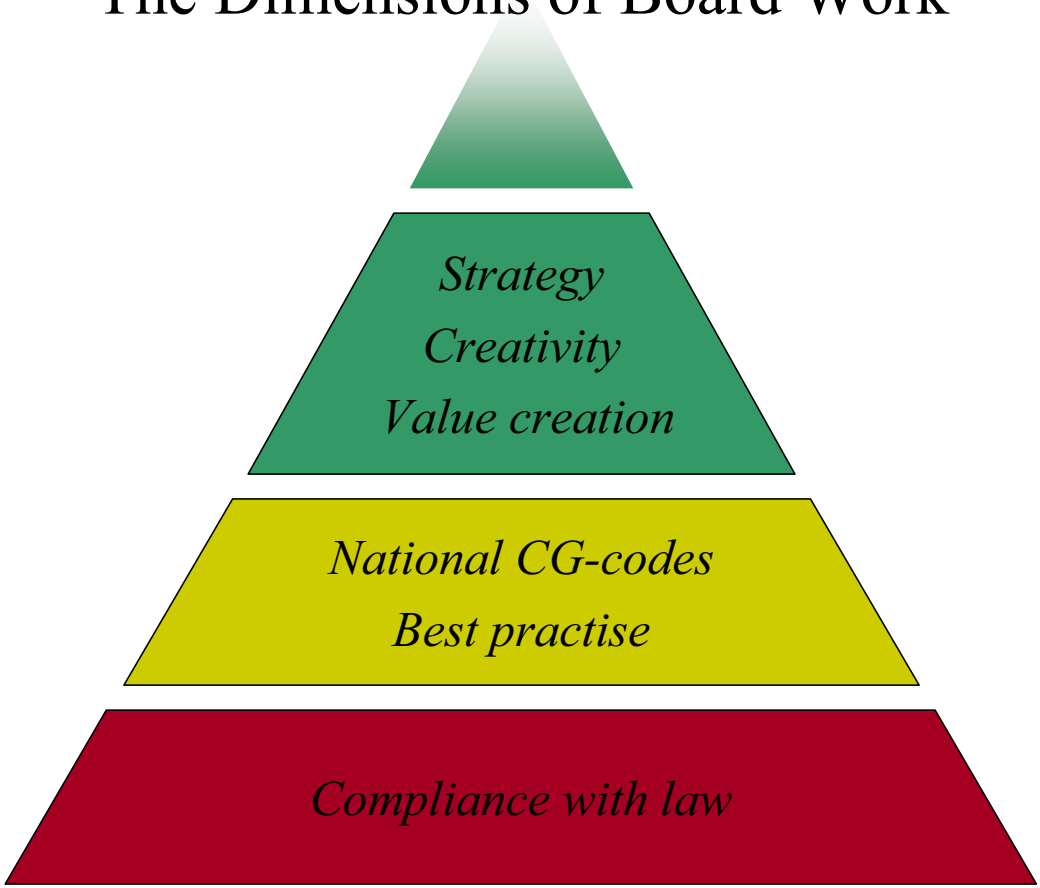
A right to vote

in general meetings

A right to demand information


OUR INTERNAL FINANCIAL REPORTING MUST BE RIGOROUSLY TRUTHFUL AND ACCURATE IF I'M TO LIE CONVINCINGLY TO THE SHAREHOLDERS.
ROGER BEALE

The Dimensions of Board Work



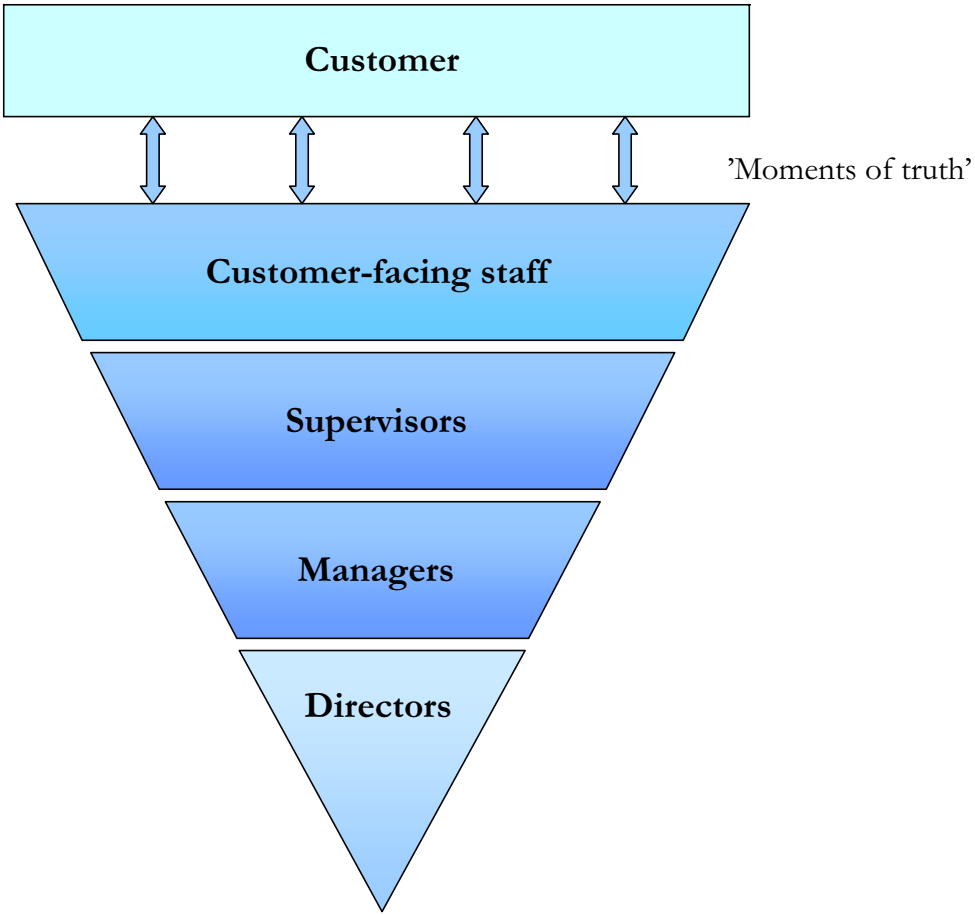
Main responsibilities of the Board

(IOD, London)

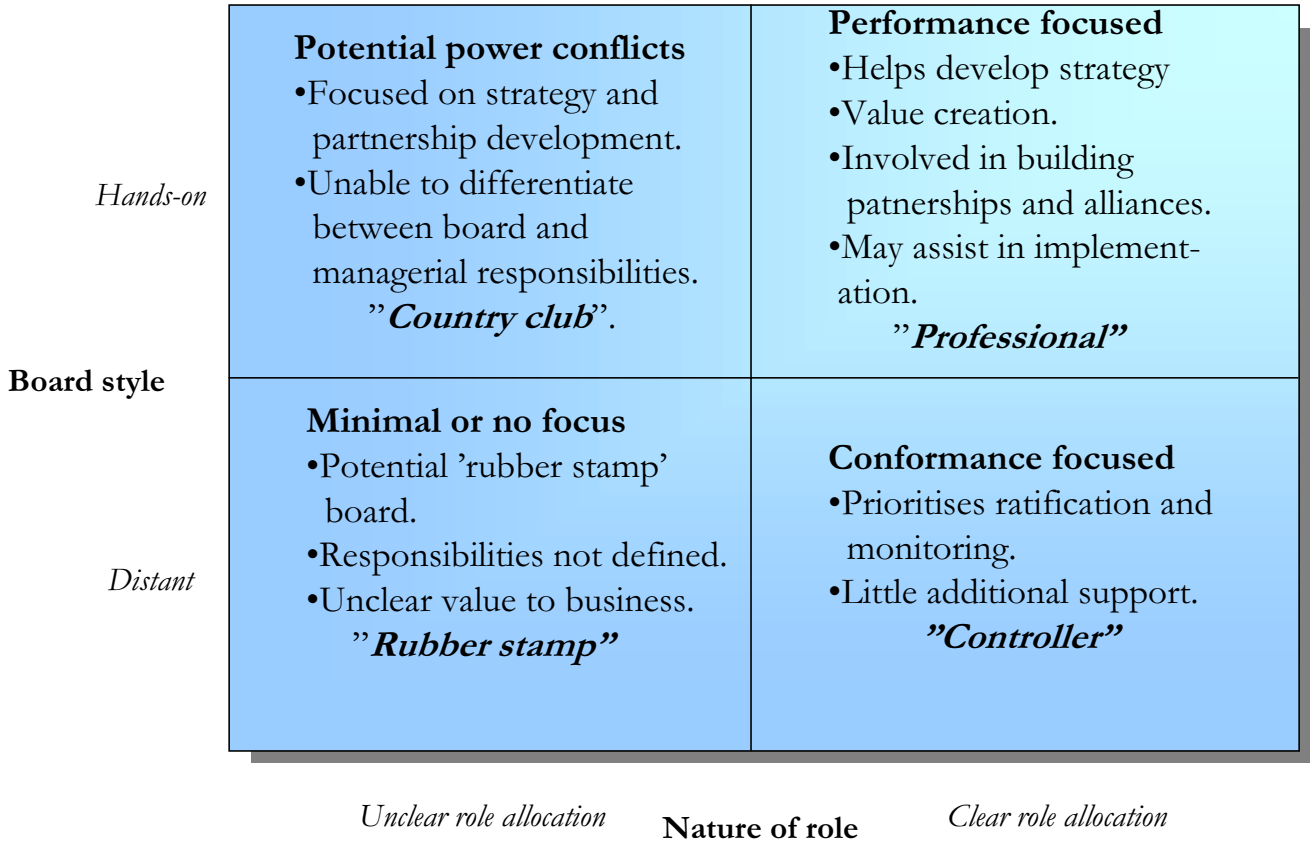
- **Determining vision, mission and values**
- **Determining strategy and structure**
- **Delegation to operative management**
- **Fulfilling responsibilities towards shareholders and other stakeholders**


The key purpose of the board
is to
ensure the company's prosperity
by
collectively directing its affairs
and
meeting the legitimate interests
of
its shareholders
and
other interested parties

The inverted organisation chart



The strategic foci of boards



Future challenges

(as presented by Jacob Wallenberg, Investor AB, 9.5.06)

- Explain executive pay
- Complexity
- Type of directors
- Board diversity
- Internationalisation

The Role of Internal Audit?

- Just Audit
- Audit and financial reporting
- Audit, financial and management reporting
- Risk monitoring
    - operational, financial, hazards, strategic
    - PUBLICITY !!! ???
- Implementation of board decisions
- Job rotation for business understanding

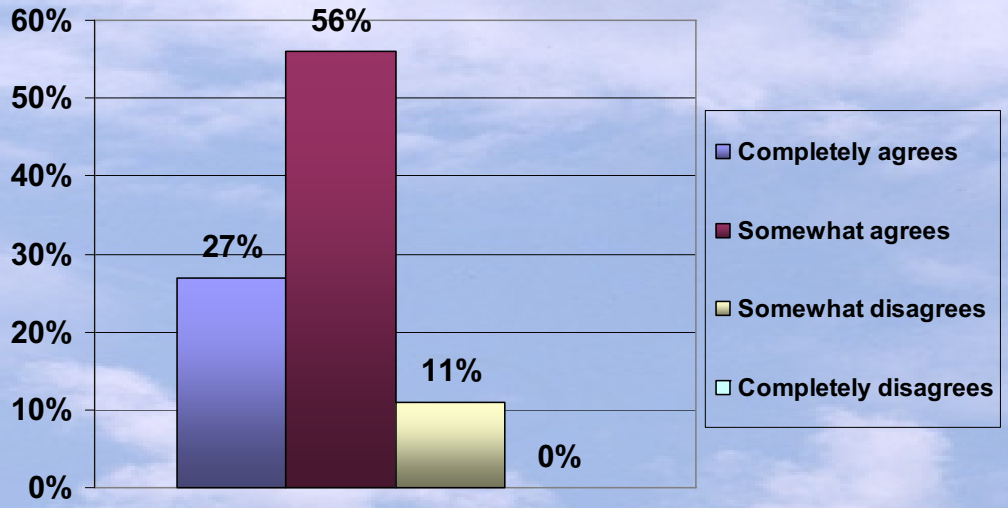
Implementing board decisions

The role of Internal Audit?

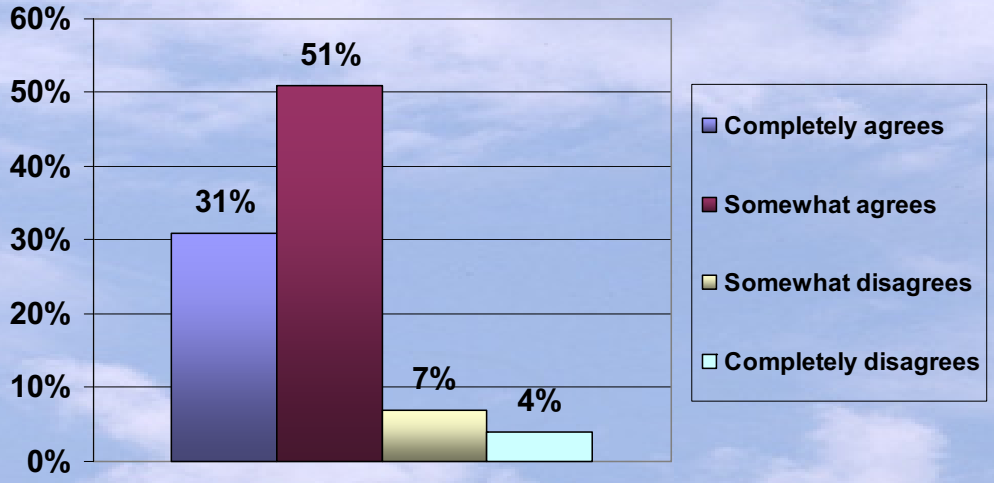
Board decisions into action

- Demand for implementation driven board minutes
- Introducing measurability
- Linking strategy implementation to incentive programmes
- Evaluating functionality of corporate ”bloodstream”

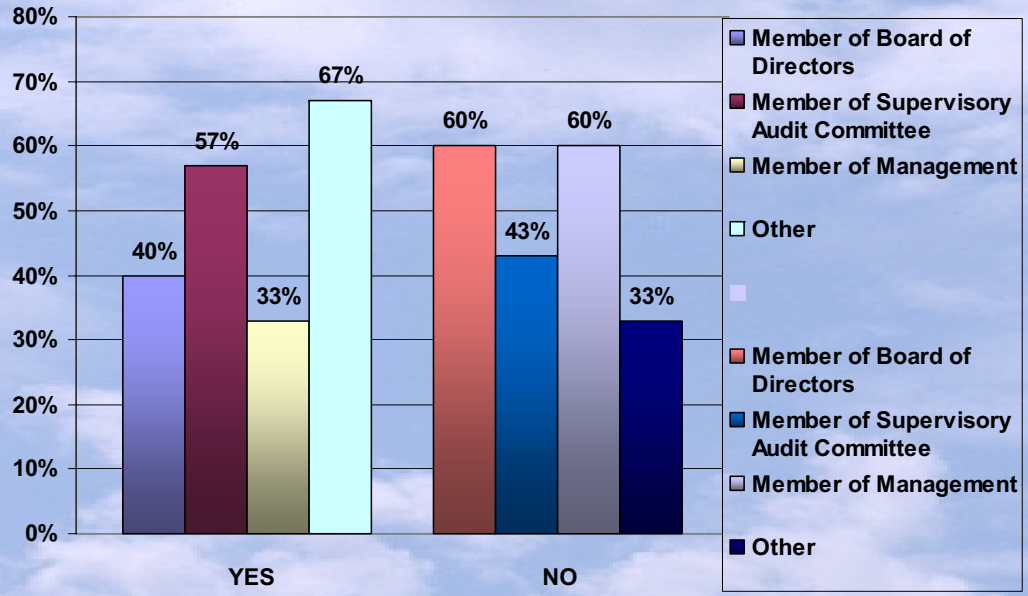
The Audit Committee has improved board work?



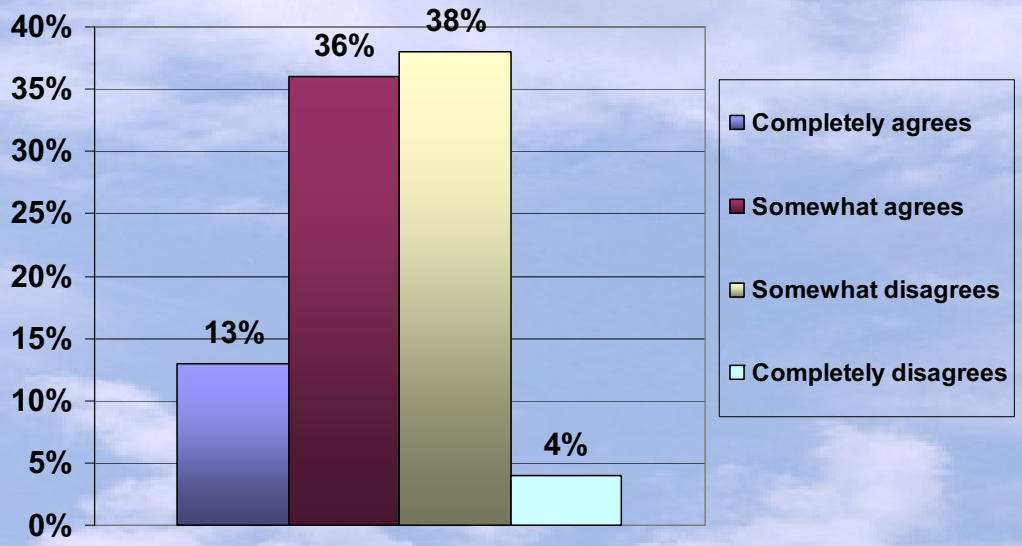
The Audit Committee has improved the directors´ duty to supervise the activities of the company?



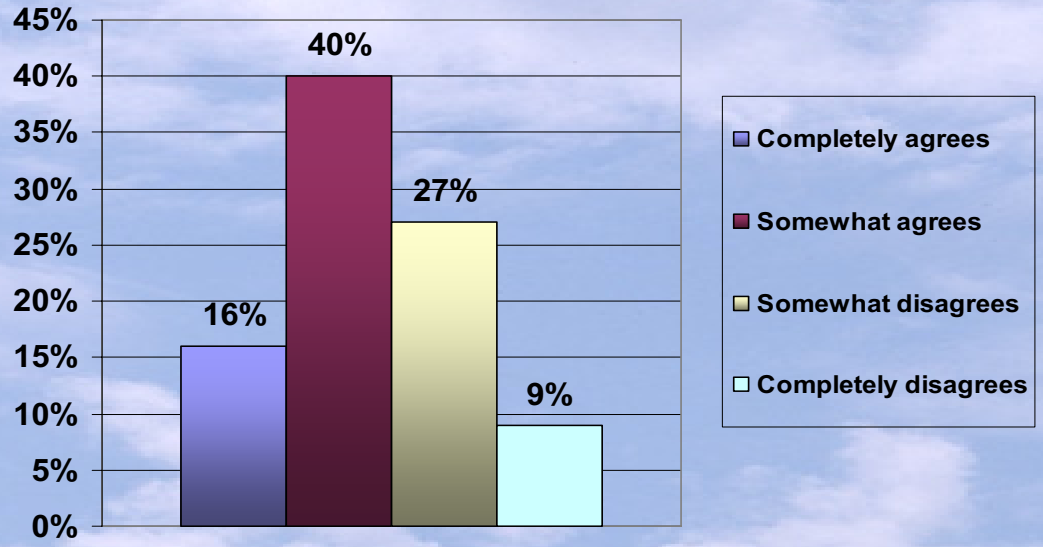
The Audit Committee should have properly experienced members even from outside the company?



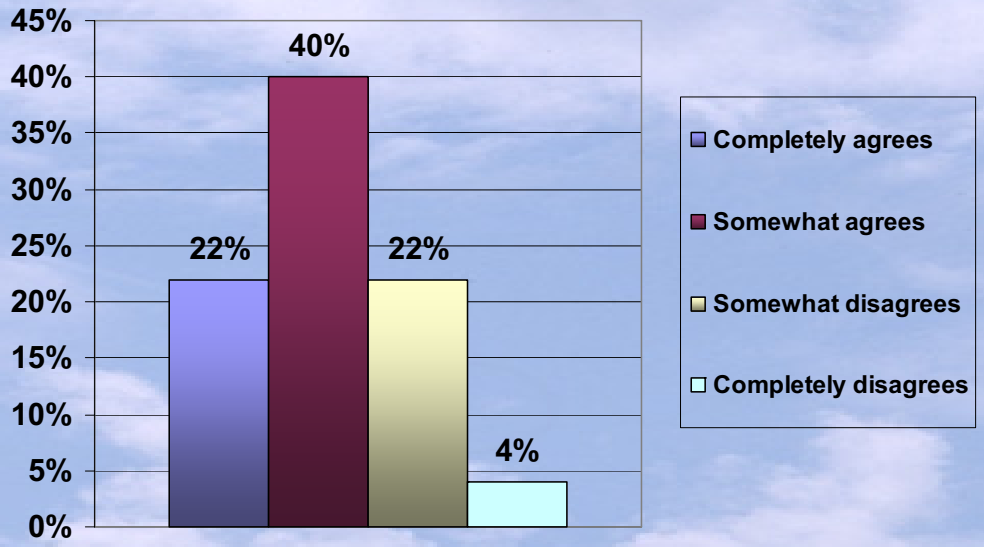
The Audit Committee has generated more work to management?



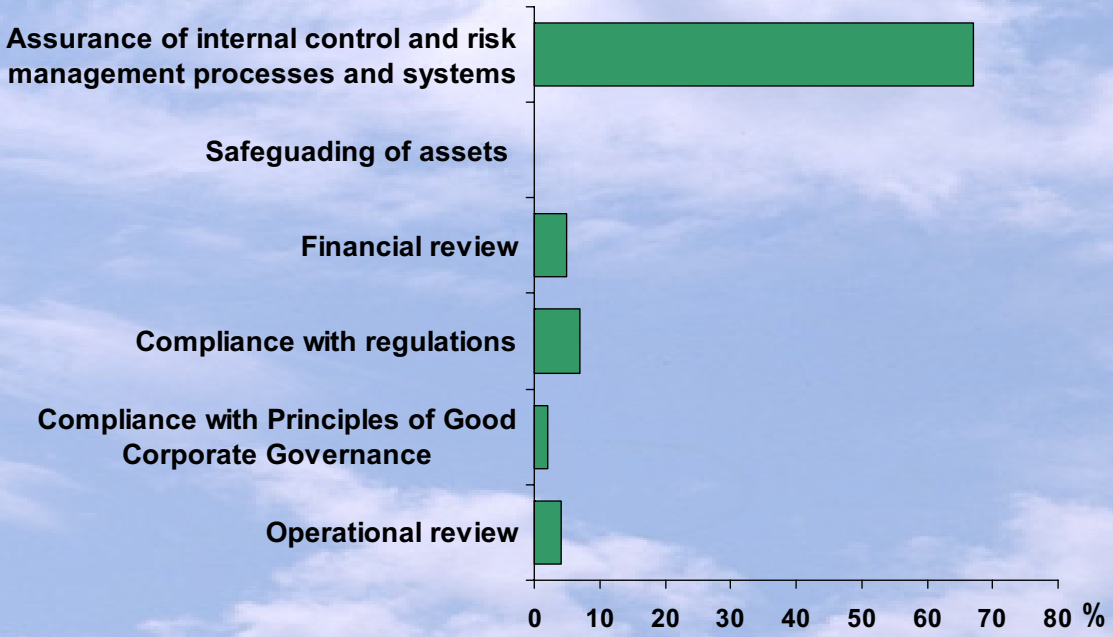
Supervising the financial performance of the company is a task for the Audit Committee?



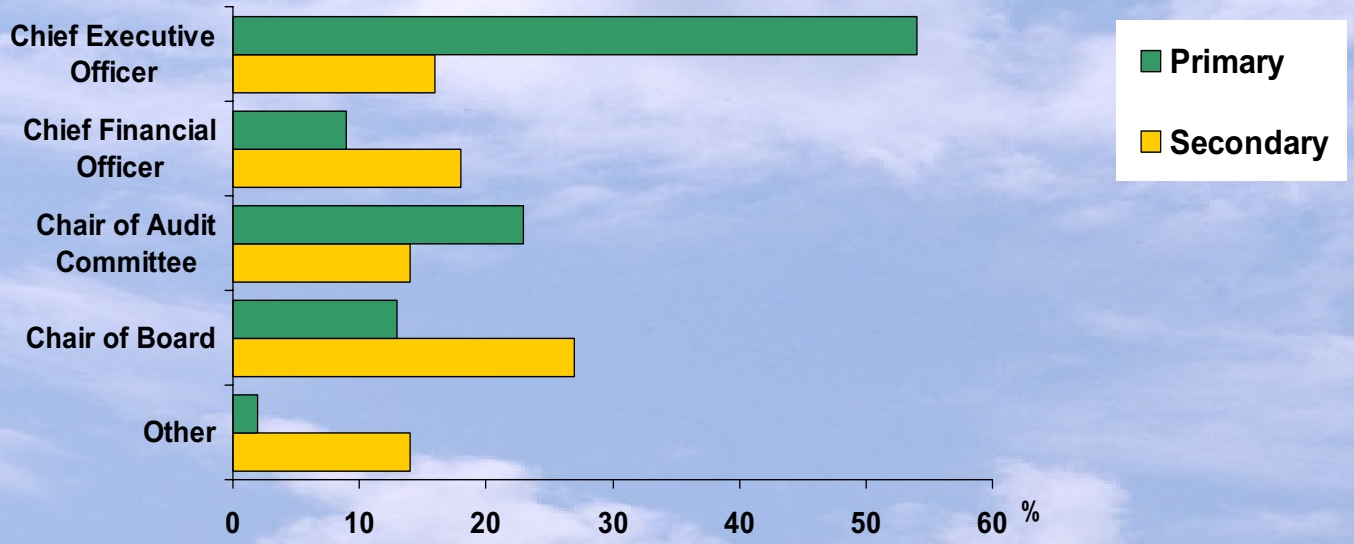
The Audit Committee has become the new ”master” for Internal Audit in addition to Management?



What is the primary role of Internal Audit in your organisation?

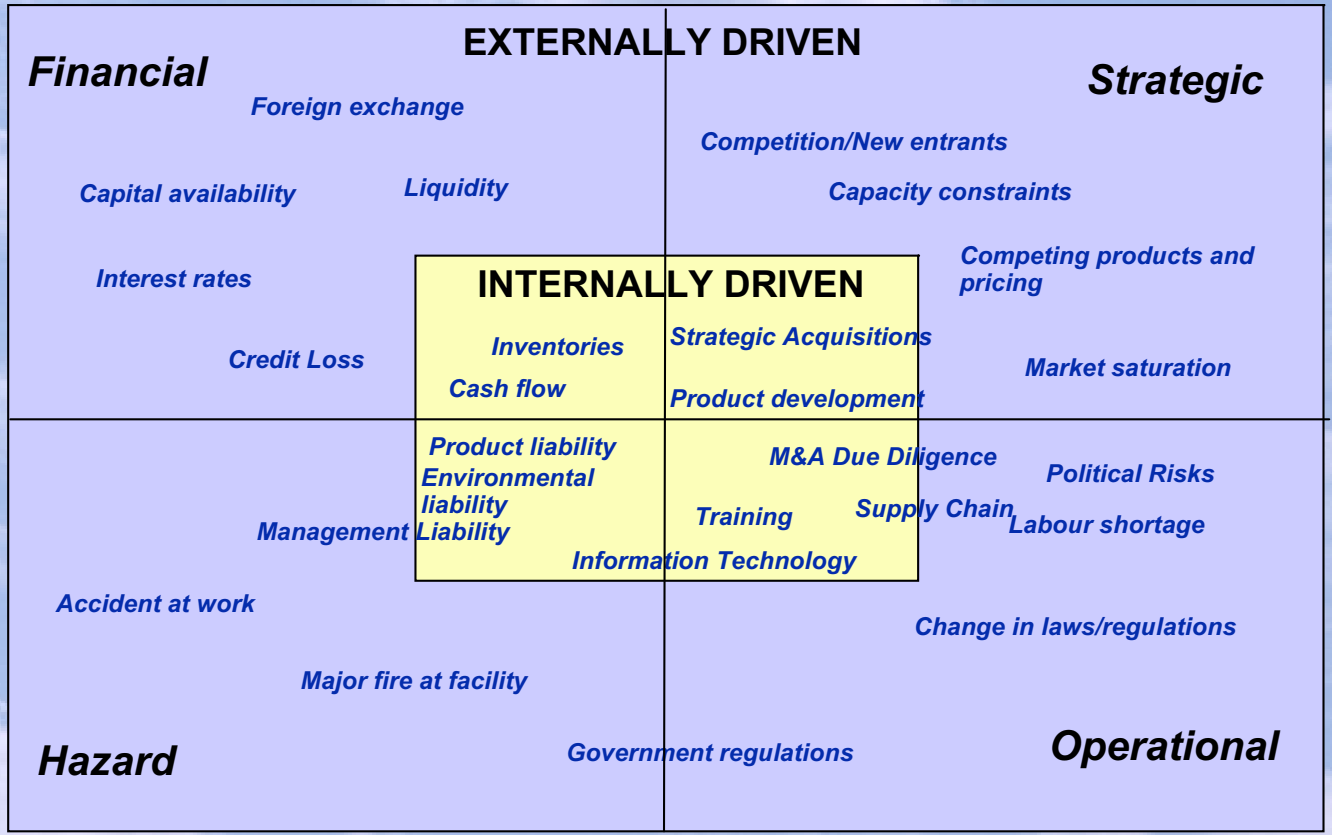


To whom does internal audit report?

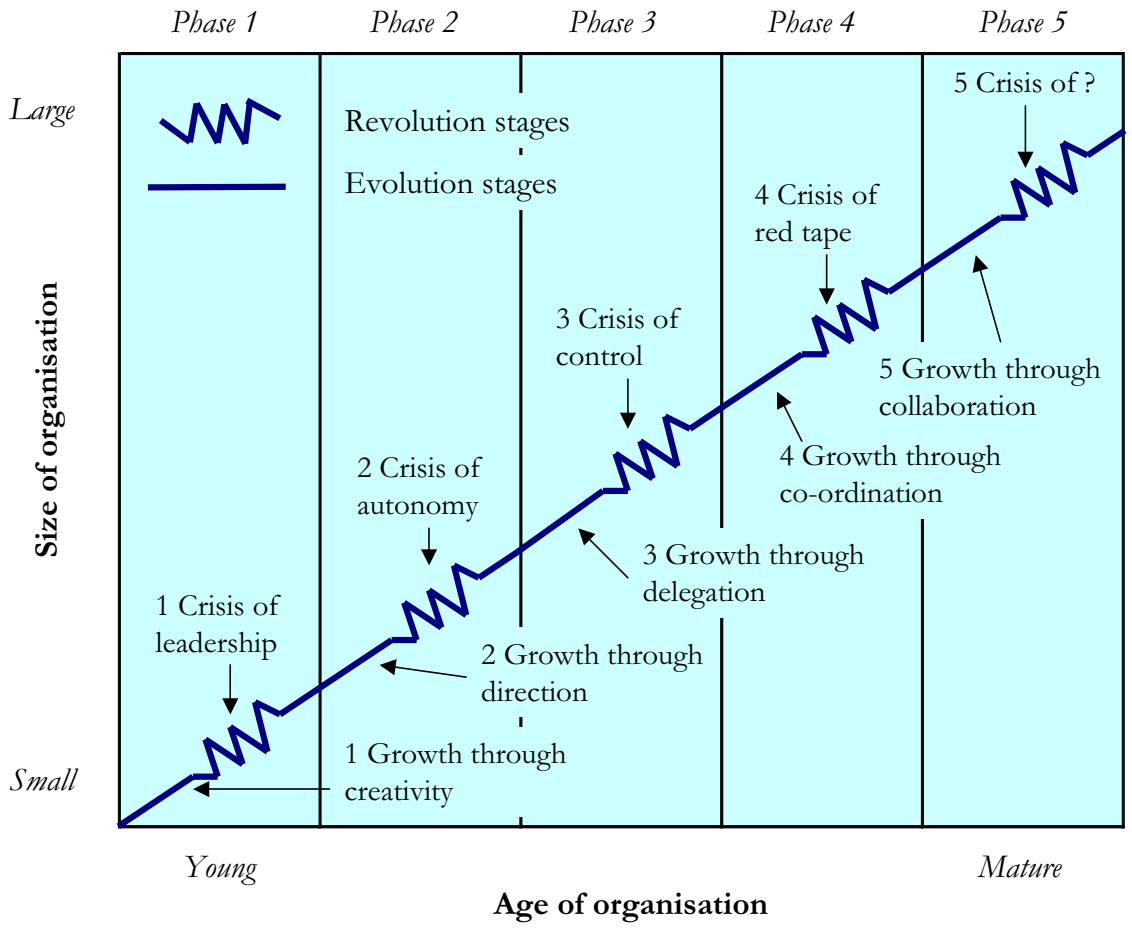


Which of the following best describes internal audit's involvement in risk management?

Risk mapping



Greiner's model of strategic change




Bon
Voyage

D-2
Internal Marketing of Internal Auditing

Stanko Tokić (CRO)
Director
Hrvatska Elektroprivreda d.d.

ECIIA
HELSINKI, 8 September 2006.

INTERNAL MARKETING OF INTERNAL AUDITING

Helsinki, 6-8 September 2006.

Stanko Tokić, HEP group, Manager Internal Audit
President of Croatian Institute of Internal Auditors
ZAGREB, CROATIA

CONTENTS OF PRESENTATION

1. Croatian Institute of Internal Auditors (IIA Croatia)
2. Key data on Croatian Electricity Company (HEP)
3. Internal Marketing and Internal Auditing
4. Internal Marketing of Internal Auditing
5. Internal Marketing process
6. Internal Marketing in Internal Audit process
   - Planning Internal Audit
   - Examining and evaluating information
   - Communication and reporting results
   - Follow up

7. CONCLUSIONS

What is marketing?

'A wise man makes more opportunities than he finds'.

Francis Bacon

Why Market Internal Audit?

'When a man knows he is to be hanged in a fortnight, it concentrates his mind wonderfully.'

Dr Johnson


Iceland
Finland
Norway
Sweden
Estonia
Russia
Latvia
Danemark
Lithuania
Ireland
United Kingdom
Belarus
Netherlands
Poland
Belgium
Germany
Czech rep.
Slovakia
Ukraine
Austria
Hungary
Moldova
France
Switz.
Slovenia
Romania
Croatia
BiH
Italy
Bulgaria
Macedonia
Albania
Spain
Portugal
Greece
Turkey
Cyprus

CROATIAN INSTITUTE OF INTERNAL AUDITORS

- Croatian Institute of Internal Auditors was founded in June 2006
- Internal Auditors in Croatia — cca 1000
- Members of the Institute (IIA) 2005 — 25 members
- Potential of Croatia:
  - Members of the Institute (IIA) 2006 — 100 members
  - Members of the Institute (IIA) 2007 — 500 members
  - Growth of new members per year cca 5-7% in the next five years
- Croatian National Association of Internal Auditors was organized in 1998
  - Members of Association — 300 members
  - Annual Conferences 1998-2006 — 9

MISSION AND VISION OF CROATIAN ELECTRICITY COMPANY (HEP)

- **MISSION**

  Secure and reliable electricity supply at minimum costs

- **VISION**

  An integrated corporation becoming a regional market player, a Croatian energy cluster - a group of related businesses, with multi-utility approach, one of the main driving forces of Croatia's economic development

CROATIAN ELECTRICITY COMPANY (HEP)
COMPANY PROFILE

- Croatian Electricity Company (HEP) was established in 1895 (1990 reunion)
- Croatian Electricity Company is state owned shareholding company and organized as a Group in accordance with the Croatian legislation and
- HEP is National Electricity Company with monopolistic position and vertically integrated businesses: Generation, Transmission and Distribution
- Core business – generation, transmission, distribution and supply of electricity, gas and central heating
- Generates 98% of its own energy through thermal, hydro and nuclear power plants
- HEP group is doing business in accordance with EU directives

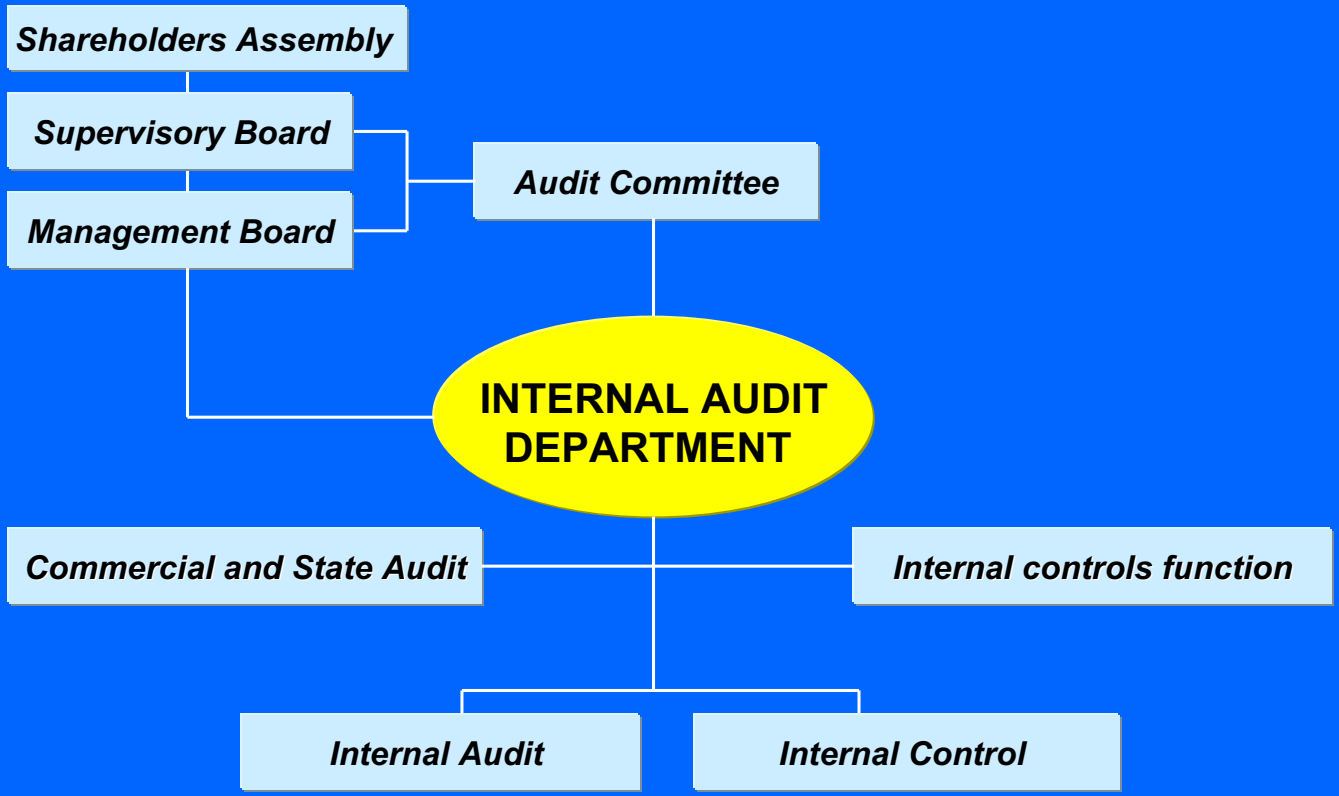
CROATIAN ELECTRICITY COMPANY (HEP)
KPI's

Installed capacity	3650 MW
Peak load	2565 MW
Total consumption	14 TWh
Net book value	Euro 3.4b
Total revenue	Euro 1.3b
Operating income	cca Euro 1.0b
Net profit	0.6% of turnover
Employees	14,700
Assets	Euro 7.0b
Investments per year	Euro 0.4b
Consumers	2.3m
Annual growth of consumption	4-6% per year

ORGANISATION, REGULATION AND STRUCTURE OF INTERNAL AUDIT

- Internal Auditing Department was founded in 1995
- Internal Audit Department is organized in accordance with Internal Audit Standards, Guidelines, Best Practice, Code of Ethics, etc.
- HEP group Internal Audit Charter defines Internal Audit
- Professional framework for internal audit in HEP
  - on HEP level: charter, statute, acts, plans, guidelines, regulations, etc.
  - on Internal Audit level: handbook for internal auditors, brochure, leaflets, standard working papers, etc.
- Internal Audit Strategic and Annual plan includes plan of Internal Marketing of Internal Auditing
- Internal Audit reports on implementation of Internal Marketing of Internal Auditing, on annual basis

ORGANISATIONAL SCHEME OF INTERNAL AUDIT DEPARTMENT



INTERNAL MARKETING OF INTERNAL AUDITING

- Some questions on Internal Marketing of Internal Auditing:

  - Why do we need Internal Marketing of Internal Auditing?
  - What is the relationship between Internal Marketing and Internal Auditing?
  - Why do we promote Internal Audit when it works represive and is a source of informations for restrictions?
  - Who uses Internal Audit reports and Internal Marketing results?
  - How can we manage with Internal Marketing of Internal Auditing throught Internal Audit process?
  - How we can improve Internal Audit activities with Internal Marketing?
  - Why Internal Auditors do not accept Internal Marketing if it can help them in their work?
  - Why should we need to have Internal Marketing and sell our services even though Internal Audit exists in the company?
  - Why do we need to improve Internal Auding process?

INTERNAL MARKETING

- Main contributions of Internal Marketing of Internal Auditing can be:
  - transparency of business – an independent, objective assurance and information about the company
  - consultants services provide information Internal Marketing and Internal Auditing
  - create additional value and improve company business
  - efficiency and effectiveness of business
  - impact on market position and image
- Internal Marketing of Internal Auditing protects shareholders
- Internal Marketing of Internal Auditing improves management system and process
- Internal Marketing of Internal Auditing helps to create objective and real information and date for decision making
- Internal Marketing of Internal Auditing helps in better communication with clients and users within the company

INTERNAL MARKETING

- Internal Marketing of Internal Auditing has major influence on efficiency and effectiveness of Internal Auditing
- Internal Marketing and Internal Audit are one of management functions, instruments or tools
- Internal Marketing defines strategies, plans, objectives and goals of Internal Audit
- Internal Marketing has to be in the focus of Internal Audit management and auditors
- Internal Marketing helps to define programms, plans, tasks, goals, etc. for Internal Audit process and support better communication between Auditors, management, auditees, clients, users, experts, etc.
- Internal Audit findings and reports serve as instruments for the management
- Internal Audit prepares realistic and transparent picture of the business
- The task of Internal Marketing of Internal Audit is to promote the company

INTERNAL MARKETING

- Internal Marketing of Internal Auditing has to be in accordance with strategy, plans, goals, etc. of Internal Audit and the company
- Internal Marketing plan for Internal Auditing has to have the main tasks as the company and separate for Internal Auditing
- Each plan of Internal Audit has to have the Internal Marketing part
- Many companies have an organisational part or staff, within the Internal Audit, who are in charge of Internal Marketing
- Internal Marketing of Internal Auditing supports achieving goals and objectives of Internal Auditing and the management process
- Internal Marketing provides good opportunity for the Internal Audit to express the initiatives of staff and management - communication, improvement, implementation, etc. for the company

RELATIONSHIP BETWEEN INTERNAL MARKETING AND INTERNAL AUDIT?

- Relationship between Internal Marketing and Internal Audit can be considered through the definition of Internal Marketing and Internal Auditing

- Internal Marketing - The application of marketing internally within the company, with programmes of communication and guidance targeted at internal audience to develop responsiveness and an unified sense of purpose among employees

- Internal Auditing - is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes

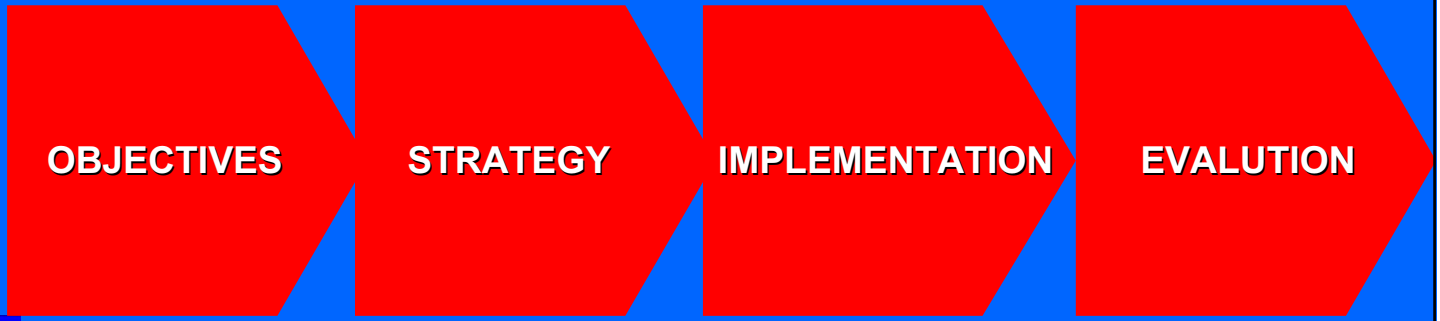
INTERNAL MARKETING

- Internal Marketing vs. External Marketing:
  - have the same rules, principles, structure, similar processes, phases, steps, etc.
  - have the same customers or clients: management, users, clients, staff, experts and colleagues within the company
  - main differences are in the field of work - Internal Marketing is present in the company or in part of the company,whereas External Marketing is broader (whole company, business group, branches, economy, etc.)
  - Internal Marketing assists every business function, such as Internal Auditing and vice versa

INTERNAL MARKETING

- Process of Internal Marketing:

1. Objectives (define objectives)
2. Strategy of Internal Marketing
3. Implementation (persuasion, negotiation, politics, tactics)
4. Evaluation (results, efficiency and effectiveness, etc.)



INTERNAL MARKETING

- Internal Marketing process can be devided in five (5) steps – AOSTC – Analysis, Objectives, Strategies, Tactics, and Control – Jobber (1995)
  - Analysis (analyse Internal Auditing and Internal Marketing)
  - Objectives (set objectives for Internal Marketing of Internal Auditing)
  - Strategies (define strategy for Internal Marketing of Internal Auditing)
  - Tactics (application of marketing mix, marketing forum, staff, presentation, intranet, personal visits, newsletters
  - Control (evaluate internal marketing process and results)

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Marketing of Internal Auditing must be oriented on all users (internal or external) of Internal Auditing findings and reports:
  - Internal - Internal Audit is primarily oriented on the management within the company and company's bodies, committees, etc. (Supervisory Board, Management Board, Audit Committee), clients, users, other committees, etc.
  - External - External users can use Internal Audit results directly or indirectly, through Annual Report, Business Reports, Financial Reports, Information, Benchmarking analyses, special issues of Management Board and Supervisory Board

INTERNAL MARKETING OF INTERNAL AUDITING

- Results of Internal Marketing of Internal Auditing can be used by the following external parties:
  - Government, ministries, government agencies, etc.
  - Non-governmental bodies, agencies, regulatory bodies, legislative bodies
  - Banks and creditors
  - Buyers
  - Funds
  - Stock exchanges
  - Commercial & State Audit
  - Consultancy services

- External clients and third parties have influence and important function in defining Internal Marketing of Internal Auditing

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Marketing of Internal Auditing brings good climate within the company
- Good climate is very important for all staff in auditing process
- Internal Marketing and Internal Auditing are primarily oriented on internal clients and users:
  - Supervisory Board
  - Management Board
  - Audit committee and other committees
  - Other business functions within the Company
  - Clients, users, colleagues, experts, etc.

INTERNAL MARKETING OF INTERNAL AUDITING AND ITS USERS

INTERNAL MARKETING OF INTERNAL AUDITING

- The means, instruments or tools of Internal Marketing include many activities, papers, reports, presentations, workshops, web sites, intranet, company newsletters, gazettes, articles, researches, projects, personal contacts, activities of internal auditors within the Institute, etc.

- HEP group Internal Audit Department has carried out several activities of Internal Marketing in the last six years:

  - Professional framework
  - Research, projects
  - Seminars, Trainnings, Presentations, Workshops Conferences, Congresses, etc.
  - Web site and Intranet
  - Articles and personal contacts

INTERNAL AUDITING OF INTERNAL AUDITING

- Professional framework for Internal Auditing consists of projects on Internal Auditing, system of internal controls, risk management, etc.

- Projects:
  - Projects with consultants to establish Internal Audit function in HEP
  - Projects on planning Internal Audit
  - Projects on Internal Auditing process
  - Projects regarding working papers
  - Projects on Risk Management

- Professional Framework:
  - Manual for internal auditors
  - Guidelines for internal auditors
  - Plans and Reports of Internal Audit
  - Working papers – standard working papers, etc.

- Internal Marketing – leaflets, brochures, papers:
  - Internal Auditing function
  - Internal Auditing process
  - Internal Control System and Internal Controls
  - Risk Management and Internal Audit

INTERNAL MARKETING OF INTERNAL AUDITING

- Seminars, Presentations, Workshops, Conferences, Congresses, etc. in last five years:
- Presentations:
  - Management presentations (40) on Internal Audit, on general level (cca 850 participants)
  - Presentations (12) on the System of Internal Control (cca 300)
  - Presentations (10) on Risk Management and Risk Based Approach of Internal Auditing (cca 200)
  - Presentations (4) on main findings and results of Internal Auditing to Audit Committee and management on annual basis

INTERNAL MARKETING OF INTERNAL AUDITING

- Seminars:
  - Seminars (21) in three cycles for HEP experts (1250 participants) in four years
  - Seminars (5) on Risk Management (200)
  - Seminars (4) on System of Internal Control (100)
- Workshops:
  - Workshops (8) for experts on Internal Auditing Process (90)
  - Workshops (4) on System of Internal Control (60)
  - Workshops (4) on Risk Management (80)
- Internal Auditors attend Conferences, Congresses, presentations, workshops, trainnings, etc., in Croatia and abroad

INTERNAL AUDIT

- Internal Audit has to get reliable and precise information which can be used by the management and Internal Marketing in decison making and managing process
- Internal Audit and Internal Marketing must create additional value or benefit
- Internal Audit has influence on the quality of Internal Marketing and vice verse
- Internal Audit tasks, scope, objectives and goals have to be in accordance with the strategy and program of Internal Marketing
- Business Performance affects tasks, scope, objectives and goals of Internal Audit and Internal Marketing
- Internal Audit cooperates with Internal Marketing function in the company but Internal Marketing, as an audit object, can be audited by the Internal Audit

INTERNAL MARKETING OF INTERNAL AUDITING

- Web site, Intranet, etc.
  - Web site of HEP group
  - Web site of Croatian Institute of Internal Auditors
  - HEP Intranet site
  - Intranet site of Internal Audit Department
  - Communicating with and reporting to clients and the management via HEP Intranet
  - HEP Intranet site on Risk Assessment and Management

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Marketing and Internal Auditing should be orientated on external users and provide findings, reports, information, analysis, data, such as:
  - External users can use findings and reports of Internal Auditing directly or indirectly
  - Internal Audit Reports in Annual Business Reports for the Management and the Supervisory Board
  - Internal Audit Reports, Annual Audit Reports, Reports of External and State Audit on the Internal udit, system of internal controls, Risk Management, etc.
  - Internal Audit provides consultancy services within the company regarding restructuring, privatisation, deregulation, etc.
  - Management and Supervisory Board should be informed on facts regarding Internal Audit, System of Internal Controls, etc. and report to Government, Ministry, Non-Government and Government organisations, bodies, agencies, etc.

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Auditing should improve Internal Auditing process every year
- Internal marketing can help Internal Audit in each phase of its auditing process
- In each phase of Internal Auditing process internal auditors must use information on plans, tasks and targets of Internal marekting
- In accordance with the Internal Auditing guidelines should be performed statutory an external analysis every three years on its results
- Internal Audit can be replaced by outsourced services
- Internal Audit gives benefits to the company or additional value
- Internal Auditors should know the values of effective governing process and the contribution of Internal Marketing

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Marketing of Internal Auditing can be considered through the Internal Auditing process:

1. Planning Internal Audit – plan of auditing should be in accordance with the Internal Marketing plan and Internal Auditing goals and objectives

2. Examining and evaluating information – auditors must carry out the audit and achieve goals and objectives

3. Communication and reporting – is a very important phase and a result of previous steps in the auditing process

4. Follow-up – monitoring of implementation of audit findings and results

INTERNAL MARKETING OF INTERNAL AUDITING

Planning Internal Audit

- Plan of Internal Audit has elements of the plan of Internal Marketing
- Internal Marketing has to be involved in each part and step of internal auditing process performed by auditors:
  - Annual Plan of Internal Marketing is a part of Internal Auditing
  - Internal Audit prepares Risk Assessment which management must consider with Internal Marketing targets
  - Internal Auditing and Internal Marketing collect information
  - Internal Auditing and Internal Marketing exchange information, data, etc. with clients, users, management, etc.
  - Internal Auditors communicate and send letters of intent to auditees, CEO and management
  - Internal Auditors prepare working papers for field work in accordance with the auditing tasks and Internal Marketing

INTERNAL MARKETING OF INTERNAL AUDITING

Examining and evaluating information

- In this phase of Internal Marketing field work, a good Internal Auditing process includes:
  - Realisation of the audit plan in order to achieve main targets, goals and objectives
  - Cooperation with management and staff of auditees during the field work
  - Communication with experts and clients within the company (Internal Audit involves experts (cca 50) from HEP group per year
  - Collecting information on objects of Internal Auditing and the plan of Internal Marketing
  - Examining and evaluating information and defining evidence, findings, conclusions, recommendations of Internal Auditing etc. and comparing these with the plan of Internal Marketing

INTERNAL MARKETING OF INTERNAL AUDITING

Communication and reporting

- In the communicating and reporting phase, the Internal Audit presents results of previous phases and the complete auditing process:
  - Internal auditors should communicate with management and clients in accordance with the task of Internal Auditing and Internal Marketing
  - Internal audit communication and reporting can be in the form of consultations, advice, recommendations, proposals
  - Internal auditors have to communicate with and continuously report to the clients, auditees, users and the management
  - Manager of Internal Audit Department periodically reports to the Management Board and the Audit Committee, on the results of audit activities e.g. corporate governance, risks, system of internal controls, compliance with regulatory framework, next steps, etc.
  - The results of Internal Auditing for Internal Marketing depend on the quality of communication and reporting system - vertical and horizontal information system within the company

INTERNAL MARKETING OF INTERNAL AUDITING

Follow-up activities

- Follow-up activities represent a very important phase in which auditors can get feedback for Internal Audit and Internal Marketing
- Follow up activities include realisation and implementation of Internal Auditing reports or results
- Follow up activities are interactive process between auditors, auditiees, clients, management and users of Internal Audit reports
- Management is responsible for implemention of Audit reports
- Internal auditors must monitor the implementation and the Internal Audit report and Manager should periodically report on the implementation results
- In this phase, Internal Audit must achieve Internal Marketing plan
- Internal Marketing of Internal Auditing can use information drawn from audit reports for subsequent tasks and plans

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Auditors do not accept very often Internal Marketing if it can help them in their work. Why?:
  - Internal Auditors don't understand the function of Internal Marketing
  - Internal Auditors don't know how they can use Internal marekting
  - Internal Auditors don't know what Internal Marketing can offer and help them to achieve the tasks and goals of Internal Auditing

  - Many Internal Auditors nowdays don't know that Internal Audit is exposed to threats :
    - Management can use outsourcing
    - Commercial audit ca carry out internal auditing
    - Management can use other business functons within the company
    - Internal Audit can be performed by other individuals
    - Management can deny the need for Internal Audit

INTERNAL MARKETING OF INTERNAL AUDITING

- Internal Auditing must be competitive business function in the company and play very important role in the company:
  - improve management system and process and company business
  - gives an independent, objective assurance and information
  - create additional value
  - assurance provider, risk consultant
  - gives consultations, advice, recommendations, proposals
  - provide consultants services on Internal Marketing
  - improve image of the company and impact on market position

- Internal Audit looks into the satisfaction of its clients, users and management on annual basis
- The check list includes contribution and improving satisfaction of clients and management on Internal Audit
- This checklist helps internal auditors to sell their services better and to increase the internal audit value and productivity

CONCLUSIONS

- Internal Marketing of Internal Auditing is a very important activity for efficiency and effectiveness of Internal Audit in the company
- Internal Marketing of Internal Auditing promotes and improves Internal Audit and company's image
- Internal Marketing of Internal Auditing contributes to the management process and system and the process of decision making
- Internal Marketing and Internal Auditing are oriented on the management system and process and the business process
- Internal Marketing is a part of Internal auditing activities throughout the year
- Internal Marketing and Internal Auditing have the same tasks in accordance with the company's strategy and its audit and marketing plan
- Internal Marketing can support Internal Auditing but it can also be audited by the Internal Audit
- Internal Auditing quality depends of the quality of Internal Marketing and vice versa

ANY QUESTIONS

D-3
Essential Interpersonal skills during the internal audit process

Carolyn Ditmeier (ITA)
Chief Audit Executive
Poste Italiane

Essential Interpersonal Skills during the Internal Audit Process

8 September, 2006

Carolyn Dittmeier
Poste Italiane
Vice President, Internal Audit

AGENDA

- Evolution of Internal Auditing
- Focus on Interpersonal Skills
- Interpersonal Skills throughout the Internal Audit Process

AGENDA

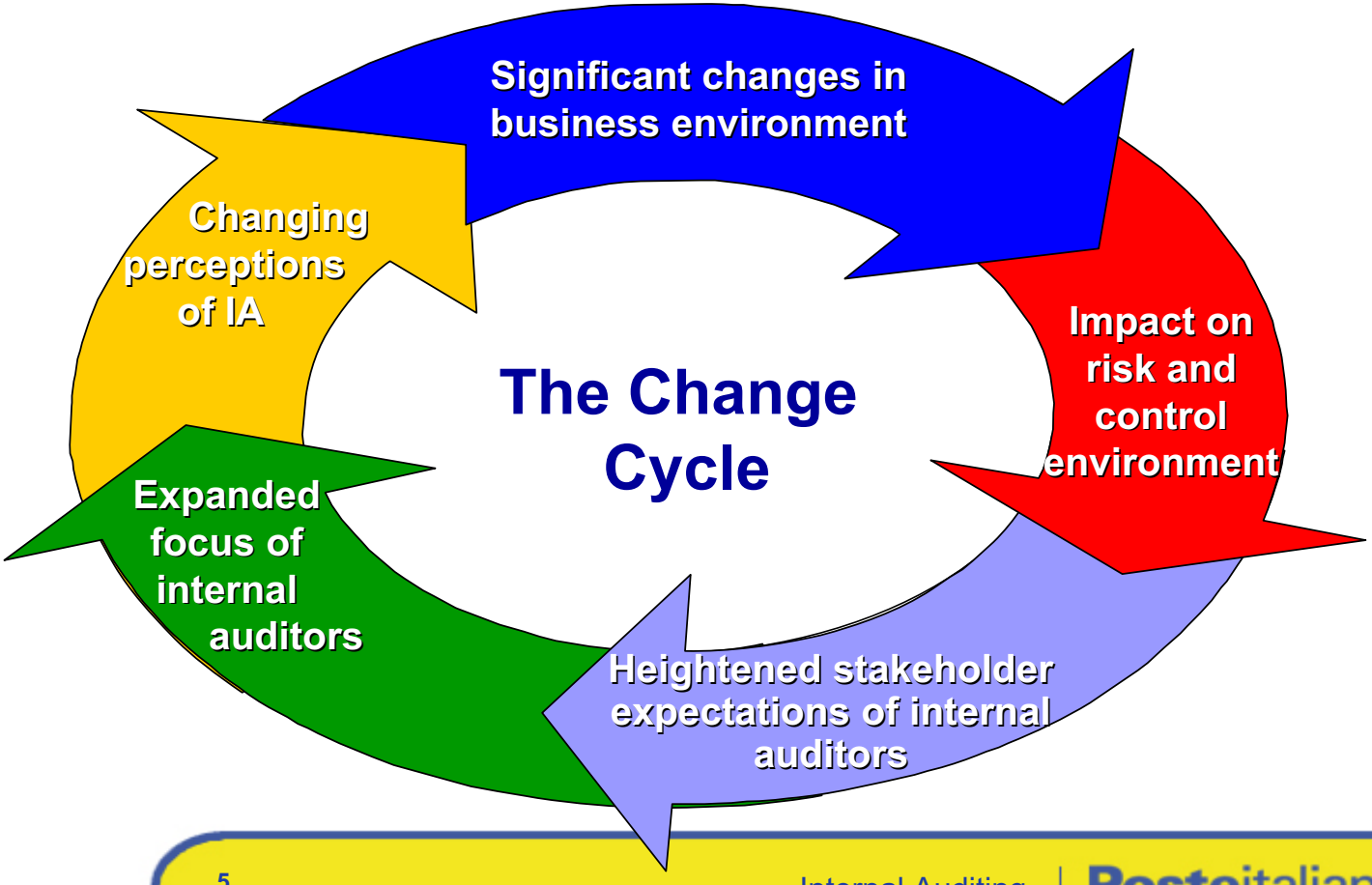
- **Evolution of Internal Auditing**
- Focus on Interpersonal Skills
- Interpersonal Skills throughout the Internal Audit Process

Evolution of Internal Auditing

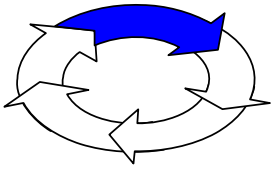
Some key words in the Current IIA Definition of Internal Auditing

Internal Auditing is an independent, ***objective*** *assurance and* ***consulting*** *activity designed to* ***add value*** *and* ***improve*** *an organization's operations. It* ***helps*** *an organization accomplish its objectives by bringing a systematic,* ***disciplined approach*** *to evaluate and improve the effectiveness of risk management, control and governance processes.*

Evolution of Internal Auditing



Evolution of Internal Auditing

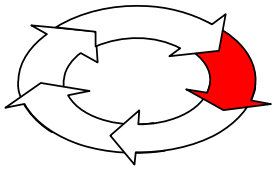


Significant changes in business environment

- Competitivity/ complexity in the market
- Focus on cost reduction and value-added products
- Increasing guidelines on Corporate Governance
- Rising domestic/international regulations
- Technology

Will this impact my interpersonal skills?

Evolution of Internal Auditing

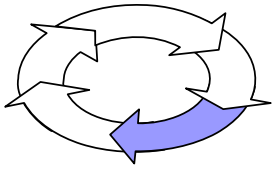


Impact on risk and control environment

- Increasing need for enterprise-wide risk culture
- Increasing importance of ethical and reputational risks
- Focus on “Risks” and “Opportunities”

Will this impact my interpersonal skills?

Evolution of Internal Auditing

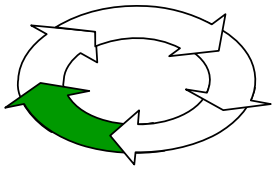


Heightened stakeholder expectations of internal auditors

- Value added approach supporting business
- Not only assurance services, but consulting for improvement
- Relations with entities and authorities involved in governance and control

Will this impact my interpersonal skills?

Evolution of Internal Auditing

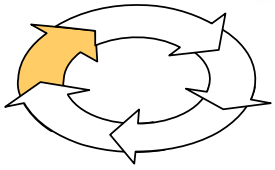


Expanded focus of internal auditors

- Involved in changes
- Driver of change
- Focused on Governance Objectives
- …and also focused on Business Objectives

Will this impact my interpersonal skills?

Evolution of Internal Auditing



Changing perceptions of IA

Significant changes in stakeholder expectations/perceptions of Internal Auditors and the Focus of Internal Auditing

Traditional

- Procedural Controls
- Detail Transactions
- Reporter of exceptions
- Cost Center
- Departmental Audits

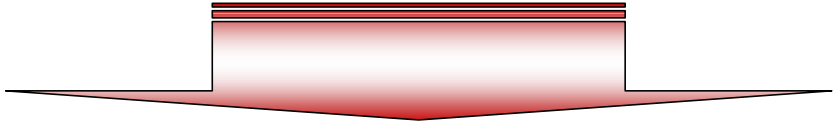
Current

1. Partner on business/Risk
2. Process analyst
3. Consultant for Improvement
4. Risk governance advisor
5. Integrated Audits

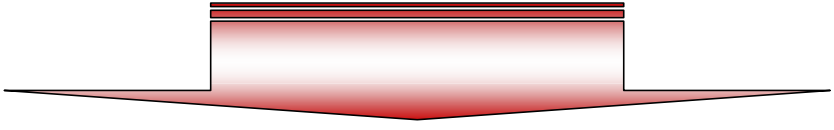
Will this impact my interpersonal skills?

Evolution of Internal Auditing

No limits to the Internal Auditing profession



New challenges, new competencies



Good interpersonal skills needed throughout

AGENDA

- Evolution of Internal Auditing
- **Focus on Interpersonal Skills**
- Interpersonal Skills throughout the Internal Audit Process

Focus on Interpersonal Skills

"… by bringing a systematic, disciplined approach …"

IA COMPETENCIES

Internal Auditing Know How

- Professional Stqndards
- Managing IA Function
- Audit planning and execution
- Evaluating Risks/Controls
- Using statistical tools
- Testing
- IT and specialized auditing

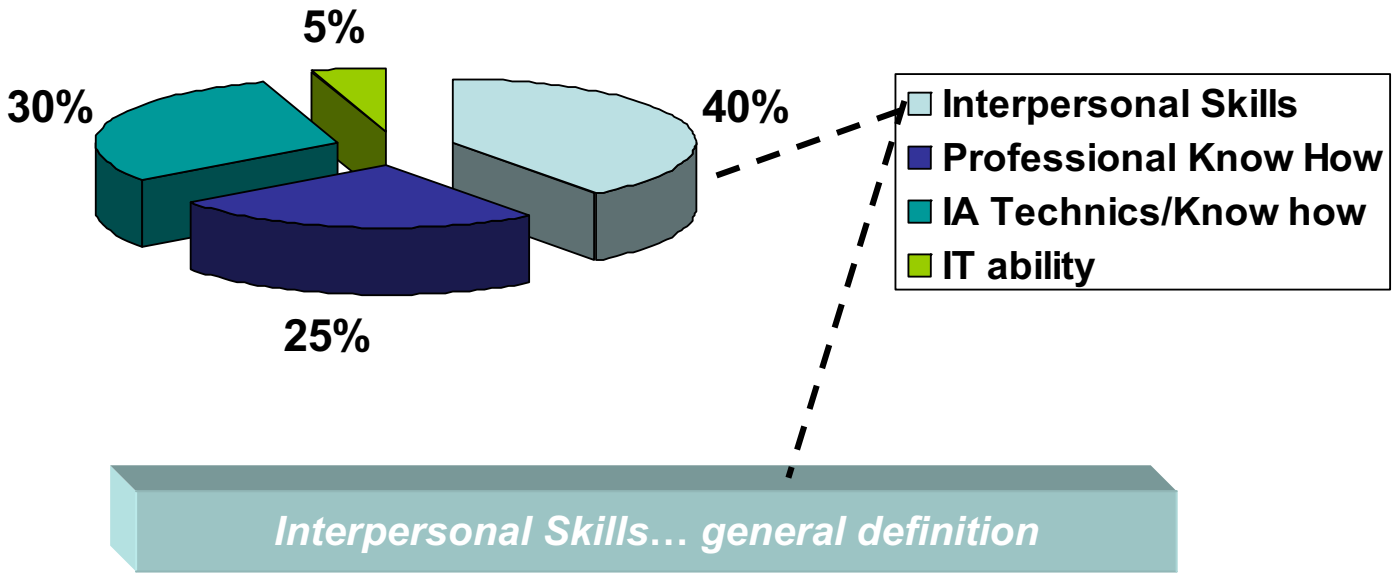
Interpersonal Skills

- **Leadership**
- **Team working**
- **Networking**
- **Communication skills:**
  - **oral & written**
- **Problem solving**

Professional Know How

- Accounting
- Finance
- Process Analysis
- Organization
- International Relations/PA
- Tax aspect
- Regulations & Laws
- Marketing
- Risk management

Focus on Interpersonal Skills



The ability to read and manage the emotions, motivations, and behaviors of oneself and others during social interactions or in a social-interactive context

Focus on Interpersonal Skills

Key elements

Leadership — The process of successfully influencing the activities of a group towards the achievement of a common goal

Teamworking — Involves working with others in a group towards a common goal

Networking — The ability to actively seek, identify and create effective contacts with others, and to maintain those contacts for mutual benefit

Communication skills — Communication is a behavior inside a system in which feedback is affecting one's behavior

Problem Solving — Forms part of thinking; it's considered one of the most complex of all intellectual functions

Leadership

...cont'd

Mentoring	Being a trusted advisor and helper with experience in a particular field. Actively supporting and guiding someone to develop knowledge and experience, or to achieve career or personal goal. A mentoring relationship may be formal or informal, but must involve trust, mutual respect, and commitment as both parties work together to achieve a goal
Decision Making	Identifying appropriate evidence and weighing up that evidence to make a choice. Taking responsibility for a decision and its outcomes
Delegation	Taking responsibility for determining when to ask someone else to make a decision or carry out a task. Distributing responsibility and authority in a group by giving someone else the discretion to make decisions that you have the authority to make
Motivating Others	Generating enthusiasm and energy by being positive, focusing on finding solutions and maintaining a positive attitude even when things are not going well. Encouraging others to come up with solutions, listening carefully to their ideas and offering constructive feedback. Being prepared to support others in taking agreed, calculated risks, and not blaming others when things go wrong

Teamworking

…cont'd

Collaboration	Working cooperatively and productively with other team members to contribute to the outcomes of the team's work
Decision Making	Identifying appropriate evidence and weighing up that evidence to make a choice. Taking responsibility for a decision and its outcomes
Mentoring	Being a trusted advisor and helper with experience in a particular field. Actively supporting and guiding someone to develop knowledge and experience, or to achieve career or personal goal. A mentoring relationship may be formal or informal, but must involve trust, mutual respect, and commitment as both parties work together to achieve a goal
Motivating Others	Generating enthusiasm and energy by being positive, focussing on finding solutions and maintaining a positive attitude even when things are not going well. Encouraging others to come up with solutions, listening carefully to their ideas and offering constructive feedback. Being prepared to support others in taking agreed, calculated risks, and not blaming others when things go wrong

…cont'd

Teamworking in the Digital Age is more complex than in past…

- Meeting
- E-mail
- Conference Call
- Videoconferencing
- Fax
- Internet-based project software

Communication skills

…cont'd

Behavior	Behavior in an interactional situation has message value, it's communication
Inside a System	Interaction is a part – a subsystem – of a lager system. The subsystems are interrelated or interdependent so as to form a part of a larger whole. Understanding communication is impossible without considering the larger context or system of which it is a part
Feedback	Feedback is a process whereby some proportion or in general, function, of the output signal of a system is passed (fed back) to the input. Often this is done intentionally, in order to control the dynamic behavior of the system
Synergic	The interaction is synergic, so that the total effect exceeds the sum of the effects of the separate parts
Equifinality	A system is able to achieve desired results by using different methods

Problem Solving

…cont'd

Think/Feel	There is no separation between mind and body, mind cannot exist or operate at all without body and one cannot make any decision only with "reason", there must be collaboration of body in this process
Brainstorming Technique	Brainstorming is a creativity technique of generating ideas to solve a problem. The main result of a brainstorm session may be a complete solution to the problem, a list of ideas for an approach to a subsequent solution, or a list of ideas resulting in a plan to find a solution
Trial and error Technique	Trial and error is a method for obtaining knowledge, both propositional knowledge and know-how. In trial and error, one tries an option to see if it works. If it works, then we have a solution. If it doesn't work - there is an error - then one tries another option
Analogy Technique	Analogy is either the cognitive process of transferring information from a particular subject to another particular subject. In a narrower sense, analogy is an inference or an argument from a particular to another particular, as opposed to deduction, induction, and abduction, where at least one of the premisses or the conclusion is general

Networking

...cont'd

Network building

Creating contacts with other people and maintaining those contacts. Acquiring and maintaining information about people who might be useful contacts for specific purposes. Using a contact in an ethical manner to help each of you meet specific goals

Motivating others

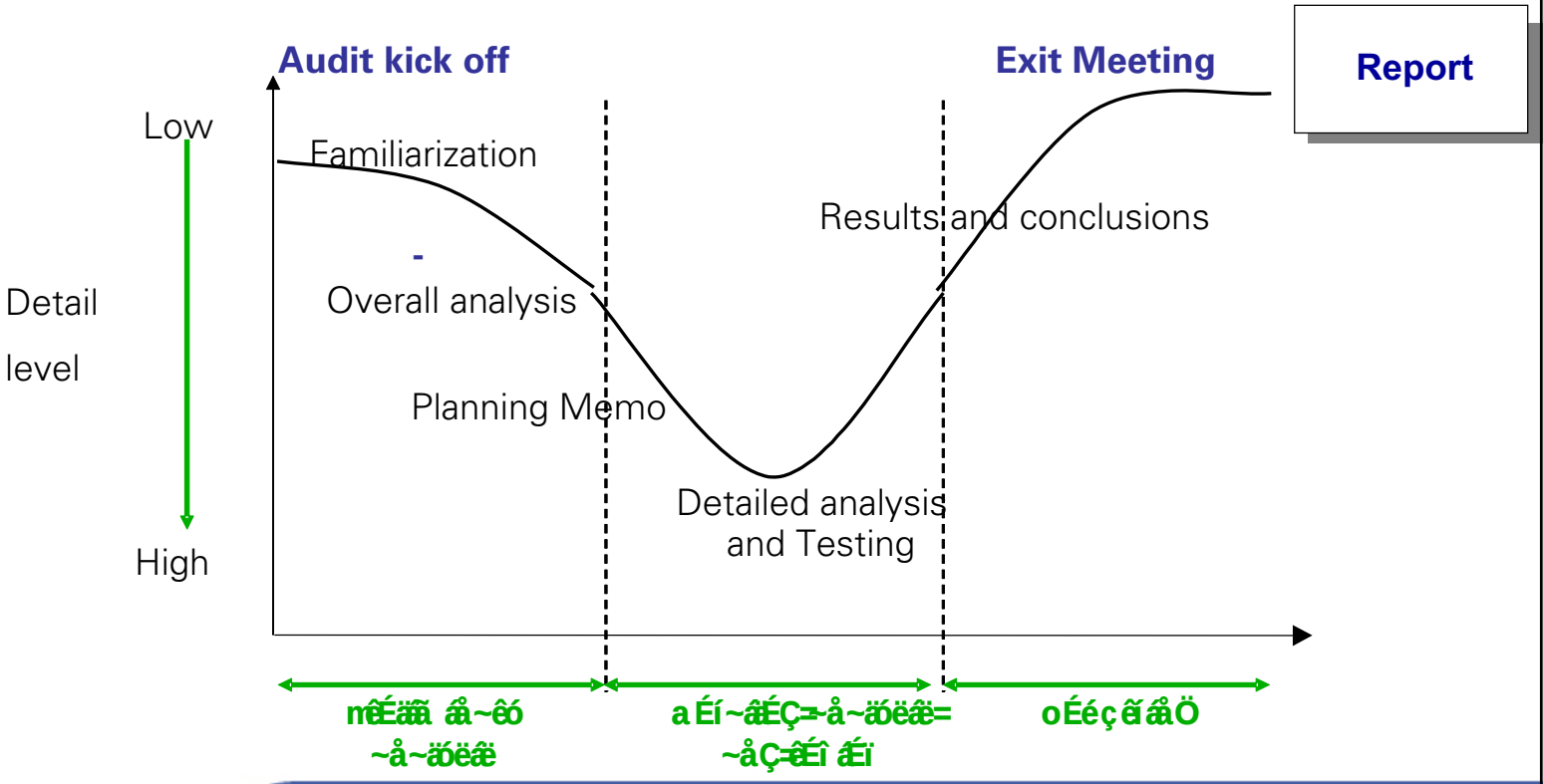
Generating enthusiasm and energy by being positive, focussing on finding solutions and maintaining a positive attitude even when things are not going well. Encouraging others to come up with solutions, listening carefully to their ideas and offering constructive feedback. Being prepared to support others in taking agreed, calculated risks, and not blaming others when things go wrong

AGENDA

- Evolution of Internal Auditing
- Focus on Interpersonal Skills
- **Interpersonal Skills throughout the Internal Audit Process**

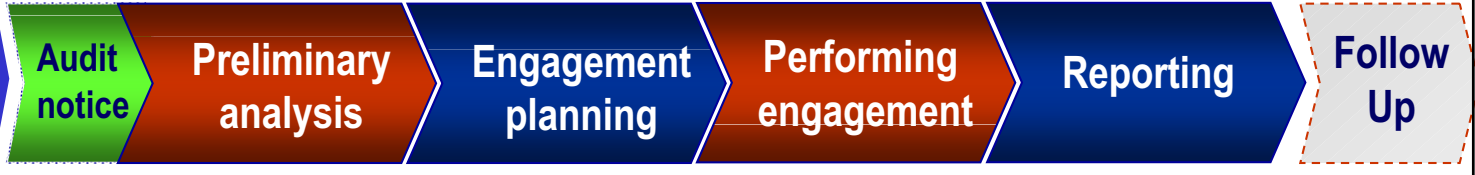
Interpersonal Skills throughout the IA Process

The "roller- coaster" of the audit process



Interpersonal Skills throughout the Audit Cycle

AUDIT PLAN



Interpersonal Skills throughout the IA Process

Audit notice

Engagement communication

- Telephone contact
- Audit Notification Letter providing objectives, team and timing

Clarify and align expectations; start relationship building

- Leadership
- Teamworking
- Networking
- **Communication skills**
- Problem Solving

Interpersonal Skills throughout the IA Process

Preliminary Analysis → **Kick-off Meeting**

- Building a common understanding on audit objectives and process
- Gathering information concerning the work (process objectives, risks/controls, management concerns/requests)

Focus on Auditee's needs

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

Interpersonal Skills throughout the IA Process

Preliminary Analysis

General information survey

- Explore business environment & activities
- Understand business objectives and risks
- Gain knowledge on regulations and procedures
- Understand organizational
- Comprehend budget/financial information

Through good information contacts, effectively analyse information, while obtaining cooperation from auditee and mazimizing audit team power

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

Interpersonal Skills throughout the IA Process

Engagement Planning

Engagement Resource Allocation

- Matching number and experience level of IA Staff with required competencies
- Training needs
- Use of external resources

Effective team building

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

Interpersonal Skills throughout the IA Process

Engagement Planning — **Work Program**

- Utilize all useful information
- Allocate tasks focusing on professional competencies
- Consider relationships within team
- Supervision process

Plan, promoting a teamworking environment and an effective approach

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

Interpersonal Skills throughout the IA Process

Meet and communicate with appropriate management in order to periodically update auditee of progress and review findings and recommendations

Communication skills

No Surprises!

Interpersonal Skills throughout the IA Process

Performing engagement

Analysing, testing, evaluating information

- Assess information properly
- Arrive at appropriate conclusions and useful recommendations

Team analysis; provide auditee with results; utilize feedback; formulate final recommendations

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

Interpersonal Skills throughout the IA Process

Performing engagement

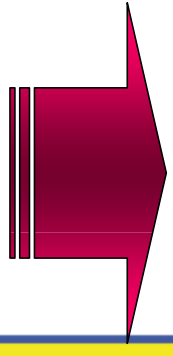
Exit Meeting

An excellent way to market the audit's products:

→ communicating/discussing results

→ selling ideas, offering solutions to problems

→ Obtaining acceptance



Action plan

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

Interpersonal Skills throughout the IA Process

Performing engagement

Exit Meeting

The 7 P's of marketing mix applied to Internal Audit

- **Product -** Engagement findings and related action plan
- **Pricing -** Activity's costs versus added value provided
- **Promotion -** Methods of promoting benefits for the needed changes
- **Placement -** During the exit meeting and reporting phase
- **People -** Clients consider auditor as inseparable part of the audit services
- **Process -** Behavior of auditors during the meeting
- **Positioning -** Show the benefits of the improvement

Interpersonal Skills throughout the IA Process

Reporting

Engagement Communication

Communicating results:

→ **Oral Presentation**

→ **Written communication**

Reporting objectives:

- Get attention and understanding of readers through concise, useful information
- Convince
- Obtain action

- Leadership
- Teamworking
- Networking
- Communication skills
- Problem Solving

E-1
ICT Literacy for all Auditors: the Inevitable Route!

Kornelis Mollema (NED)
Professor of ICT Auditing
Erasmus University Rotterdam

ESAA

ICT literacy for all auditors, the inevitable route

by dr Kornelis Mollema RE RA

Professor in IT auditing

Erasmus School of Accountancy & Assurance

Rotterdam, the Netherlands

Sept 2006

ESAA

THE BUSINESS DEVELOPMENT LADDER

Stronger need for computer literacy?

Strong tightening of rules (IFRS, SoX, etc.)

Stronger awareness need for internal assurance

twenties repeat of the cycle?

tens business failures

nineties business booming, consolidation

eighties business failures

seventies business consolidation

sixties business booming

ESAA

THE AUDIT DEVELOPMENT LADDER

twenties computer literate auditing?

operational auditing

tens integrated r & c oriented auditing

nineties strategy-oriented auditing

ICT auditing

Eighties financial audit around the ICT

seventies analytical financial auditing

sixties synthetical financial audit

ESAA

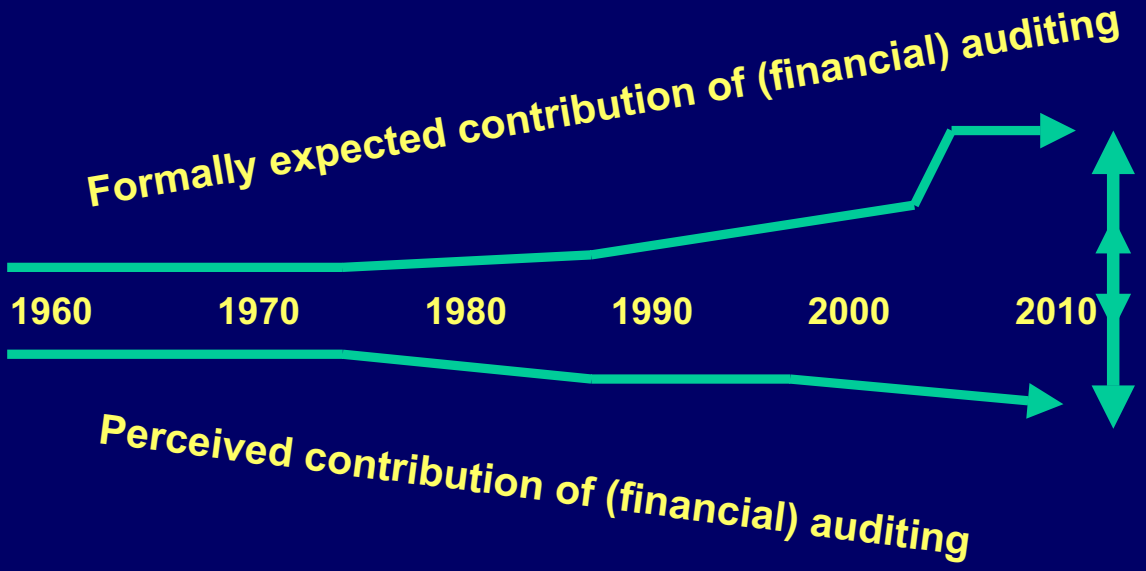
STRONG INCREASE OF BUSINESS COMPLEXITY THROUGH:

- globalisation
- science / technology developments
- business consolidation
- financing developments
- risk thinking
- production robotisation
- micro automation
- network ICT
- paperless society

ESAA

Business trends	Audit response
• globalisation	internationalisation of services
• science / techn. developments	line of industry specialisation
• business consolidation	consolidation firms/deptms
• corporate finance	IFRS
• risk thinking	risk oriented auditing
• production robotisation	??
• micro automation	??
• network ict	ICT audit
• paperless society	??

ESAA


Formally expected contribution of (financial) auditing
1960
1970
1980
1990
2000
2010
Perceived contribution of (financial) auditing
expectation gap

ESAA

Deus ex machina

If you, auditor, meet complexity: hire an expert!

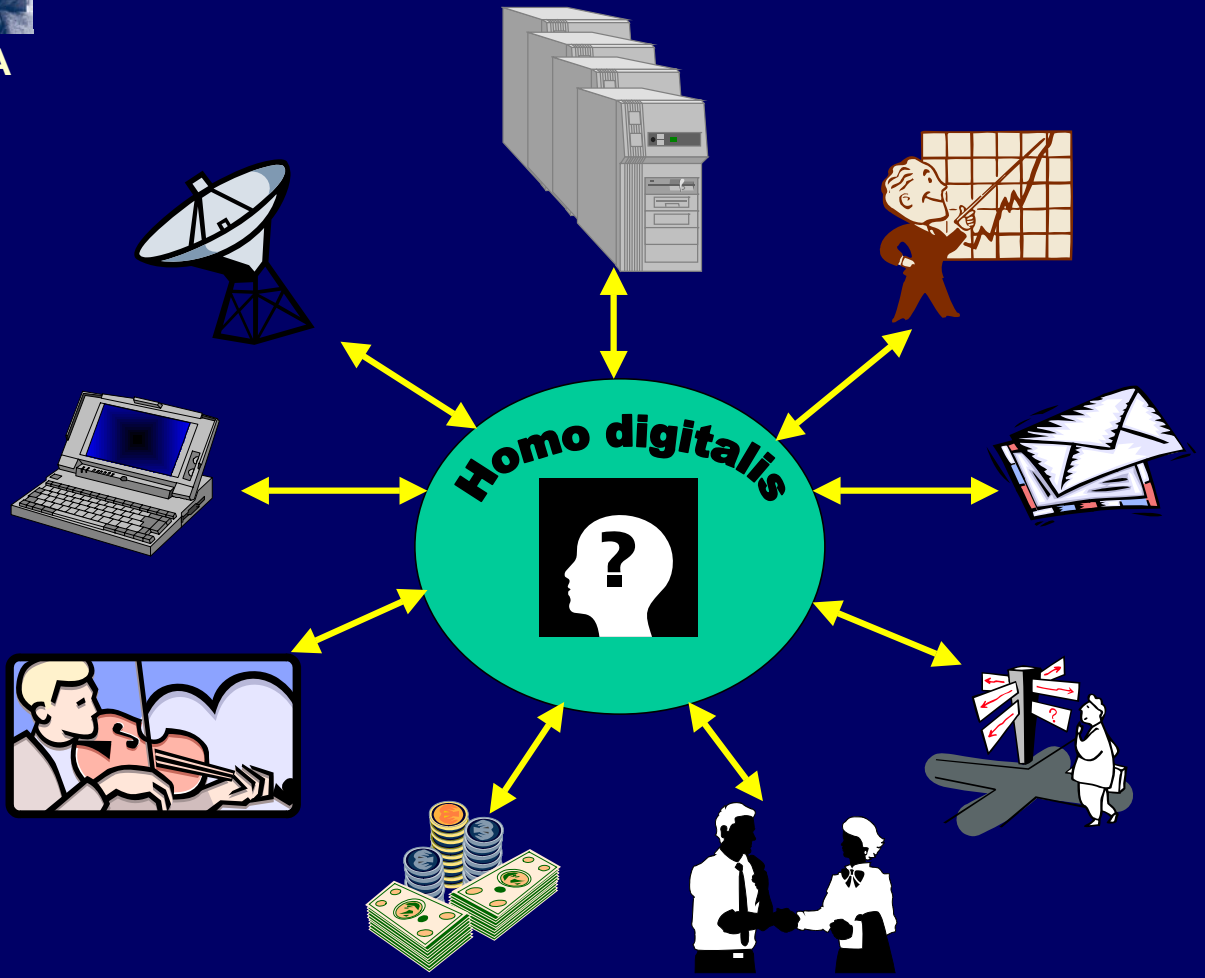
Complex insurance contracts? Hire an actuary!
Complex financial structure? Hire an economist!
Complex legal environment? Hire a lawyer!
Complex logistical situation? Hire an operational auditor!
Complex risk situation? Hire a risk management specialist!
Complex ICT situation? Hire an IT auditor?

ESAA

Mr. Audit

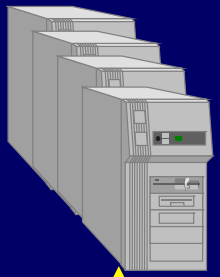
ESAA

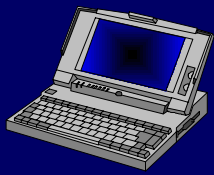
HOMO QUOD?



ESAA

AUDITOR QUOD?

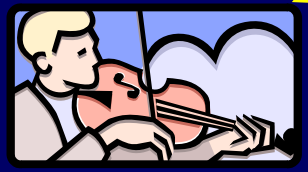




Homo digitalis

?

Auditor desperatus?



ESAA

NEW CORPORATE GOVERNANCE

RULES OBLIGE TO

- maintenance of an adequate internal risk management & control system
- accounting for the effectiveness of this system
- auditor's assurance (implicit or explicit)

ESAA

IMPACT OF ICT ON CORPORATE GOVERNANCE RULES

- ICT tends to have a major impact as ICT has heavily penetrated business conduct
- ICT risk is a major and increasing subset of operational risk
- The internal control system houses mainly in the ICT

ESAA

corporate governance

design & implementing strategy

(risk) management

service contracting

i c t	treasury	human capital	marketing procurement production sales delivery after sales	logistics	int. control sys.	i c t

accounting & reporting

audit

MODEL OF AN ENTERPRISE

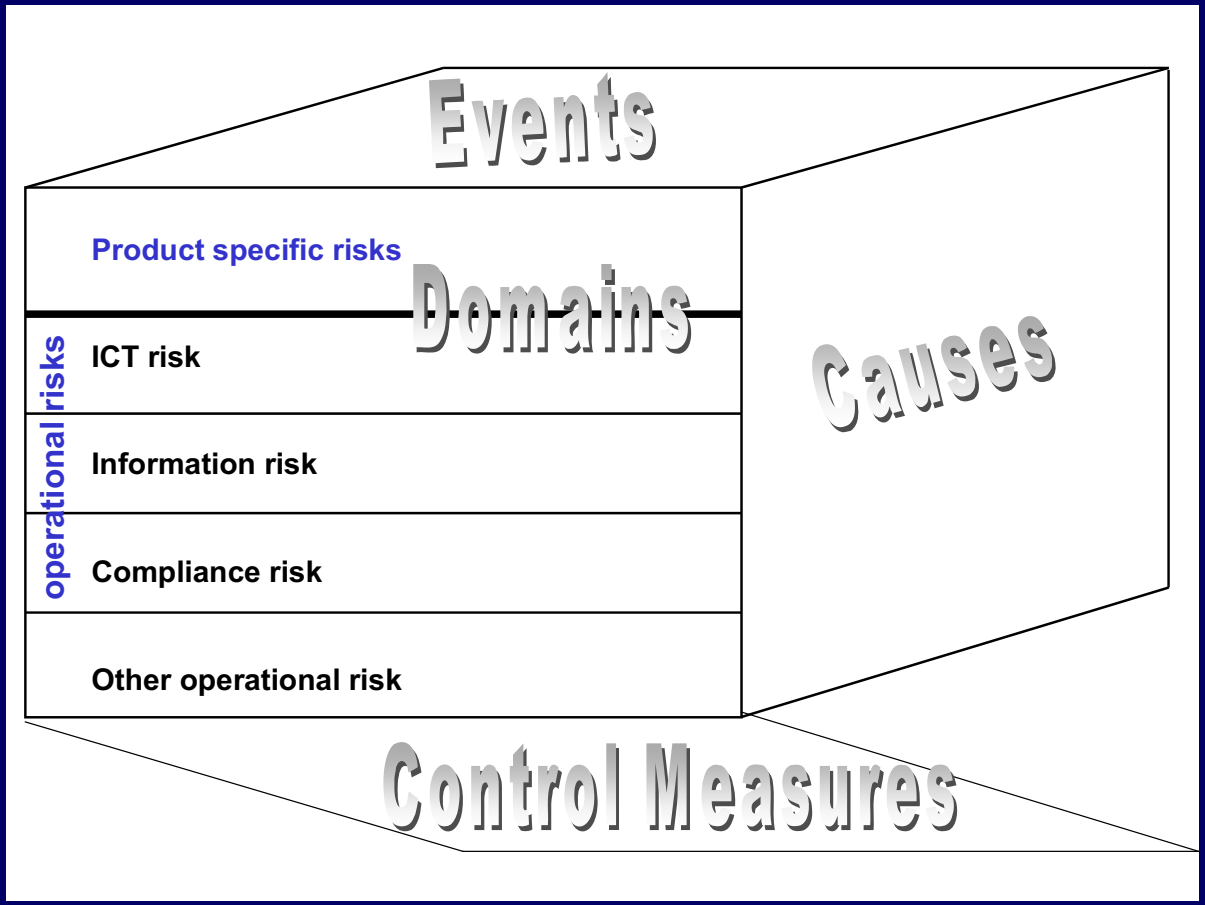
ESAA

IMPACT OF ICT ON CORPORATE GOVERNANCE RULES

- ICT tend to have a major impact as ICT has heavily penetrated business conduct
- ICT risk is a major and increasing subset of operational risk
- The internal control system houses mainly in the ICT

ESAA

BUSINESS RISK & CONTROL MODEL



ESAA

ICT RISK IS A MAJOR AND INCREASING SUBSET OF OPERATIONAL RISK, DUE TO

- its impact on information risk
- same on business effectiveness
  efficiency
  continuity

ESAA

ICT RISK IN ITSELF IS INCREASING CAUSED BY

- strong increase of individual ICT responsibility
- connectivity (Internet, intranet)
- strong ICT dependence
- dependence on external structures
- all eggs in one basket
- ICT target of crime (virusses, hacking)
- cyberterrorism
- inherent complexity of ICT →

ESAA

ICT INHERENTLY COMPLEX

speed	⟷	quality
tailored solutions	⟷	modular setup
flexibility	⟷	robustness
streamlining	⟷	non-monolithical
paperless	⟷	auditable
accessible	⟷	secure
affordable	⟷	competitive

WE ALWAYS HAVE TO BALANCE BETWEEN A ROCK AND A HARD PLACE!

ESAA

IMPACT OF ICT ON CORPORATE GOVERNANCE RULES

- ICT tend to have a major impact as ICT has heavily penetrated business conduct
- ICT risk is a major and increasing subset of operational risk
- The internal control system houses mainly in the ICT

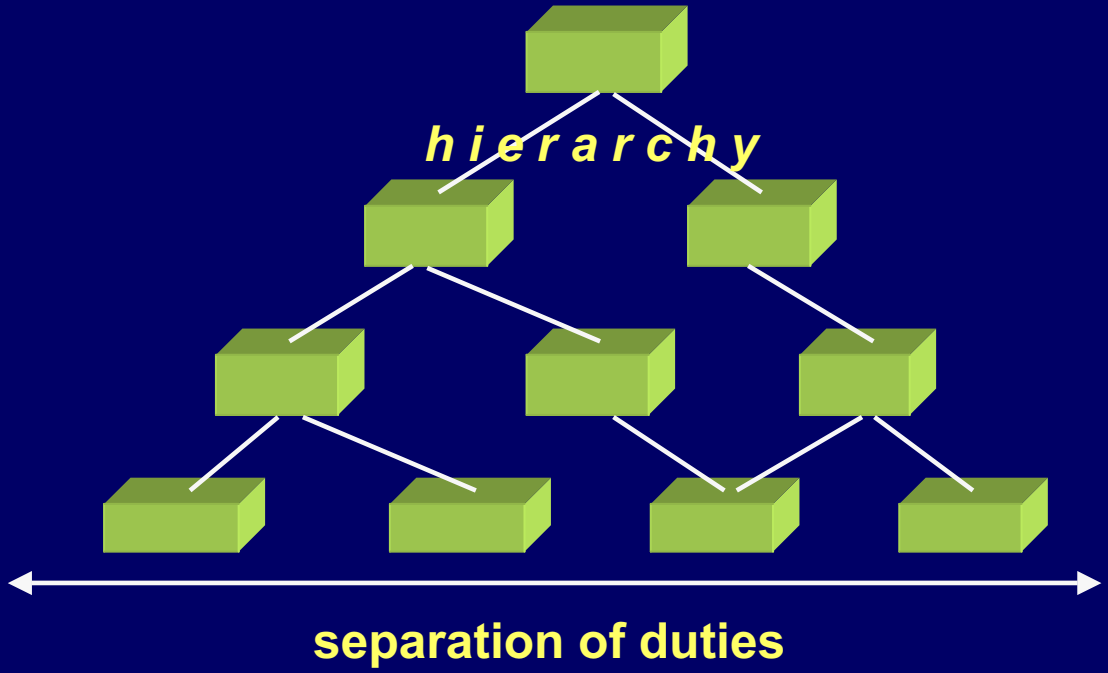
ESAA

THE INTERNAL CONTROL SYSTEM HOUSES MAINLY IN THE ICT

- the internal control is being increasingly automated
- separation of duties shrink as a result of workflow automation
- automated routing, a refined system of authorisations and refined automated controls give compensation

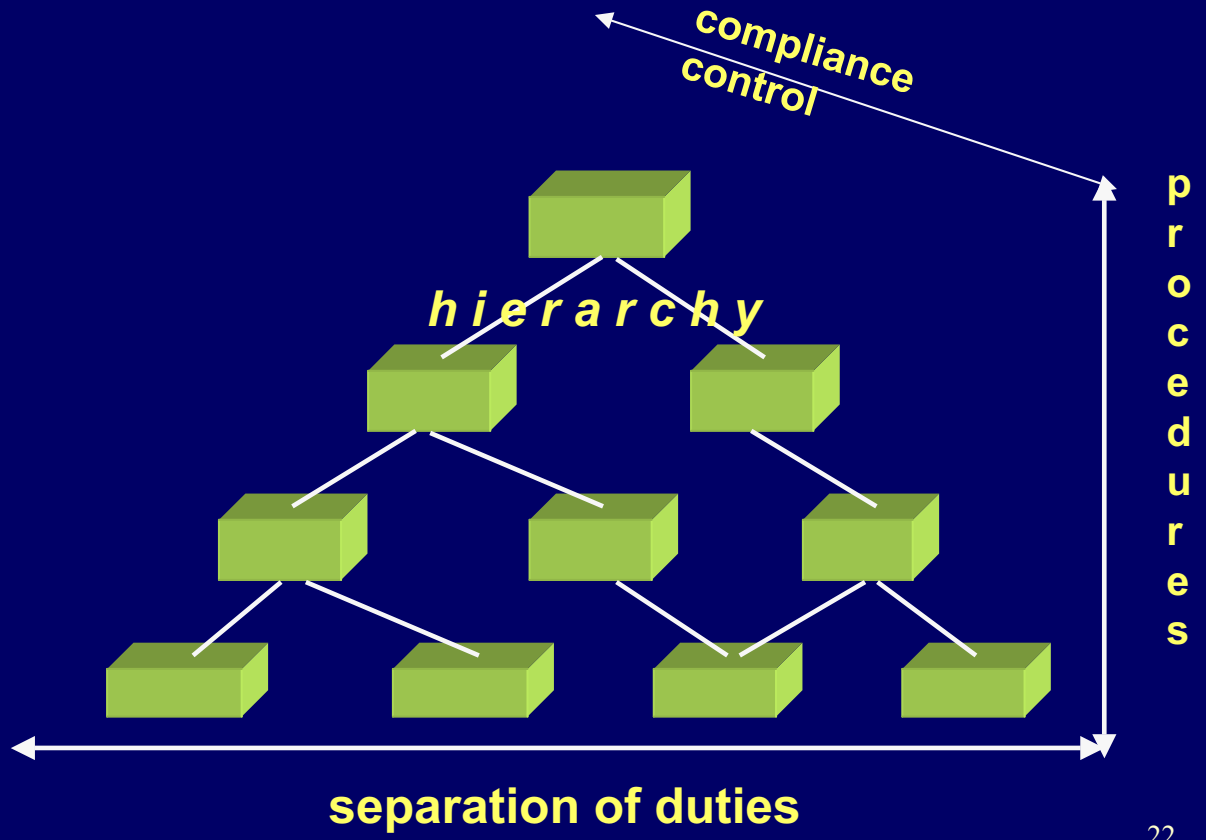
ESAA

INTERNAL CONTROL AS IT WAS



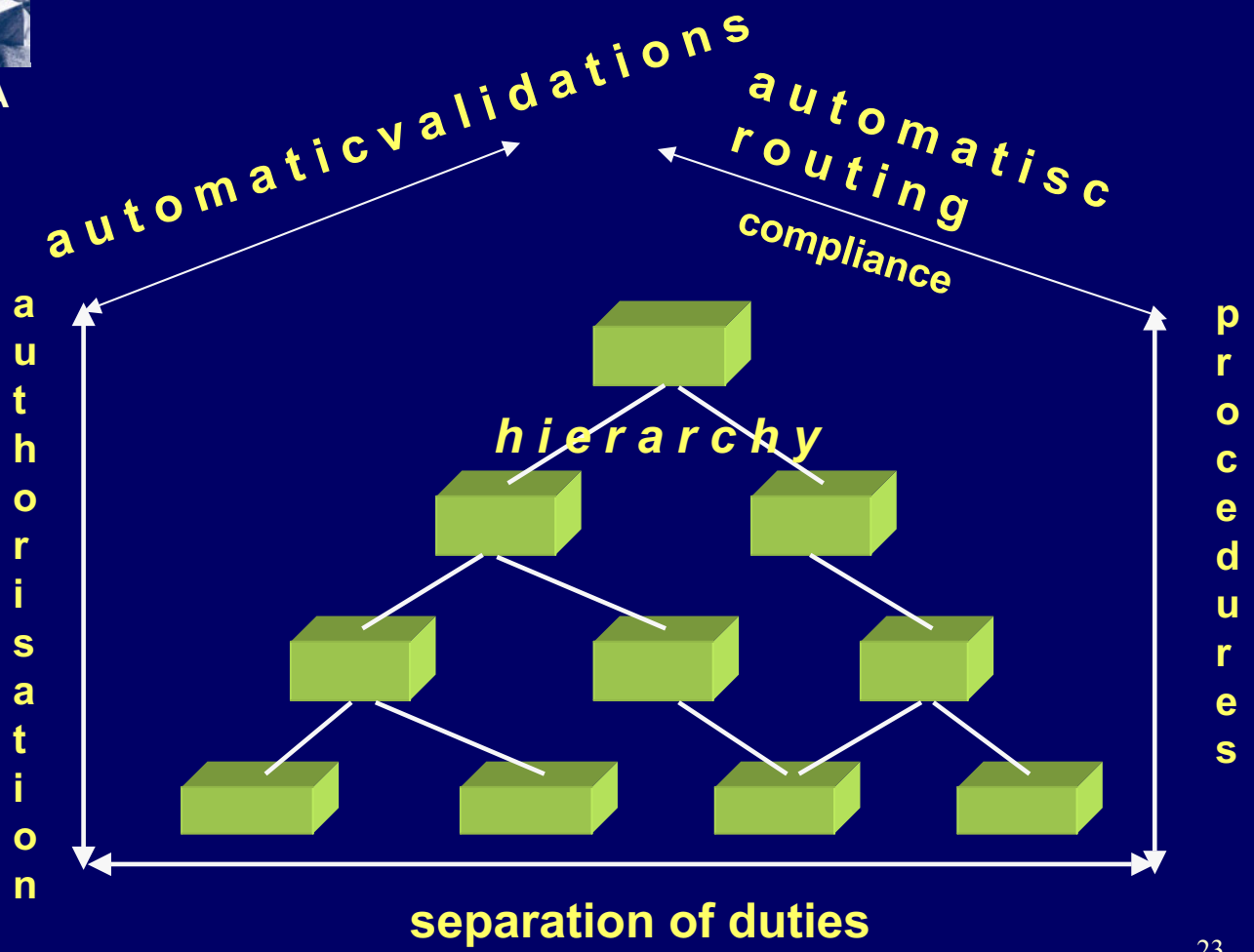
ESAA

INTERNAL CONTROL AS IT IS



ESAA

INTERNAL CONTROL IN ICT



ESAA

ICT GAINS IMPORTANCE AS THE PAPERLESS SOCIETY BECOMES REALITY

- (original) paper documents disappear
- transactions and payments are digitalised
- audit through the computer system is the only way
- reporting frequency going up

ESAA

ACTIVITIES IN THE COMPANY

Crossing the company's border always led to an original document

ESAA

PAPER EVIDENCE IN A PAPER BASED SOCIETY

These documents are the pillars of the traditional audit

ESAA

LOSS OF THE ORIGINAL DOCUMENTS

The original document is replaced by :

- **e-mail**
- **web files**
- **electronic data interchange**
- **xbrl**

This process is stimulated by:

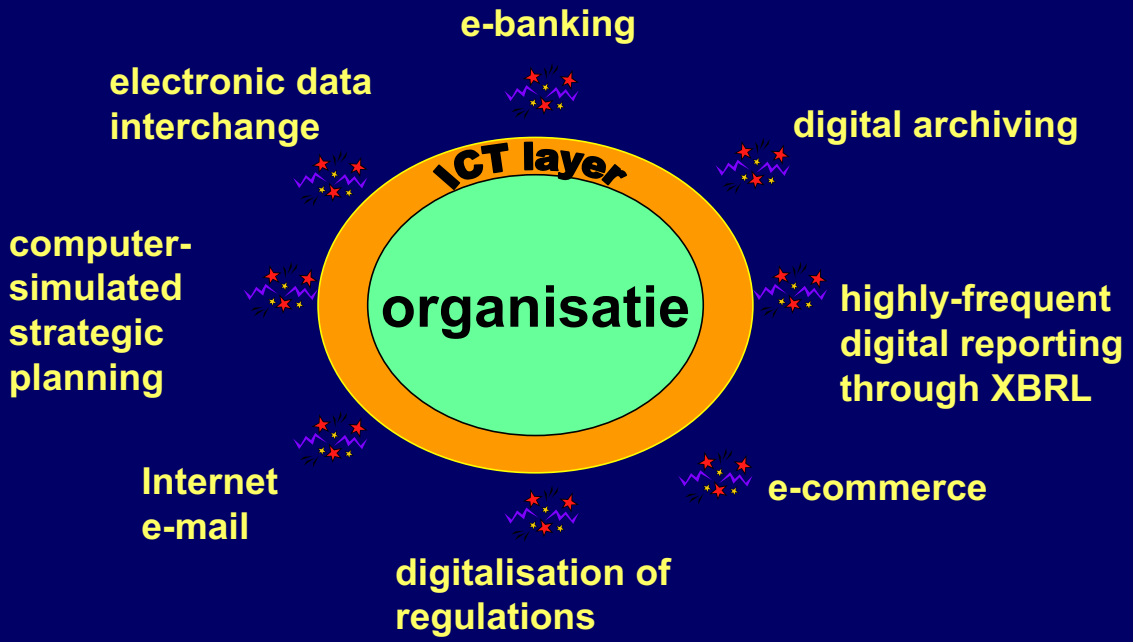
- **legal recognition of data, information and information carrier**
- **tough handling of paper volume**
- **the hay stack of information retaining obligations**

The authenticity of the original document erodes by:

- **photocopying & printing techniques**
- **scanning- / imagingtechniques**

ESAA

DIGITAL EVIDENCE IN THE DIGITAL SOCIETY



Crossing the company's border no longer results in a mandatory original paper document but in a trusted digital record.

DIGITAL RECORDS

ESAA

A trusted digital record is a non-exclusive thruthful digital image of a fact, an act or an event. Its integrity is guaranteed by like surrounding, such as:

- availability assurance
  - back up
  - escrows
- access control / change management
- readability measures
- management trail
- digital signature
- other authentication measures
- encryption techniques
- redundant bytes

Establishing the integrity of a trusted digital record requires considerable ICT knowledge!

ESAA

The digital society also requires

a different communication structure

ESAA

THE INFORMATION SUPPLY CHAIN

The communication explosion entails the need for safeguarding information quality whilst at the same time costs have to be kept low.

These can only be achieved by replacing man-to-man communication by computer-to-computer communication, reducing the need for frequent and time consuming human interpretation.

ESAA

HUMAN NEEDS FOR COMMUNICATION

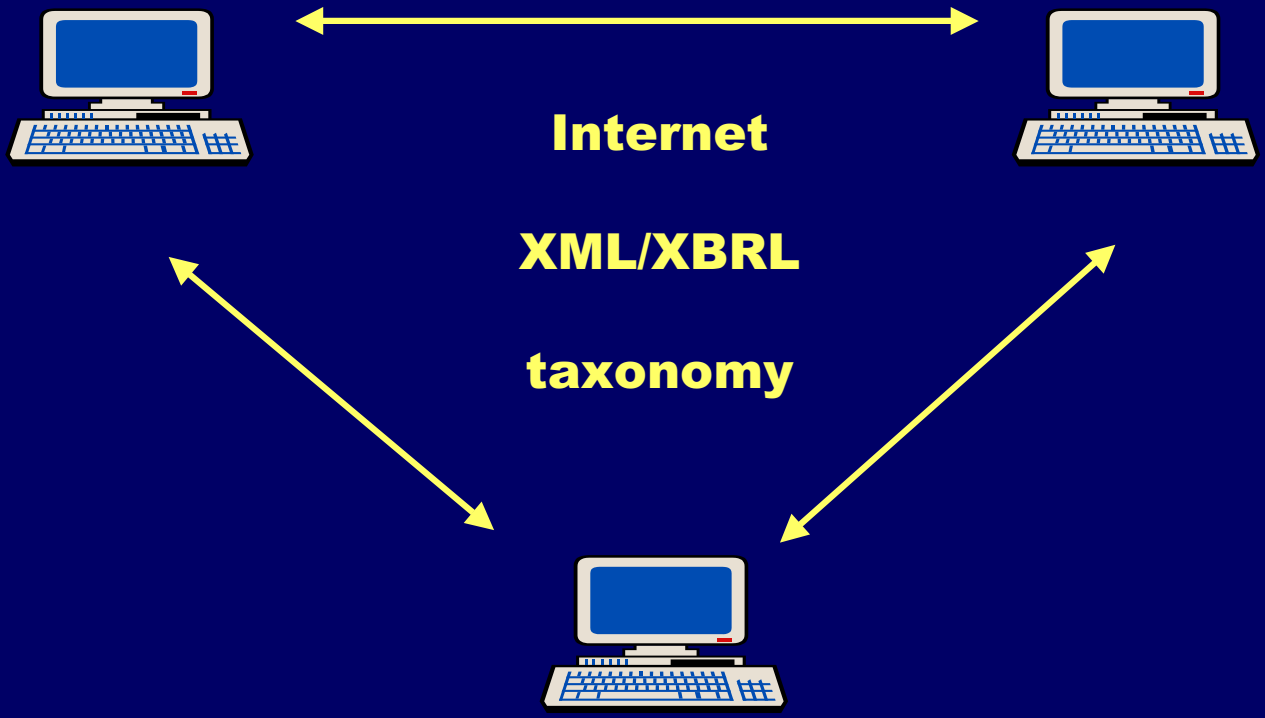
telephone

English

Webster

ESAA

ICT NEEDS FOR COMMUNICATION



ESAA

RESULTING REQUIREMENTS FOR CONTEMPORARY AUDIT

- dynamisation
- focus on risk, including ICT
- judgement of ICT/EDI/XBRL contracts and implementation
- intensive use of audit software for datamining etc
- new challenges for ICT auditing

ESAA

CONSEQUENCES FOR THE ICT AUDIT PROFESSION

- training higher numbers of ICT auditors at the universities
- help to make FA's and CIA's computer literate

ESAA

In the Netherlands several universities, amongst which the Erasmus School of Accountancy & Assurance provide supplementary ICT-audit courses for Registered Accountants and Registered Internal / Operational auditors, allowing them to qualify as a Registered ICT auditor in fifteen months.

ESAA

ACKNOWLEDGEMENT

Thank you for your patience

with your speaker!

E-2
IT Governance – Common Sense not Common Practice

Erik Guldentops (BEL)
Advisor to the Board
The IT Governance Institute

IT Governance

Common Sense, Not Common Practice

Erik Guldentops, CISA, CISM
Executive Professor
University of Antwerp – Management School, BE
Advisor to the Board
IT Governance Institute, USA

<erik.guldentops@pandora.be>

GOVERNANCE INSTITUTE

IT Governance

The IT Governance Institute

- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT– The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

IT GOVERNANCE INSTITUTE

What makes IT Governance so important?

Business and Operational Management want Value Transparency and Risk Mitigation

	2003	2005
Inadequate view on how well IT is performing	1	4
Operational failures of IT	2	3
Amount of security problems and incidents	3	7
High cost of IT with low return on investment	4	2
IT staffing problems	5	1
Lack of knowledge of critical systems	6	-
Disconnect between IT strategy and business strategy	7	6
Unmanaged dependencies on entities beyond own control	8	5
IT not meeting compliance requirements	-	8

- More Problems (operational ↑; security ↓)
- Transparency still an issue but shift to value
- Alignment slightly better
- Compliance top of agenda

Surveys by PwC for the IT Governance Institute Sep-Oct2003 and Sep-Oct2005

IT Governance Institute

What makes IT Governance so important?

Gartner: firms waste $351bn each year on ill-conceived IT projects

Nick Huber

THE average company wastes 20% of its IT budget on misguided and inefficient spending, the analyst firm Gartner has claimed.

debate about IT spending and return on investment (ROI).

Although Gartner has admitted that the 20% figure is an approximation it said that many chief information

tor. "They are being asked to cut costs to the business and do more with less.

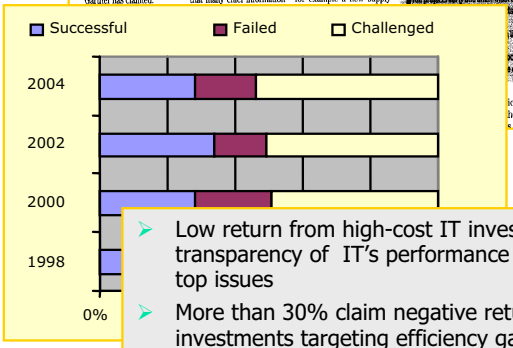
"But at the same time they are being asked to implement changes to the IT systems, for example a new supply

How to get most benefit from your spend

they have a common licensing agreement," said Kyte.

IT managers and company boards also need to be more ruthless when taking decisions about when to pull the plug on a troubled IT project, Gartner added. In the long run this will save time, money and professional reputations.

IT managers should bite the bullet. "In most organisations it is regarded as a badge of shame to terminate a project but we believe that killing projects is a sign of maturity," said Kyte.



- Low return from high-cost IT investments, and transparency of IT's performance are two of the top issues
- More than 30% claim negative return from IT investments targeting efficiency gains
- 40% do not have good alignment between IT plans and business strategy
- Interest in and use of active management of the return on IT investment has doubled in 2 years (28 to 58%)

- Gartner – more than 600 billion $ thrown away annually on ill conceived or ill executed IT projects
- Standish Group – about 20% of projects fail outright, 50% are challenged and only 30% are successful
- ITGI 2005 Survey early findings confirm concerns

IT GOVERNANCE INSTITUTE

What makes IT Governance so important?

- Financial Reliability
- Information Privacy
- Operational Risk
- Shareholder confidence
- Investor trust

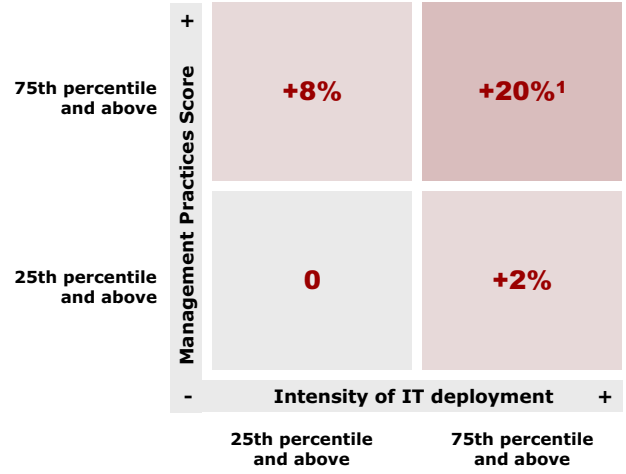
NEEDS

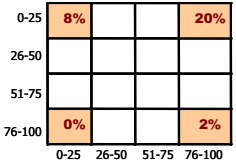
- Transparent, accountable and effective governance
- Awareness of corporate officers of the risk to and dependence on the information infrastructure
- More frequent, broader and deeper assurance about risk, information integrity and internal control

IT Governance Institute

What makes IT Governance so important?

In October 2005 Mc Kinsey and the London School of Economics measured the increase in productivity from investments in IT versus investments in management practices in 100 enterprises.





Additional spending in Information Technology can raise productivity.....

.....but only in well managed companies!

GOVERNANCE INSTITUTE

[1]For 9 out of 10 companies whose management-practices scores and levels of IT deployment are both in top quartile.

IT Governance

The IT Governance Institute

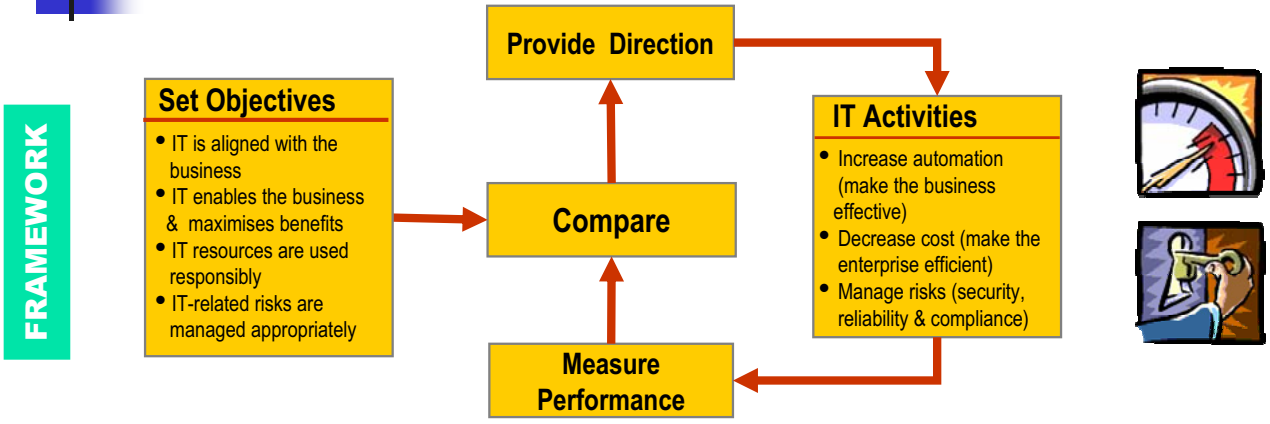
- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

IT Governance Institute

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT– The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

What is IT Governance?



- Objective: ensure that IT enables, sustains and extends the organisation's strategies and objectives
- Method: providing direction and exercising control
- Content: Leadership, organisational structures and processes
- Responsibility: board of directors and executive management

IT GOVERNANCE INSTITUTE

What is IT Governance?

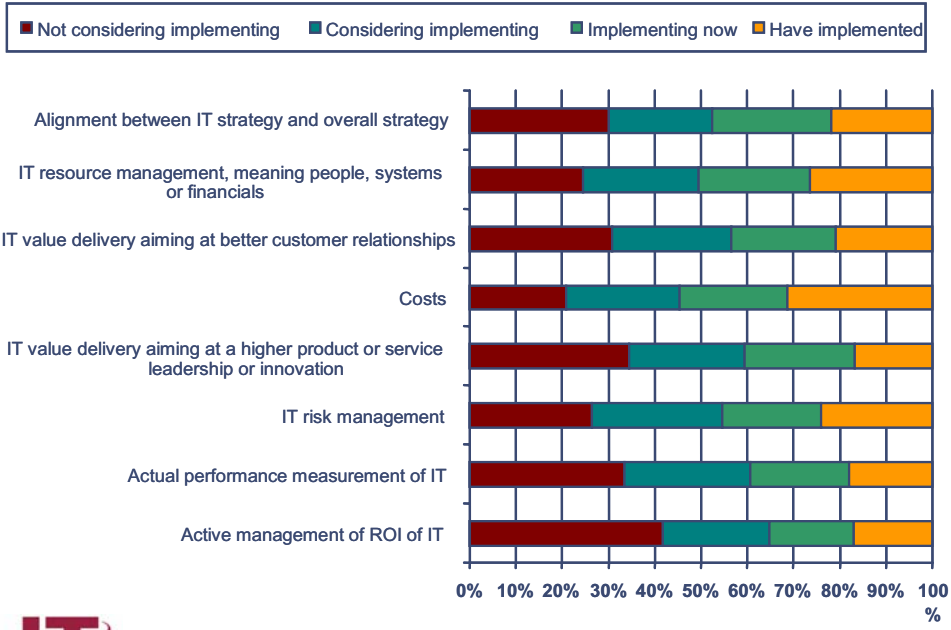
Board Briefing on IT Governance, 2nd Edition

- IT Governance : Definitions, facts, approach
  - Framework
  - Definitions
  - Five domains : Value and Risk focus
- Toolkit
  - Questions to ask
  - IT Governance Practices
  - Metrics to consider
- Supporting material
  - IT Strategy committee charter
  - IT Governance implementation advice
  - Roles and responsibilities of key players

A free download at www.itgi.org

IT GOVERNANCE INSTITUTE

What is being done about IT Governance?



- \+ Cost
- \+ Resources
- \+ Risk
- \- Value
- \- Performance

ITGI Survey of 700 CEO/CIO's worldwide by PwC – Oct 2005

IT Governance Institute

eg26042006-10

What is IT Governance?

DOMAINS

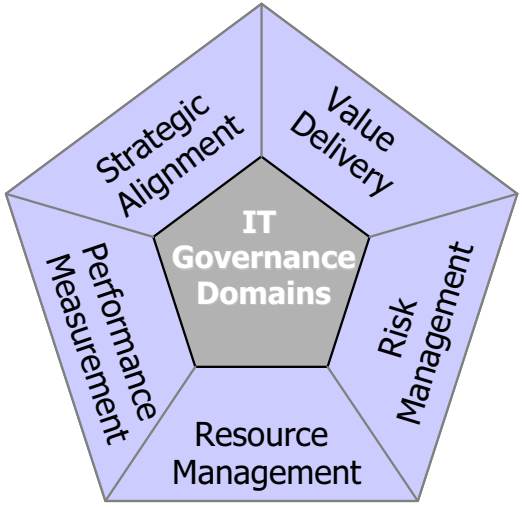
1. Strategic Alignment
aligning with the business and providing collaborative solutions

2. Value Delivery
focus on IT expenses and proof of value

3. Resource Management
knowledge, infrastructure and partners

4. Risk Management
safeguarding assets and disaster recovery

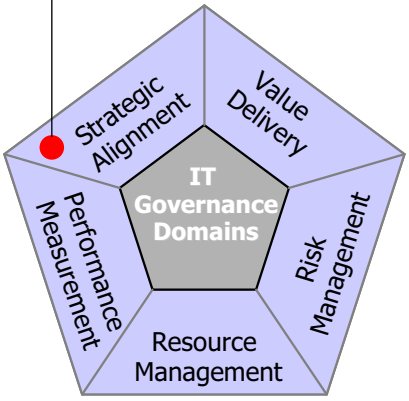
5. Performance Measurement
IT Scorecards



GOVERNANCE INSTITUTE

IT Governance – The Five Domains

Strategic Alignment
- Linking business and IT plan
- Defining, maintaining & validating the IT value proposition
- Aligning IT operations with the enterprise operations
- Provide collaborative solutions that
  - Adding value and competitive positioning to the enterprise's products and services
  - Containing costs while improving administrative efficiency and managerial effectiveness

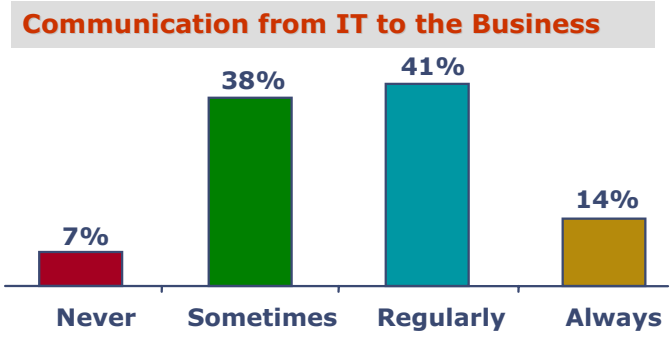


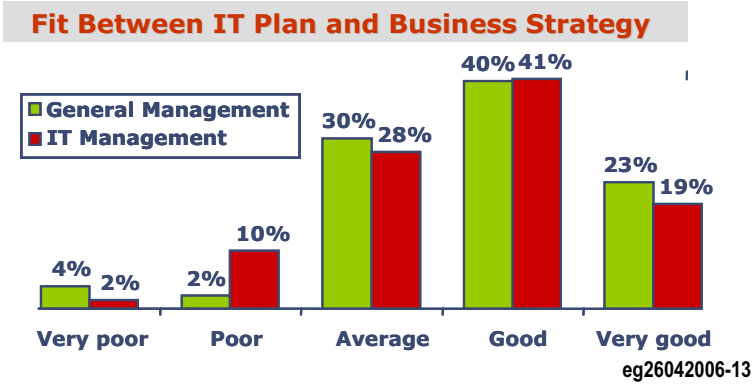
Best Practices
- Integrated approach to business/IT strategy
- Cascading strategy and objectives down into the organisation
- Co-responsibility of business and IT
- Business relationship managers
- Clearer objectives for IT investments
- IT Strategy & IT Steering Committees

In 2003, 49% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 70%.

GOVERNANCE INSTITUTE

IT Governance – Strategic Alignment

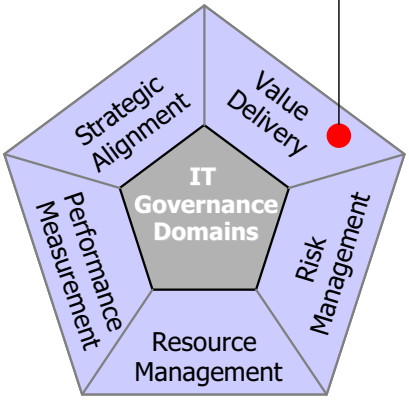




GOVERNANCE INSTITUTE

eg26042006-13

IT Governance – The Five Domains



Value Delivery

- Executing the value proposition throughout the delivery cycle
- Ensuring that IT delivers the promised benefits against the strategy
- Concentrating on optimizing expenses & proving IT's value
- Controlling projects and operational processes with practices that increase the probability of success (quality, risk, time, budget, cost, etc.).

Best Practices

- Clarify value, educate, involve stakeholders and manage perceptions
- Formal tracking of business value of IT
- Enabling effective value measurement (ROI, TCO, NPV…)
- Disciplined approach to project management with a larger role for the business
- Technology standardisation

In 2003, 39% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 69%.

GOVERNANCE INSTITUTE

Risk and Value are very closely related

Sainsbury share price

Suffered major embarrassment and financial loss when their failure to implement fully and on time their major new logistic support system became public knowledge became public knowledge

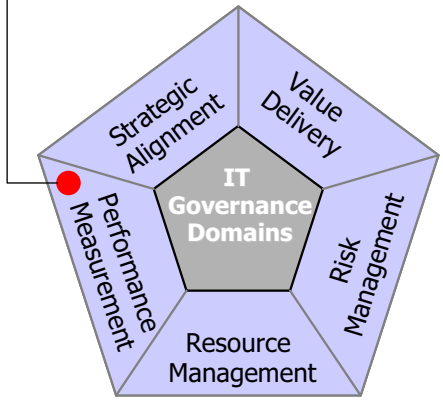
MFI share price

Share price drops following difficulties with the implementation of their SAP based warehousing and logistics system presenting them with significant issues with their order fulfilment.

… both have recovered well since then

GOVERNANCE INSTITUTE

IT Governance – The Five Domains



Performance Measurement

- Tracking project delivery and monitoring IT services
- Using balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting
- Measuring relationships and assets necessary to compete: customer focus, process efficiency and the ability to learn and grow

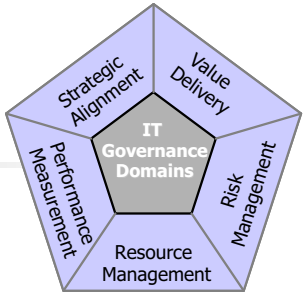
Best Practices

- IT Balance Scorecard as emerging reporting system
- A management reporting system that feeds back into the strategy
- The most effective means to achieve IT and Business alignment
- IT Scorecard approval by the key stakeholders for alignment

In 2003, 34% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 67%.

GOVERNANCE INSTITUTE

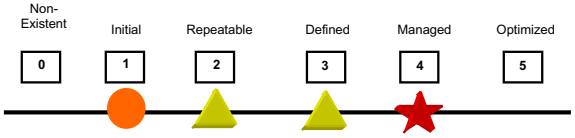
Measuring Progress



How far we've come...

I.S. Governance Assessment

Maturity Model Applied: CobiT 3 Management Guidelines



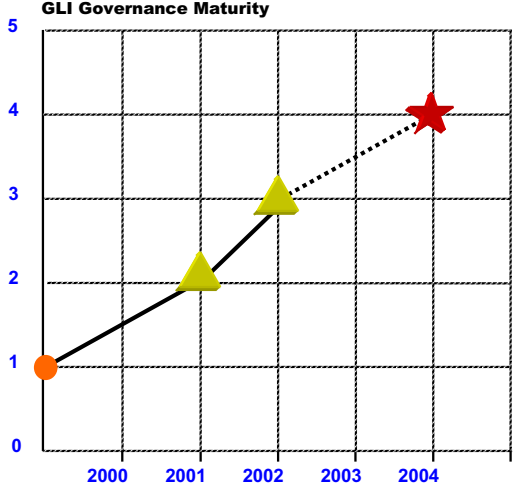
Legend for symbols used

- Starting Point
- Interim Target states
- Organization's strategy for improvement - where the organization wants to be

Legend for rankings used

0 - Management processes are not applied at all
1 - Processes are ad hoc & disorganized
2 - Processes follow a regular pattern
3 - Processes are documented and communicated
4 - Processes are monitored and measured
5 - Best practices are followed and automated

GLI Governance Maturity



IT Governance Institute

IT Governance

The IT Governance Institute

- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT– The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

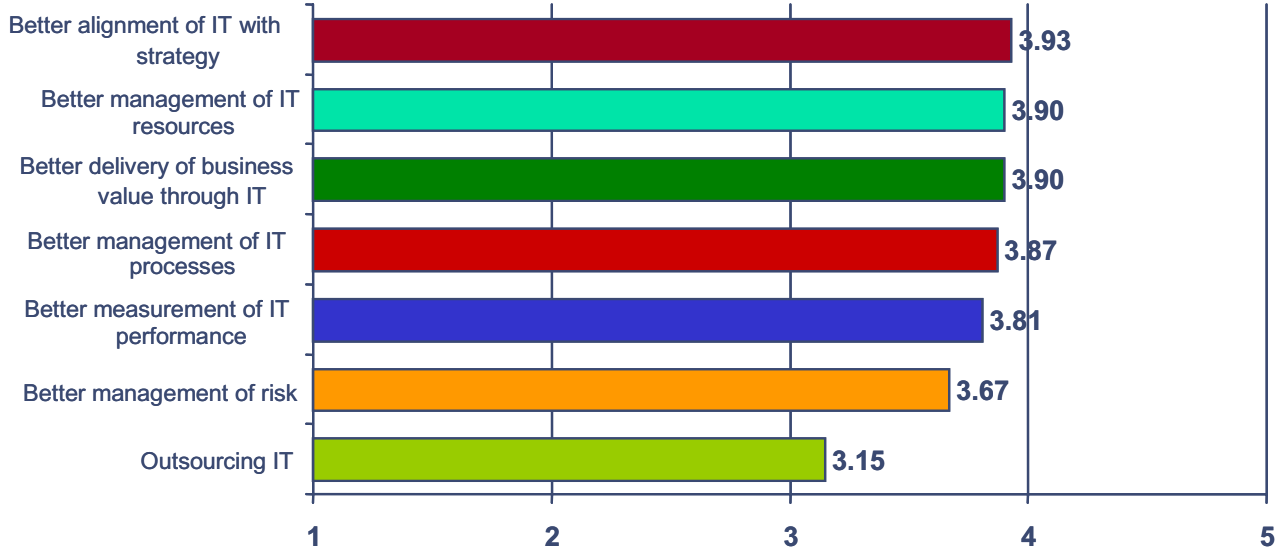
IT GOVERNANCE INSTITUTE

Which IT Governance Practices are in use?

ITGI Survey of 700 CEO/CIO's worldwide by PwC – Oct 2005

IT Governance Institute

Which IT Governance Practices are effective?



ITGI Survey of 700 CEO/CIO's worldwide by PwC – Oct 2005

IT Governance Institute

Why does IT Governance need a framework?

To deal with the complexities of not only ensuring that risks are mitigated, but also ensuring that objectives are achieved

- cost, time and functionality are as expected and promised benefits are returned
- risks are mitigated and resources are responsible managed
- opportunities for process, product and services are leveraged

The solution: a management control framework that

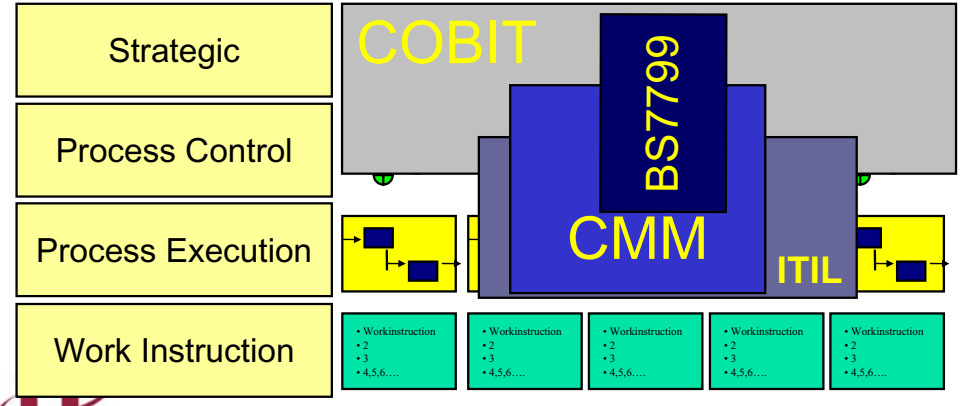
Supplies a common language for IT activities and key management practices	To avoid misunderstandings, to have efficient dialogues and to enable synergy
Provides a business focus and supports governance expectations	To enable alignment between business and IT and engage the executives
Organises IT tasks and activities into discrete processes	To define scope, responsibilities and extent of coverage
Is consistent with generally accepted IT good practices and corporate governance standards	To be generally acceptable and to have a provably complete basis to select from

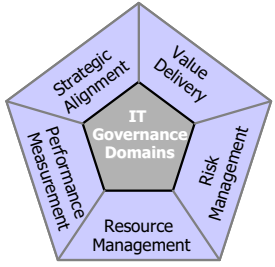
GOVERNANCE INSTITUTE

IT Governance framework candidates

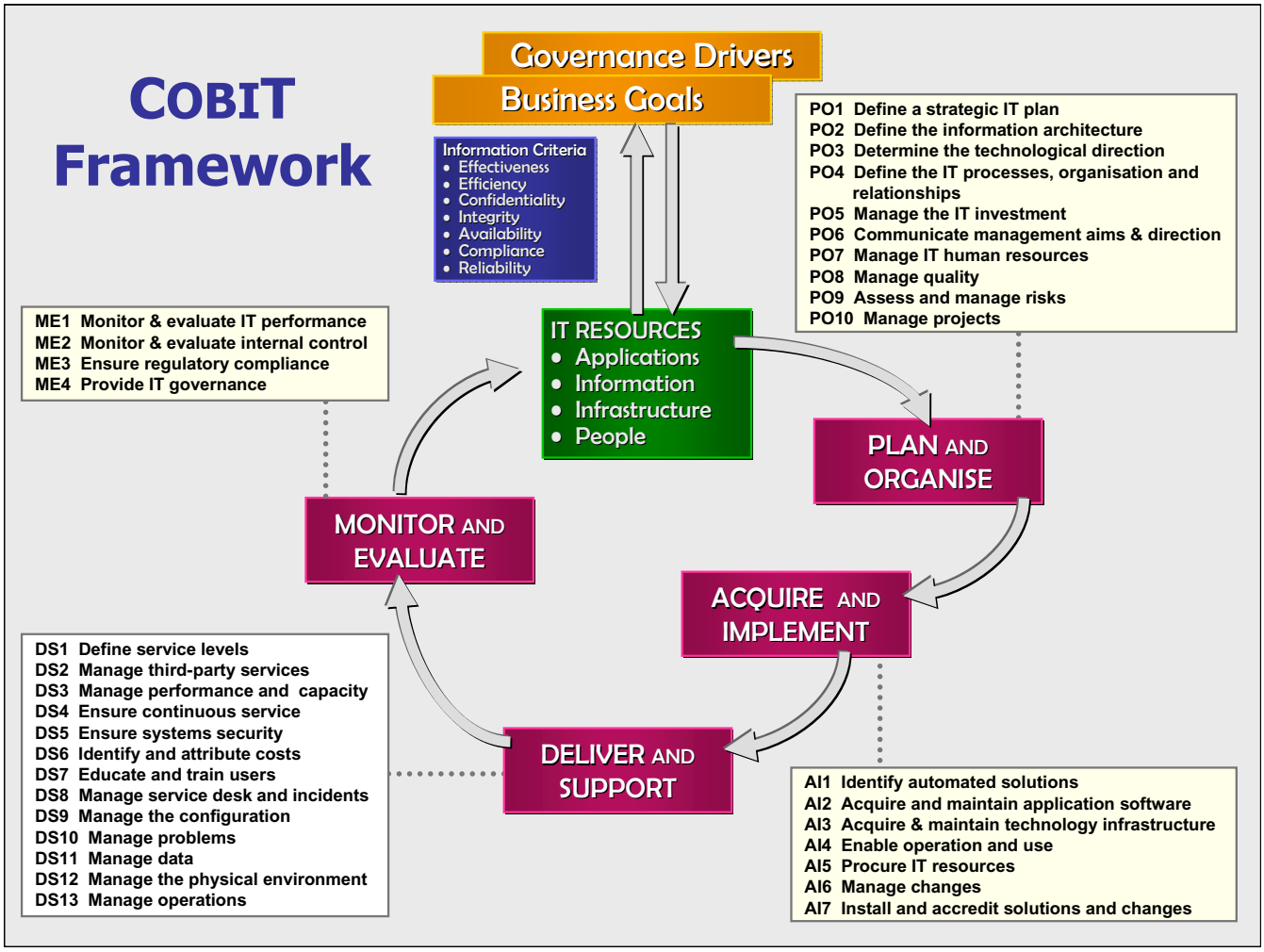
- ITIL for service delivery
- CMM for software development
- Prince2 for project management
- .....

- Governance
- Strategy
- Planning
- Value delivery
- Performance measurement
- Risk management
- Control and assessment





GOVERNANCE INSTITUTE


COBIT Framework
Governance Drivers
Business Goals
Information Criteria
• Effectiveness
• Efficiency
• Confidentiality
• Integrity
• Availability
• Compliance
• Reliability
PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT processes, organisation and relationships
PO5 Manage the IT investment
PO6 Communicate management aims & direction
PO7 Manage IT human resources
PO8 Manage quality
PO9 Assess and manage risks
PO10 Manage projects
ME1 Monitor & evaluate IT performance
ME2 Monitor & evaluate internal control
ME3 Ensure regulatory compliance
ME4 Provide IT governance
IT RESOURCES
• Applications
• Information
• Infrastructure
• People
PLAN AND ORGANISE
MONITOR AND EVALUATE
ACQUIRE AND IMPLEMENT
DS1 Define service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and attribute costs
DS7 Educate and train users
DS8 Manage service desk and incidents
DS9 Manage the configuration
DS10 Manage problems
DS11 Manage data
DS12 Manage the physical environment
DS13 Manage operations
DELIVER AND SUPPORT
AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire & maintain technology infrastructure
AI4 Enable operation and use
AI5 Procure IT resources
AI6 Manage changes
AI7 Install and accredit solutions and changes

COBIT - The Emerging IT Governance Framework

Each of the 34 IT processes, while referring to the major business requirement supported and the important resources leveraged, is provided with:

- **Control Objectives** describing the characteristics of a well governed process
- **Control Practices** providing more details on how to implement
- **Performance Metrics** to track process goals and actual performance
- **Critical Success Factors** for managing processes efficiently and effectively
- **Maturity Models** to support continuous improvement planning

IT GOVERNANCE INSTITUTE

Free download from www.isaca.org

IT Governance

The IT Governance Institute

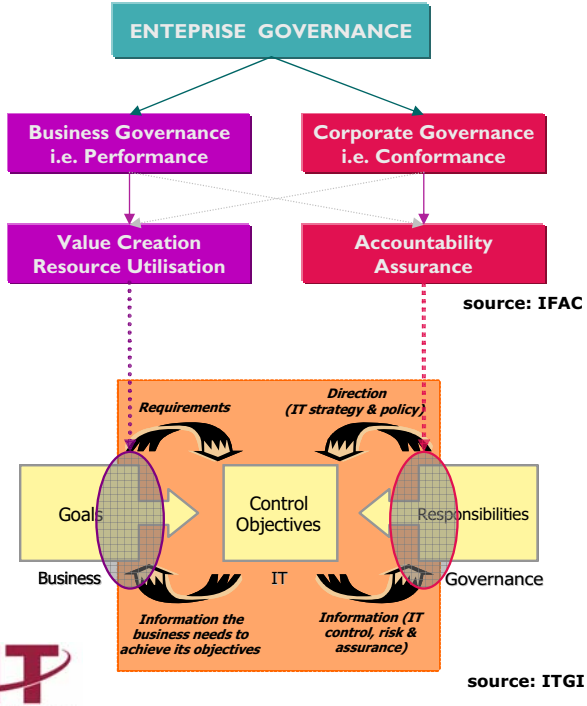
- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

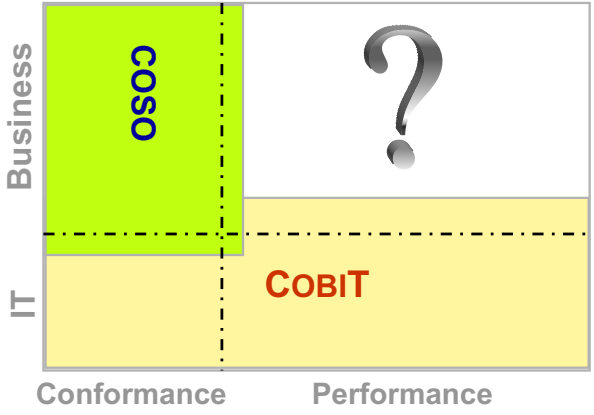
IT GOVERNANCE INSTITUTE

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

CobiT and COSO

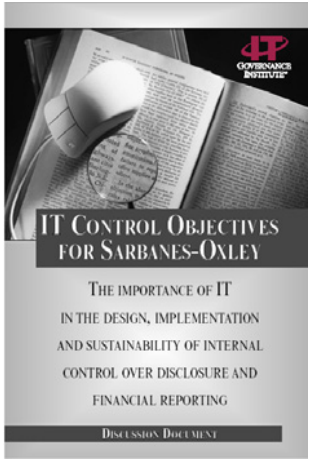




GOVERNANCE INSTITUTE

CobiT and COSO

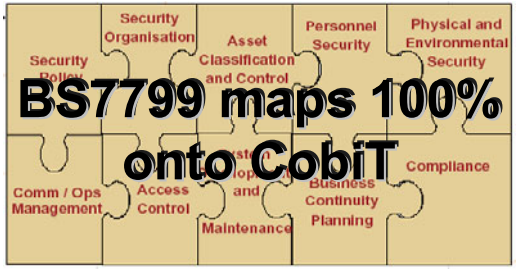
Sarbanes-Oxley Compliance initiatives have shown that COSO and CobiT are complimentary.

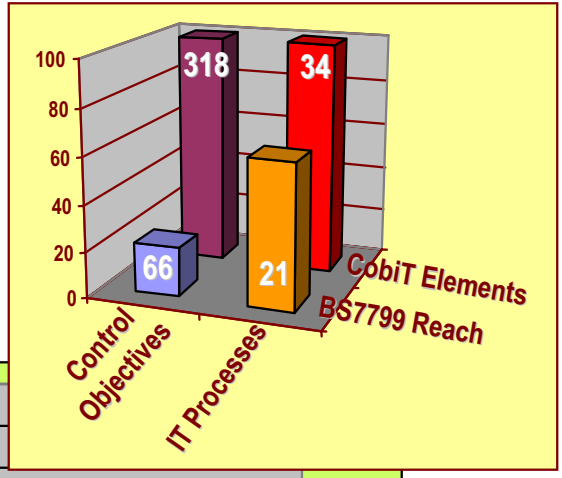


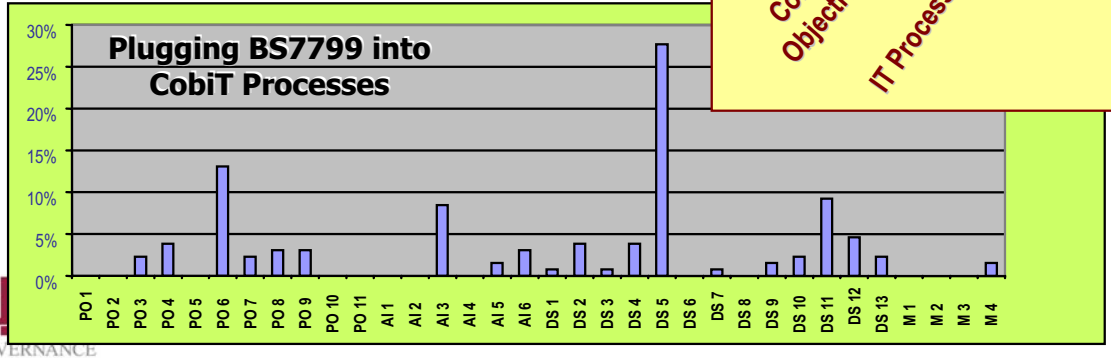
IT Governance Institute

CobiT Control Objectives	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plann and Organize					
Define a strategic IT plan.		●		●	●
Define the information architecture.			●	●	
Determine technological direction.					
Define the IT organization and relationships.	●			●	
Manage the IT investment.					
Communicate management aims and direction.	●			●	●
Manage human resources.	●			●	
Ensure compliance with external requirements.				●	●
Assess risks.		●			
Manage projects.					
Manage quality.	●		●	●	●
Acquire and Implement					
Identify automated solutions.					
Acquire and maintain application software.			●		
Acquire and maintain technology infrastructure.			●		
Develop and maintain procedures.			●	●	
Install and accredit systems.			●		
Manage changes.			●		●
Deliver and Support					
Define and manage service levels.	●		●		●
Manage third-party services.	●	●	●		●
Manage performance and capacity.			●		
Ensure continuous service.			●		●
Ensure systems security.			●	●	●
Identify and allocate costs.					
Educate and train users.	●			●	
Assist and advise customers.					
Manage the configuration.			●	●	
Manage problems and incidents.			●	●	●
Manage data.			●	●	
Manage facilities.			●		
Manage operations.			●	●	
Monitor and Evaluate					
Monitor the processes.				●	●
Assess internal control adequacy.					●
Obtain independent assurance.	●				●
Provide for independent audit.					

CobiT and ISO17799







CobiT and ITIL

Gartner Advisory

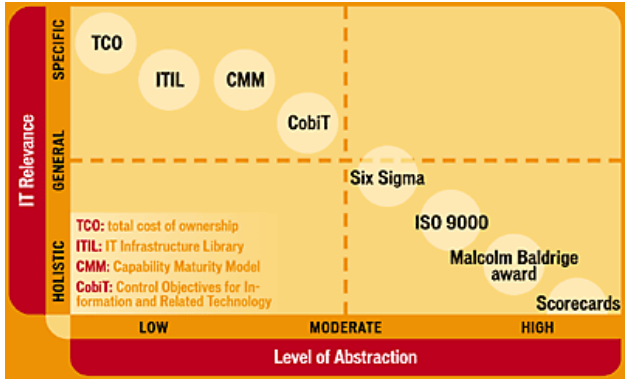
Tactical Guidelines, TG-16-1849
S. Mingay, S. Bittinger

Research Note
10 June 2002

Combine CobiT and ITIL for Powerful IT Governance

Strong framework tools are essential for ensuring IT resources are aligned with an enterprise's business objectives, and that services and information meet quality, fiduciary and security needs.

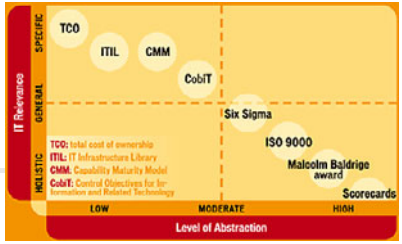
Bottom Line: CobiT and ITIL are not mutually exclusive and can be combined to provide a powerful IT governance, control and best-practice framework in IT service management. Enterprises that want to put their ITIL program into the context of a wider control and governance framework should use CobiT.

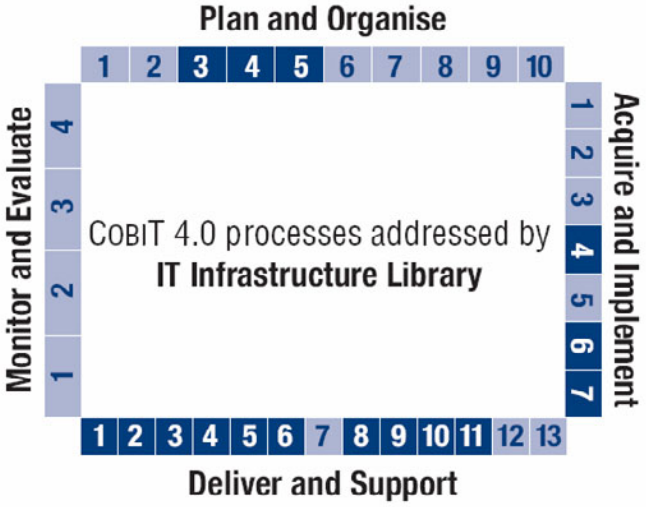


- CobiT and other standards
  - Integrator of technical standards
  - Interface to business standards
  - Generally accepted "de facto" standard

GOVERNANCE INSTITUTE

CobiT and ITIL



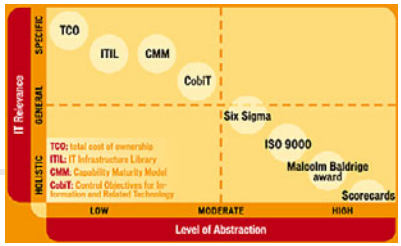


Legend:
Requirements of the CobiT process are…

- …frequently addressed
- …not or rarely addressed

GOVERNANCE INSTITUTE

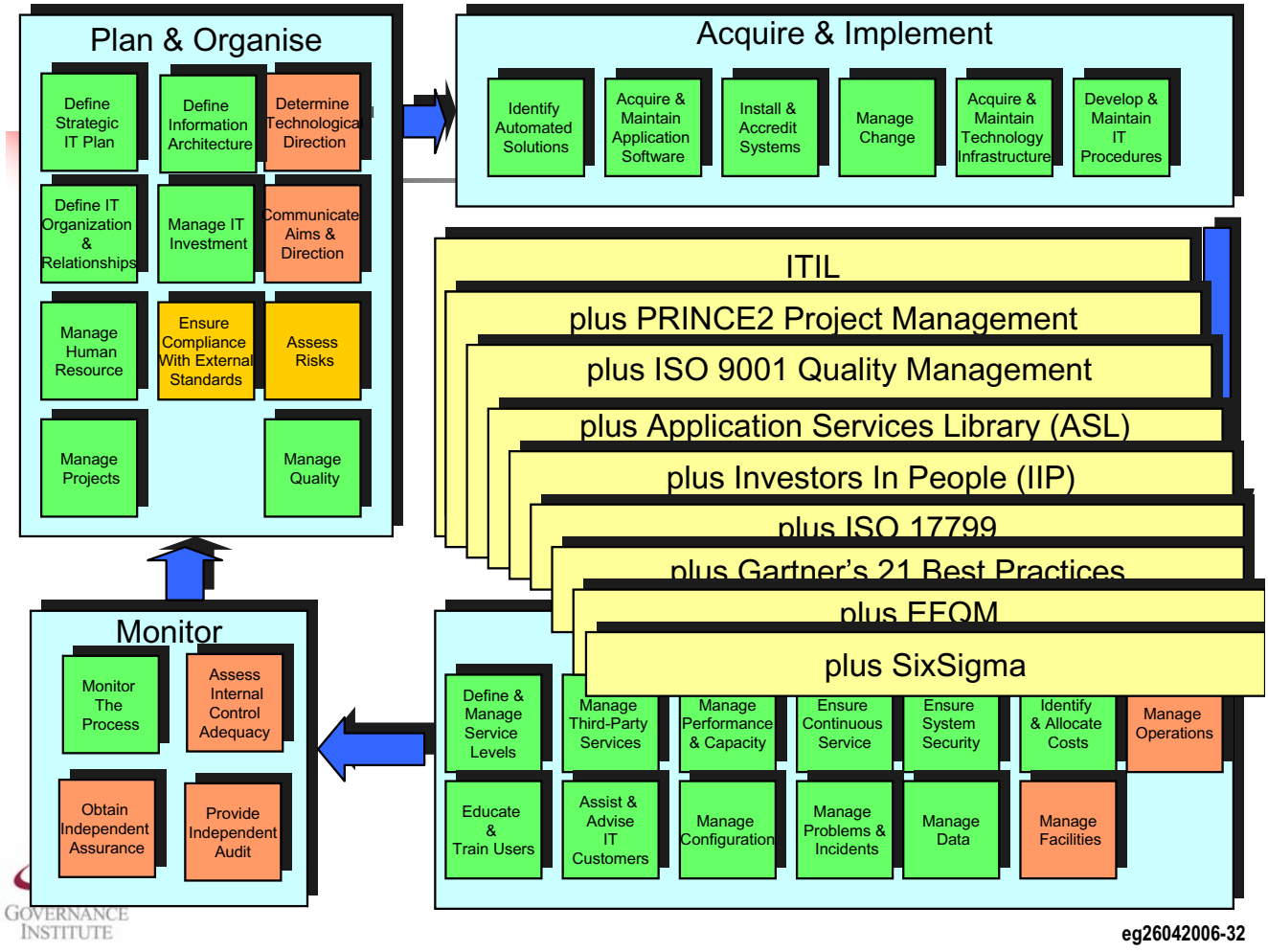
CobiT, ITIL and ISO17799



COBIT Domain: Acquisition & Implementation AI6: Manage Changes			
Managing changes With the business goal of minimising the likelihood of disruption, unauthorised alterations and errors... Is enabled by a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure			
COBIT Control Ref.	Keywords	ITIL mapping	ITIL mapping
Change Request initiation and Control	RFC; formal Change Management; Change categories; priorities; status; urgency	Basic concepts of Change Management (SS 8.3) Activities (SS 8.5)	8.5.1 Change control procedures
Impact assessment	Impact analysis (system & functionality); Change assessment	Scope of Change Management (SS 8.2) Impact & Resource Assessment (SS 8.5.6)	8.5.1 Change control procedures
Control of Changes	Change management, Software Control & Distribution, Configuration Management integrated; Changes recorded & tracked		8.5.3 Restrictions on changes to software packages 8.5.1 Change control procedures
Emergency Changes	Management assessment	Scope of Change Management (SS 8.2) Change Advisory Board (SS 8.3.2)	8.5.1 Change control procedures
Documentation and Procedures	Change implementation; documentation updates	Change Management (SS 2.2) Scope of Change Management (SS 8.2)	8.5.1 Change control procedures
Authorised Maintenance	System access rights; risk avoidance		8.5.1 Change control procedures
Software Release Policy	Release approval; sign-off; regression testing; handover	Scope of Release Management (SS 9.2)	8.5.1 Change control procedures
Distribution of Software	Internal controls; integrity; audit trails		8.5.1 Change control procedures

- Management Awareness
- Joint publication ITGI and OGC
- Maps CobiT to ITIL and ISO17799
- Follows the CobiT process structure
- Free download www.itgi.org

IT GOVERNANCE INSTITUTE


Plan & Organise
Define Strategic IT Plan
Define Information Architecture
Determine Technological Direction
Define IT Organization & Relationships
Manage IT Investment
Communicate Aims & Direction
Manage Human Resource
Ensure Compliance With External Standards
Assess Risks
Manage Projects
Manage Quality
Acquire & Implement
Identify Automated Solutions
Acquire & Maintain Application Software
Install & Accredit Systems
Manage Change
Acquire & Maintain Technology Infrastructure
Develop & Maintain IT Procedures
ITIL
plus PRINCE2 Project Management
plus ISO 9001 Quality Management
plus Application Services Library (ASL)
plus Investors In People (IIP)
plus ISO 17799
plus Gartner's 21 Best Practices
plus EFQM
plus SixSigma
Monitor
Monitor The Process
Assess Internal Control Adequacy
Obtain Independent Assurance
Provide Independent Audit
Define & Manage Service Levels
Manage Third-Party Services
Manage Performance & Capacity
Ensure Continuous Service
Ensure System Security
Identify & Allocate Costs
Manage Operations
Educate & Train Users
Assist & Advise IT Customers
Manage Configuration
Manage Problems & Incidents
Manage Data
Manage Facilities
GOVERNANCE INSTITUTE
eg26042006-32

IT Governance

The IT Governance Institute

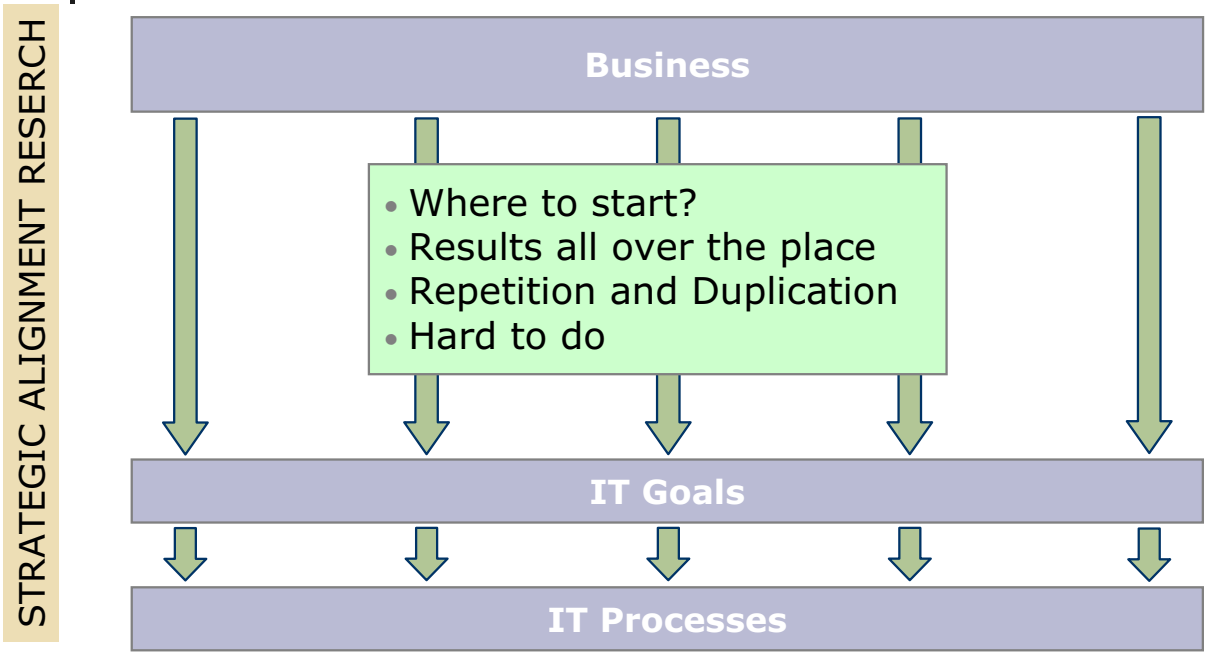
- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

IT GOVERNANCE INSTITUTE

AGENDA

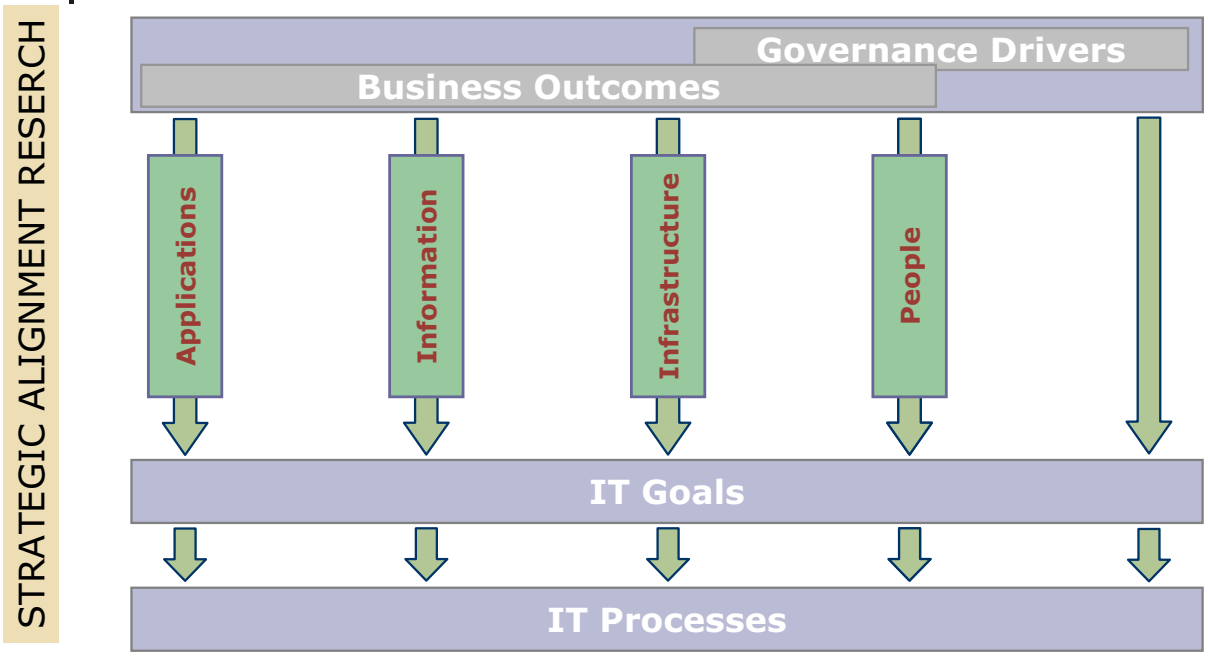
- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

How Do Governance and the Business Drive IT?



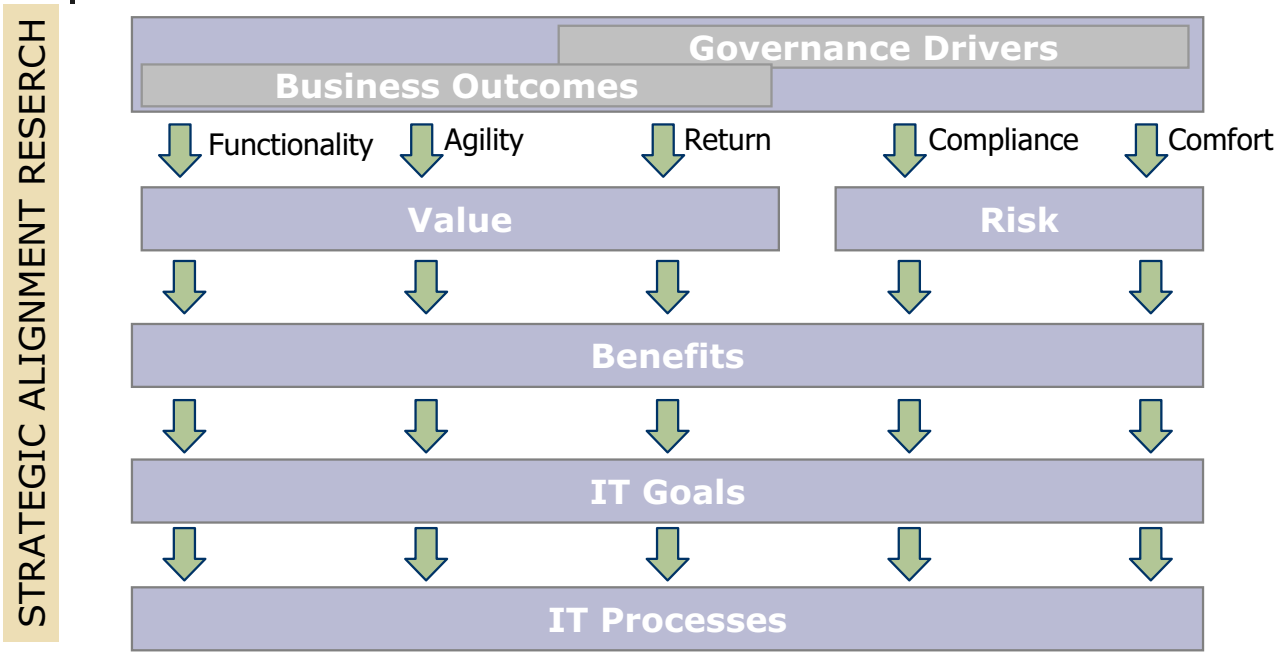
IT Governance Institute

How Do Governance and the Business Drive IT?



GOVERNANCE INSTITUTE

How Do Governance and the Business Drive IT?



GOVERNANCE INSTITUTE

How do governance and the business drive IT?

BUSINESS GOALS

Financial perspective	Expand market share
	Increase revenue
	Return on investment
	Optimise asset utilisation
	Manage business risks
Customer perspective	Improve customer orientation and service
	Offer competiteve products and services
	Service Availability
	Agility in responding to changing business requirements (time to market)
	Cost optimisation of service delivery
Internal perspective	Automate and integrate the enterprise value chain
	Improve and maintain business process functionality
	Lower process costs
	Compliance with external laws and regulations
	Transparency
	Compliance with internal policies
	Improve and maintain operational and staff productivity
Learning and growth perspective	Product/business innovation
	Obtain reliable and useful information for strategic decision making
	Acquire and maintain skilled and motivated personnel

IT Governance Institute

How do governance and the business drive IT?

IT GOALS

1	Respond to business requirements in alignment with the business strategy
2	Respond to governance requirements in line with board direction
3	Ensure satisfaction of end-users with service offerings and service levels
4	Optimise use of information
5	IT Agility
6	Define how business functional and control requirements are translated in effective and efficient automated solutions
7	Acquire and maintain integrated and standardised application systems
8	Acquire and maintain an integrated and standardised IT infrastructure
9	Acquire and maintain IT skills that respond to the IT strategy
10	Ensure mutual satisfaction of third-party relationships
11	Seamlessly integrate applications and technology solutions into business processes
12	Transparency and understanding of IT cost, benefits, strategy, policies and service levels
13	Ensure proper use and performance of the applications and technology solutions
14	Account for and protect all IT assets
15	Optimise the IT infrastructure, resources and capabilities
16	Reduce solution and service delivery defects and rework
17	Protect the achievement of IT objectives
18	Establish clarity of business impact of risks to IT objectives and resources
19	Ensure critical and confidential information is withheld from those who should not have access to it
20	Ensure automated business transactions and information exchanges can be trusted
21	Ensure IT services and the IT infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster
22	Ensure minimum business impact in the event of an IT service disruption or change
23	Make sure that IT services are available as required
24	Improve IT's cost efficiency and its contribution to business profitability
25	Deliver projects on time and on budget meeting quality standards
26	Maintain the integrity of information and processing infrastructure
27	Ensure IT compliance with laws and regulations
28	IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change

IT GOVERNANCE INSTITUTE

Linking Business and IT Goals

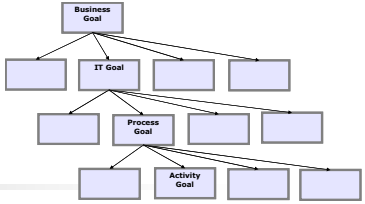
		BUSINESS GOALS	IT Goals									Information Criteria: Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial perspective	1	Expand market share	25	28								✔	✔					
	2	Increase revenue	25	28								✔	✔					
	3	Return on investment	24										✔					
	4	Optimise asset utilisation	14									✔	✔					
	5	Manage business risks	2	14	17	18	19	20	21	22				✔	✔	✔		
Customer perspective	6	Improve customer orientation and service	3	23								✔						
	7	Offer competitive products and services	5	24									✔	✔				
	8	Service Availability	10	16	22	23										✔		
	9	Agility in responding to changing business requirements (time to market)	1	5	25								✔	✔				
	10	Cost optimisation of service delivery	7	8	10	24							✔					
Internal perspective	11	Automate and integrate the enterprise value chain	6	7	8	11						✔	✔					
	12	Improve and maintain business process functionality	6	7	11							✔						
	13	Lower process costs	7	8	13	15	24						✔					
	14	Compliance with external laws and regulations	2	19	20	21	22	26	27					✔			✔	
	15	Transparency	2	10														✔
	16	Compliance with internal policies	2	13										✔			✔	
	17	Improve and maintain operational and staff productivity	7	8	11	13						✔	✔					
Learning and growth perspective	18	Product/business innovation	5	25	28							✔						
	19	Obtain reliable and useful information for strategic decision making	2	4	12	20	26											✔
	20	Acquire and maintain skilled and motivated personnel	9									✔	✔					

GOVERNANCE INSTITUTE

Linking IT Goals to IT Processes

	IT GOALS	Processes										Information Criteria						
												Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	✔			✔	✔		
2	Respond to governance requirements in line with board direction	PO1	PO4	PO10	ME1	ME3						✔	✔	✔			✔	✔
3	Ensure satisfaction of end-users with service offerings and service levels	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			✔						
4	Optimise use of information	PO2	DS11										✔		✔			
5	IT Agility	PO2	PO4	PO7	AI3								✔					
6	Define how business functional and control requirements are translated in effective and efficient automated solutions	AI1	AI2	AI6								✔	✔					
7	Acquire and maintain integrated and standardised application systems	PO3	AI2	AI5		AI2	AI5					✔	✔		✔			
8	Acquire and maintain an integrated and standardised IT infrastructure	AI2	AI5									✔	✔		✔			
9	Acquire and maintain IT skills that respond to the IT strategy	PO7	AI5									✔	✔		✔			
10	Ensure mutual satisfaction of third-party relationships	DS2										✔	✔					
11	Seamlessly integrate applications and technology solutions into business processes	PO2	AI4	AI7								✔			✔	✔		
12	Transparency and understanding of IT cost, benefits, strategy, policies and service levels	PO5	PO6	DS1	DS2	DS6	ME1	ME3				✔	✔				✔	✔
13	Ensure proper use and performance of the applications and technology solutions	PO6	AI4	AI7	DS7	DS8						✔	✔		✔		✔	
14	Account for and protect all IT assets	PO9	DS5	DS9	DS12	ME2							✔				✔	
15	Optimise the IT infrastructure, resources and capabilities	PO3	AI3	DS3	DS7	DS9							✔					
16	Reduce solution and service delivery defects and rework	PO8	AI4	AI6	AI7	DS10						✔	✔		✔	✔		
17	Protect the achievement of IT objectives	PO9	DS10	ME2								✔	✔	✔	✔	✔	✔	✔
18	Establish clarity of business impact of risks to IT objectives and resources	PO9										✔		✔	✔	✔		
19	Ensure critical and confidential information is withheld from those who should not have access to it	PO6	DS5	DS11	DS12									✔			✔	
20	Ensure automated business transactions and information exchanges can be trusted	PO6	AI7	DS5											✔			
21	Ensure IT services and the IT infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster	PO6	DS4	DS5	DS12	DS13	ME2					✔				✔		
22	Ensure minimum business impact in the event of an IT service disruption or change	PO6	AI6	DS4	DS12							✔				✔		
23	Make sure that IT services are available as required	DS3	DS4	DS8	DS13	DS13						✔				✔		
24	Improve IT's cost efficiency and its contribution to business profitability	PO5	AI5	DS6									✔					
25	Deliver projects on time and on budget meeting quality standards	PO8	PO10									✔	✔					
26	Maintain the integrity of information and processing infrastructure	AI6	DS5													✔		
27	Ensure IT compliance with laws and regulations	DS11	ME2	ME3	ME4												✔	
28	IT demonstrates cost efficient service quality, continuous improvement and readiness for future change	PO5	DS6	ME1	ME3													✔

Goals and Metrics



Business Goal	IT Goal	Process Goal	Activity Goal
Maintain enterprise reputation and leadership	Ensure IT Services can resist and recover from attacks	Detect and resolve unauthorised access	Understand security requirements, vulnerabilities and threats
Number of incidents causing public embarrassment	Number of actual IT incidents with business impact	Number of actual incidents because of unauthorised access	Frequency of review of the type of security events to be monitored
Outcome Metric	**Outcome Metric**	**Outcome Metric**	**Outcome Metric**

Business Goal	IT Goal	Process Goal
Maintain enterprise reputation and leadership	Ensure IT Services can resist and recover from attacks	Detect and resolve unauthorised access
Number of actual IT incidents with business impact	Number of actual incidents because of unauthorised access	Frequency of review of the type of security events to be monitored
Performance Metric	**Performance Metric**	**Performance Metric**

IT Governance Institute

eg26042006-41

IT Governance

The IT Governance Institute

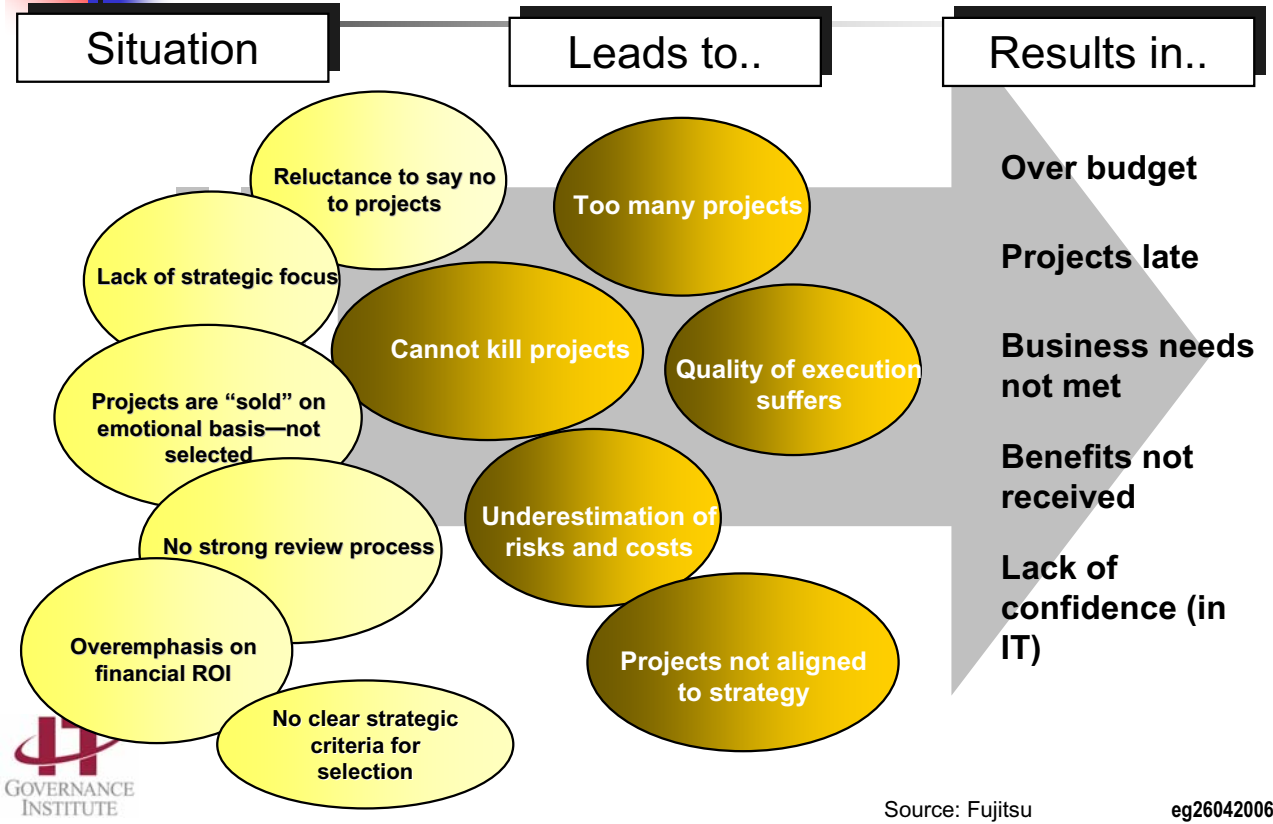
- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

IT GOVERNANCE INSTITUTE

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

Without Effective Value Governance...



GOVERNANCE INSTITUTE

Source: Fujitsu

CobiT - Research

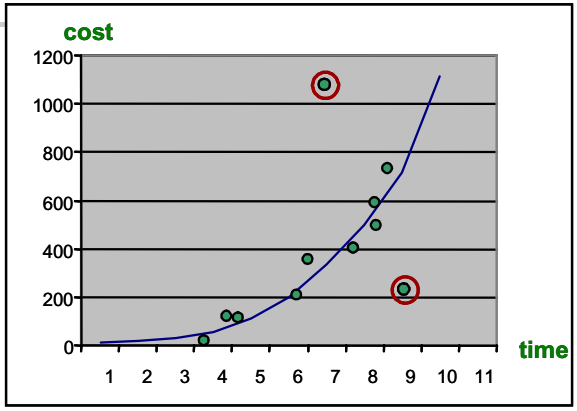
Key is the delivery of IT Value

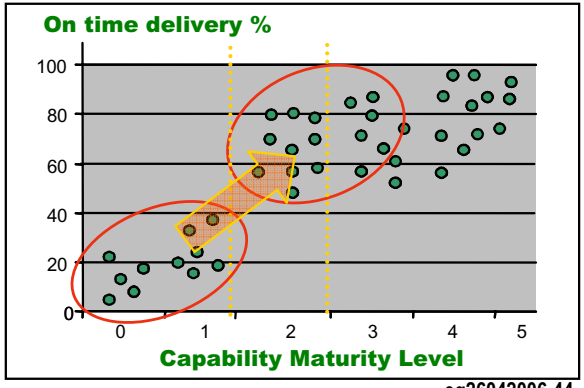
- Comparison of cost vs. duration
- Correlation of delivery vs. capability

COBIT Financials -- VALIT

- Research, develop and promote a free internationally accepted set of good practices for optimising the value of IT enabled change through sound investment decisions, value transparency, cost optimisation and risk management, based on CobiT, supported with empirical data

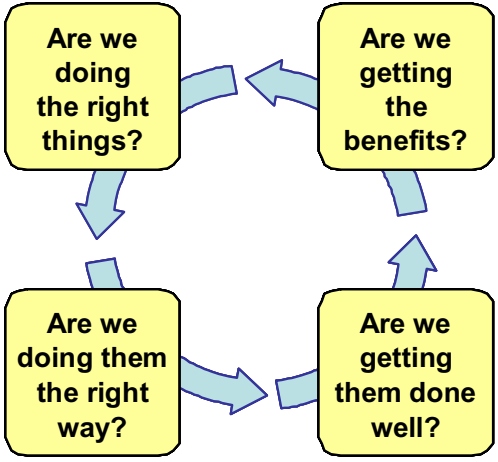
- Principles
- Definitions
- Management Processes
  - IT Value Governance
  - Portfolio Management
  - Investment Management
- Control Objectives <> COBIT





Val IT The 4 "Ares"

Some fundamental questions



about the value delivered by IT

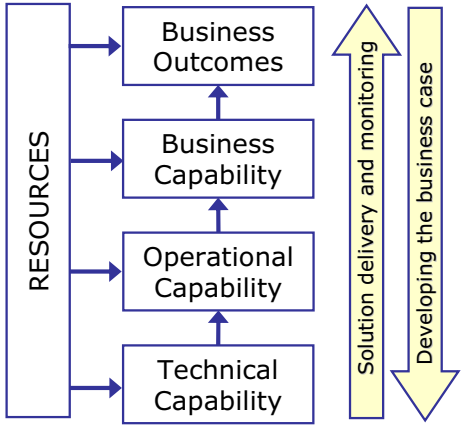
Val IT Principles

- **IT-enabled investments will be managed as** a portfolio of investments.
- **IT-enabled investments will include the** full scope of activities **that are required to achieve business value**.
- **IT-enabled investments will be managed through their** full economic life cycle.
- **Value delivery practices will recognize that there are** different categories of investments **that will be evaluated and managed differently**.
- **Value delivery practices will define and monitor** key metrics **and will respond quickly to any changes or deviations**.
- **Value delivery practices will engage all stakeholders and assign** appropriate accountability **for the delivery of capabilities and the realization of business benefits**.
- **Value delivery practices will be** continually monitored, evaluated and improved.

Val IT Project

Val IT is based on COBIT and deals with:

- Investment in IT-enabled business initiatives
- Taking a portfolio view of projects and programs
- Making and tracking business cases



Why the business case?

- Understanding of what you plan to achieve; how you are going to manage it and who is accountable
- Basis for comparison and choice
- Recording all that needs to be tracked (cost, risks, benefits, etc.)

Why Portfolio Management ?

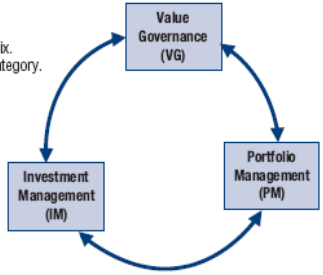
- Portfolios and scorecards are the 'engine' of IT Governance, they provide a global view of programmes and resources

IT Governance Institute

Val IT Framework

3 Processes and 40 Key Management Practices

VG1 Ensure informed and committed leadership.
VG2 Define and implement processes.
VG3 Define roles and responsibilities.
VG4 Ensure appropriate and accepted accountability.
VG5 Define information requirements.
VG6 Establish reporting requirements.
VG7 Establish organisational structures.
VG8 Establish strategic direction.
VG9 Define investment categories.
VG10 Determine a target portfolio mix.
VG11 Define evaluation criteria by category.



PM1 Maintain a human resource inventory.
PM2 Identify resource requirements.
PM3 Perform a gap analysis.
PM4 Develop a resourcing plan.
PM5 Monitor resource requirements and utilisation.
PM6 Establish an investment threshold.
PM7 Evaluate the initial programme concept business case.
PM8 Evaluate and assign a relative score to the programme business case.
PM9 Create an overall portfolio view.
PM10 Make and communicate the investment decision.
PM11 Stage-gate (and fund) selected programmes.
PM12 Optimise portfolio performance.
PM13 Re-prioritise the portfolio.
PM14 Monitor and report on portfolio performance.

IM1 Develop a high-level definition of investment opportunity.
IM2 Develop an initial programme concept business case.
IM3 Develop a clear understanding of candidate programmes.
IM4 Perform alternatives analysis.
IM5 Develop a programme plan.
IM6 Develop a benefits realisation plan.
IM7 Identify full life cycle costs and benefits.
IM8 Develop a detailed programme business case.
IM9 Assign clear accountability and ownership.
IM10 Initiate, plan and launch the programme.
IM11 Manage the programme.
IM12 Manage/track benefits.
IM13 Update the business case.
IM14 Monitor and report on programme performance.
IM15 Retire the programme.

Val IT Framework

Process: Value Governance (VG)

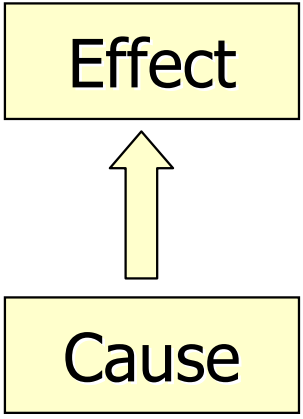
Process Description	Key Management Practices	CobiT Cross-references	RACI Chart		
			Exec	Bus	IT
Establish governance, monitoring and control framework. Establish strategic direction. Establish portfolio characteristics.	*VG1 Ensure informed and committed leadership.* The reporting line of the CIO should be commensurate with the importance of IT within the enterprise. All executives should have a sound understanding of strategic IT issues, such as dependence on IT, and technology insights and capabilities, so there is a common and agreed understanding between the business and the IT function regarding the potential impact of IT on the business strategy. The business and IT strategy should be integrated, clearly linking enterprise goals and IT goals, and should be broadly communicated.	Primary: PO1.2, PO1.4, PO4.4, ME4.1, ME4.2	A/R	C	C
	VG2 Define and implement processes. Define, implement and consistently follow processes that provide for clear and active linkage amongst the enterprise strategy, the portfolio of IT-enabled investment programmes that execute the strategy, the individual investment programmes, and the business and IT projects that make up the programmes. The processes should include planning and budgeting, prioritisation of planned and current work within the overall budget, resource allocation consistent with the priorities, stage-gating of investment programmes, monitoring and communicating performance, taking appropriate remedial action, and benefits management so there is an optimal return on the portfolio and on all IT assets and services.	Primary: PO4.1, ME1.1, ME1.3, ME4.1 Secondary: PO5.2, PO5.3 PO5.4, PO5.5, PO10.2	A	R	C
	VG3 Define roles and responsibilities. Define and communicate roles and responsibilities for all personnel in the enterprise in relation to the portfolio of IT-enabled business investment programmes, individual investment programmes, and other IT assets and services to allow sufficient authority to exercise the roles and responsibilities assigned. These roles should include, but not necessarily be limited to, an investment decision body, programme sponsorship, programme management, project management and associated support roles. Provide the business with procedures, techniques and tools enabling it to address its responsibilities. Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and other stakeholders inside and outside the enterprise.	Primary: PO4.6, PO4.15 Secondary: PO4.8, PO4.9, PO10.1, PO10.2	A	R	C

IT GOVERNANCE INSTITUTE

Val IT Deliverables

Empirical Analysis – Cause/Effect

- End Results
  - The on-time delivery of projects
  - Completeness of functionality delivery
  - The on-budget delivery of projects
  - Customer satisfaction
  - Benefits for end user
  - Risk-adjusted return (final project output).
  - Risk-adjusted return for a portfolio
- Drivers
  - CobiT and ValIT maturity level
  - Project size and funding model
  - Portfolio size and mix
  - Business unit size, staff and cost profile
  - Governance practices
  - Organisational structures
  - Transparency level



IT Governance Institute

Val IT Deliverables

Empirical Analysis – Pilot results

Major IT Value Drivers

- Intelligent application of processes as defined in CobiT and ValIT
- Process maturity
- IT Intensity and project size but only in combination with the above
- Outsourcing cost

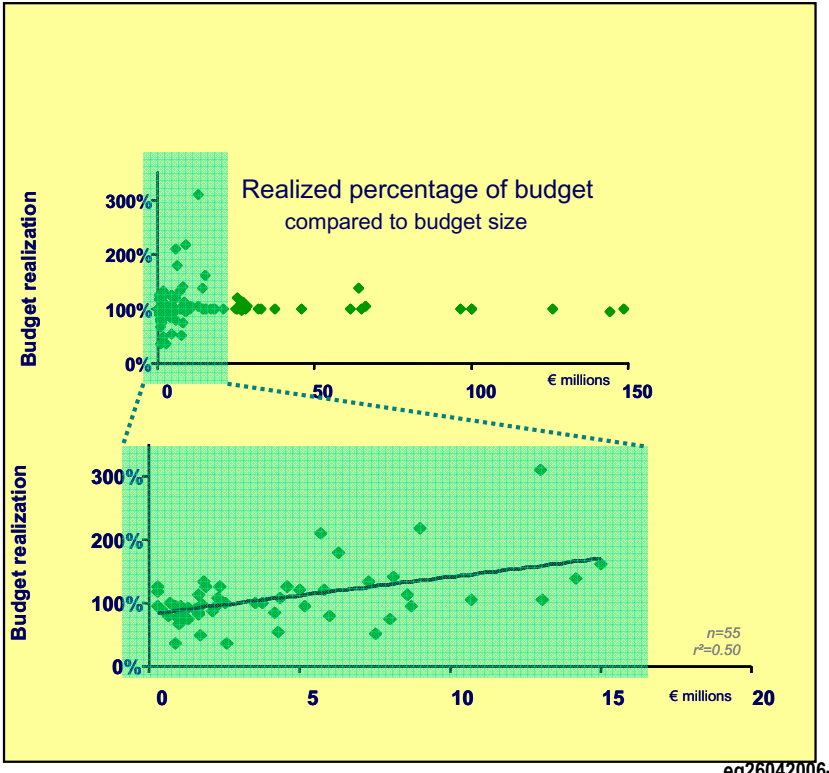
Key Findings

- CMM improvement
- Greater control over smaller projects through PMOs
- Do more risky projects but with tight risk mitigation strategies
- Full financial and risk transparency
- Factoring budget overruns and late delivery into return expectations

Big and risky projects do well
Medium sized and informational don't

Larger projects
up to a certain size tend to overrun more.

Very large projects
are likely to be subject to greater management attention and tend to stay within budget.



GOVERNANCE INSTITUTE

eg26042006-52

Big and risky projects do well
Medium sized and informational don't

	Correlation coefficient
High-risk IT-projects are attractive because:	
Internal Rate of Return is high	**+0.28**
Business demand is high	**+0.29**
Innovativeness of the solution is high	**+0.53**
Strategic impact is high	**+0.48**
The risk of failure or budget overrun is lowered by:	
Fit with strategy	**-0.10**
Synergy with existing infrastructure	**-0.32**
Commitment of top management	**-0.22**

IT GOVERNANCE INSTITUTE

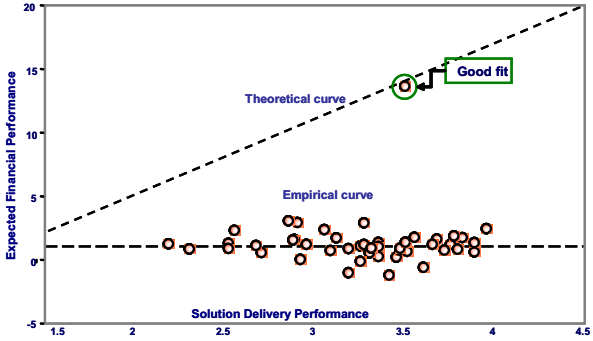
We don't learn from our past

ROI as expected in the Business Case

Expected Benefits

Budgeted ROI = (€114 m - € 100 m) / € 100 m * 100% = + 14%

Expected Budget



Actual ROI allowing for typical solution delivery performance

Functionality achieved -16%

Approximately two years delay, so benefits discounted at 12% After - Tax Rate

€211m

Actual ROI = (€ 114 m x 84 % x (1 / 1.12)^2 - € 100 m x 124 %) / (€ 100 m x 124 %) * 100 %= - 38% → + 14%

Budget Overrun +24%

IT Governance Institute

eg26042006-54

Why is it not being done?

- **We are good at apportioning blame after the fact for the bad things that we did not plan to happen.**
- **We are bad at assigning accountability beforehand for the good things we do plan to happen.**

What do CIOs say?

Val IT Principles

	Results CIO Interviews
IT-enabled investments will be managed as a portfolio of investments.	
IT-enabled investments will include the full scope of activities **that are required to achieve business value**.	
IT-enabled investments will be managed through their full economic life cycle.	
Value delivery practices will recognize that there are different categories of investments **that will be evaluated and managed differently**.	
Value delivery practices will define and monitor key metrics **and will respond quickly to any changes or deviations**.	
Value delivery practices will engage all stakeholders and assign appropriate accountability **for the delivery of capabilities and the realization of business benefits**.	
Value delivery practices will be continually monitored, evaluated and improved.	

IT Governance

The IT Governance Institute

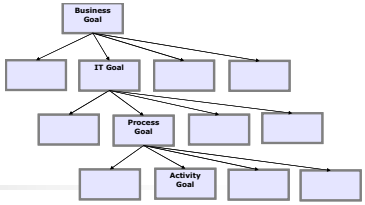
- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

IT GOVERNANCE INSTITUTE

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

Goals and Metrics



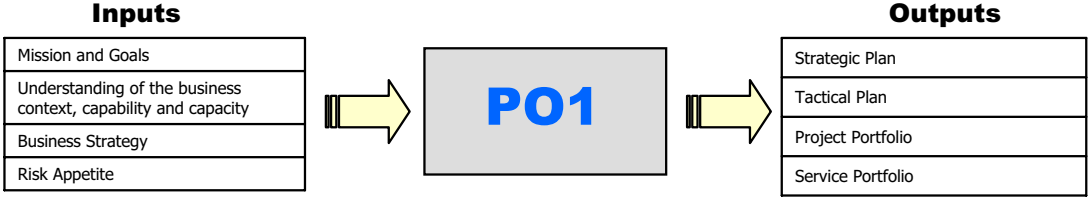
Business Goal	IT Goal	Process Goal	Activity Goal
Maintain enterprise reputation and leadership	Ensure IT Services can resist and recover from attacks	Detect and resolve unauthorised access	Understand security requirements, vulnerabilities and threats
Number of incidents causing public embarrassment	Number of actual IT incidents with business impact	Number of actual incidents because of unauthorised access	Frequency of review of the type of security events to be monitored
Outcome Metric	**Outcome Metric**	**Outcome Metric**	**Outcome Metric**

Business Goal	IT Goal	Process Goal
Maintain enterprise reputation and leadership	Ensure IT Services can resist and recover from attacks	Detect and resolve unauthorised access
Number of actual IT incidents with business impact	Number of actual incidents because of unauthorised access	Frequency of review of the type of security events to be monitored
Performance Metric	**Performance Metric**	**Performance Metric**

IT Governance Institute

Process Relationships and RACI Charts

Process inputs and deliverables describe the activity flow and process relationships



Major activities and associated responsibilities are added with a RACI Chart.

RACI Chart

PO1

Key Activities	CEO	CFO	Business Exec	CIO	Business Sr Mngmt	Head Operations	Chief Architect	Head Development	Head IT Admin	PMO	CARS
1 Link business goals to IT goals	C	I	A/R	R	C						
2 Identify critical dependencies and current performance	C	C	R	A/R	C	C	C	C	C		C
3 Build IT strategic plan	A	C	C	R	I	C	C	C	C	I	C
4 Build IT tactical plans	C	I		A	C	C	C	C	C	R	I
5 Analyze and manage project and service portfolios	C	I	I	A	R	R	C	R	C	C	I

GOVERNANCE INSTITUTE

COBIT - The Emerging IT Governance Framework

CobiT4.0 is providing a better interface to the business and IT Governance layer of the enterprise but also to the operational layer with a better interface to operational standards and practices

- *Full IT governance framework* and IT governance best practices to foster compliance and increase the value of IT
- *Stronger business focus* and more specificity on process ownership and responsibilities, enabling strategic alignment and making implementation easier
- Easier to *design IT scorecards* with goals and metrics material with greater focus on process performance via the key activitites
- Better understanding of *scope and purpose of IT processes* with process definitions, relationships, activities and responsibilities
- Key elements remain *Control Objectives, Control Practives and Maturity Models*

GOVERNANCE INSTITUTE

COBIT4.0

IT Governance

- Portfolio Management
- IT Steering Committees
- Investment Decision Making
- Business cases
- Risk Tolerance

Implementation

- Process relationships
- Key activities and RACI charts
- Goals and metrics towards a Balanced Scorecard
- Detailed Control Practices

GOVERNANCE INSTITUTE

IT Governance

The IT Governance Institute

- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Management Audit Approach
- Conclusions

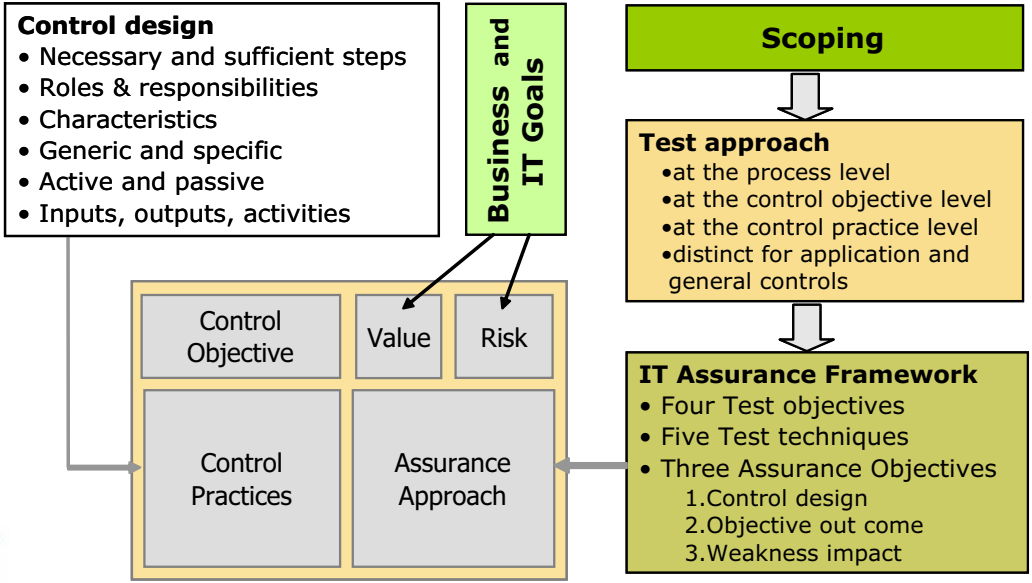
IT GOVERNANCE INSTITUTE

COBIT4.1

- New control practices
- Control design and assurance framework
- Detailed assurance steps
- Extensive assurance advice
- Implementation and Assurance Processes Aligned
- IT Control scoping

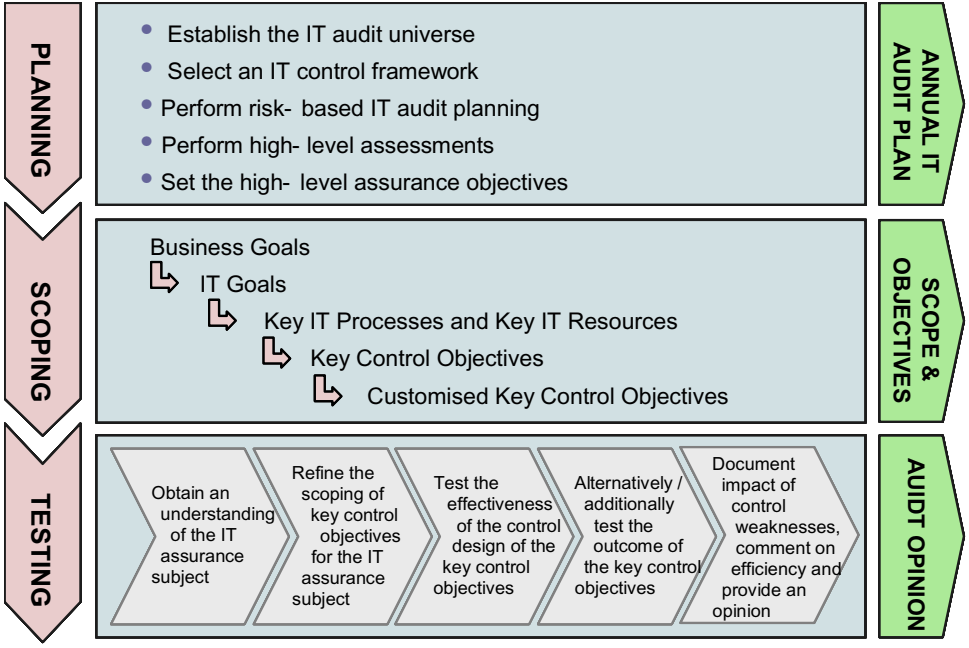
COBIT4.1

IT Control Practices and Assurance Steps

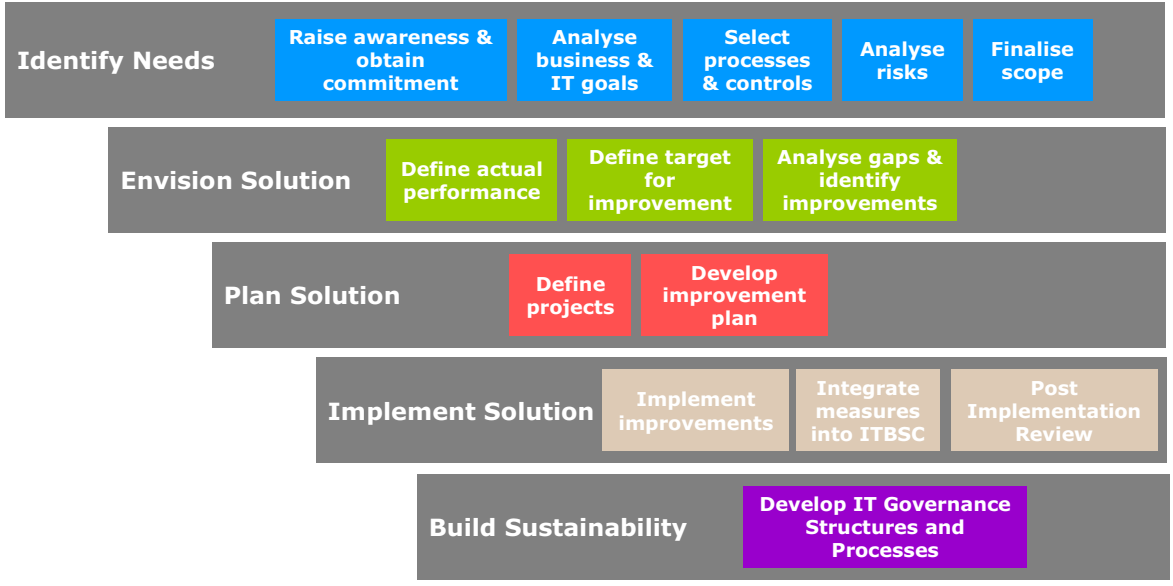


GOVERNANCE INSTITUTE

COBIT4.1 – IT Assurance Roadmap



COBIT4.1 –Implementation Roadmap



IT GOVERNANCE INSTITUTE

IT Governance

The IT Governance Institute

- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Governance Audit Approach
- Conclusions

IT Governance Institute

Five IT governance questions for the Board

	IT Governance Concerns	Where you are	1	2	3	4	5	Where you want to be
1	VALUE	2	It is viewed as a cost				IT is a value enabler	2
2	TRANSPARENCY	1	Uncertainty about risks and value outcome				Risk and value outcomes are predictable	1
3	PERFORMANCE	4	IT issues create aggravation				Comfortable about IT's abilities and performance	4
4	ENABLEMENT	5	IT is largely a technical problem				IT primarily seen as a business opprtunity	5
5	AGILITY	3	IT is inflexible				IT is agile and responsive	3
		1,5						1,5

GOVERNANCE INSTITUTE

Ten process questions for Management

	< Process Name >	Status	1	2	3	4	5
1	Is the IT process important to the success of the enterprise?		Critical	Very significant	Makes things easier	Can survive without it if need be	Not at all
2	Is it clear who is ultimately accountable for the end-result?		Everyone knows	Person knows and accepts	Person knows	Person suspects	Not clear at all
3	Is the process being performed in a formal manner?		All aspects documented	All aspects repeatable	Some aspects documented	Some aspects repeatable	Not at all
4	Is the process being performed well?		All is done well always	Parts are always done well	All aspects sometimes	Some aspects sometimes	Some aspects rarely
5	Is it clear who is responsible for the process?		Everybody knows; responsible fully accepts	Most people know; responsible largely accepts	Some know; responsible partially accepts	Some know; responible knows but does not accept	Nobody knows
6	Does the process have clear direction and goals?		Integrated in performance mesurement	Communicated not linked to measures	Documented but not communicated	Known by senior management; not documented	Not at all
7	Is the process measured?		Integrated and linked to IT and business goals	Efficiency and effectiveness, not linked to goals	Some effectiveness measures	Some financial measures	Not at all
8	Is the process audited?		Risk based and results always actioned	Part of risk based plan and results regularly actioned	Regularly & results occasionally actioned	Ad hoc	Not at all
9	Does the process have known control weaknesses?		Continuously monitored and mitigated	Regularly monitored and many under control	Recognised but not yet treated	Aware we need to do something about it	Don't know if there are weaknesses
10	Does the technology used have vulnerabilities?		Continuously monitored and mitigated	Regularly monitored and many under control	Recognised but not yet treated	Aware we need to do something about it	Don't know if there are vulnerabilities
	Overall Assessment	**0**					

Ten Value Questions To Ask the Executive

1. Is the company getting adequate return from its investment in information resources?
2. Does the firm have the appropriate IT to exploit its intellectual assets?
3. Does the firm have management practices to guard against technology obsolescence?
4. Does the company have adequate security to protect its information assets?
5. Does the company have management processes to ensure 24/7 service levels?
6. Are processes in place to exploit discovery and execution of IT strategic opportunities?
7. Are processes in place to ensure that an IT failure will not damage the business?
8. Is benchmarking a standard practice to ensure the company's competitive cost structure?
9. Are procedures in place to ensure against costly lawsuits?
10. Are processes in place to ensure against IT-based surprises to senior management?

IT GOVERNANCE INSTITUTE

Four Elaborate Questions to ask Business and IT Management

Are we doing the right things?

The ***strategic*** question. Is the investment:

- In line with our vision
- Consistent with our business principles
- Contributing to our strategic objectives
- Providing optimal value, at affordable cost, at an acceptable level of risk

Are we doing them the right way?

The ***architecture*** question. Is the investment:

- In line with our architecture
- Consistent with our architectural principles
- Contributing to the population of our architecture
- In line with other initiatives

Are we getting them done well?

The ***delivery*** question. Do we have:

- Effective and disciplined delivery and change management processes
- Competent and available technical and business resources to deliver:
  - The required capabilities
  - The organizational changes required to leverage the capabilities

Are we getting the benefits?

The ***value*** question. Do we have:

- A clear and shared understanding of the expected benefits
- Clear accountability for realizing the benefits
- Relevant metrics
- An effective benefits realization process

IT Governance Institute

IT Governance

The IT Governance Institute

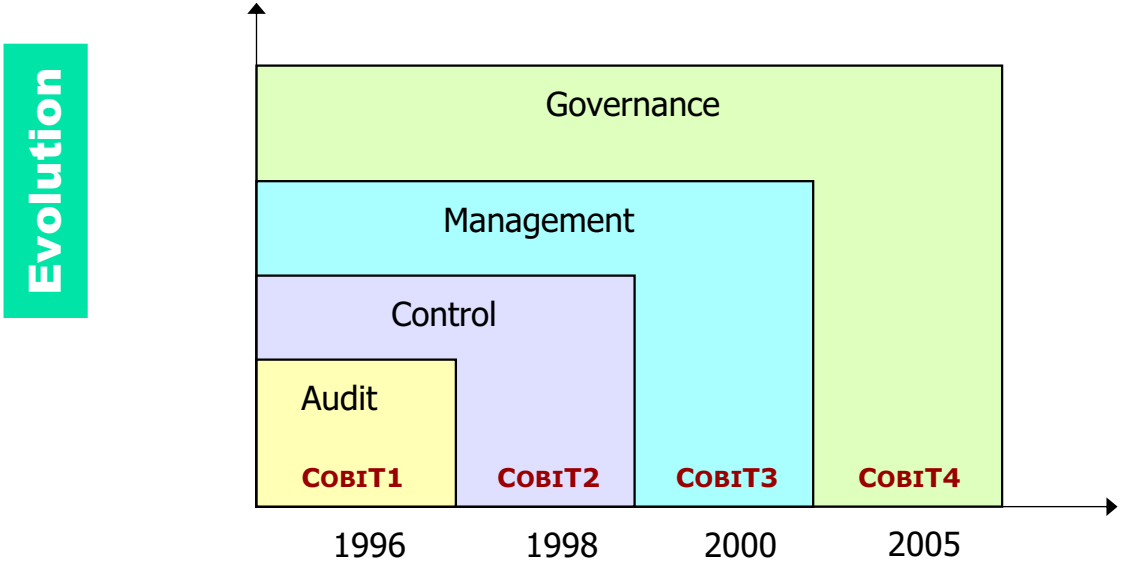
- Established by ISACA in 1998 to serve as "think tank" on IT governance principles and concepts
- To assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- To promote through publications and forums, good practices for effective control and governance over IT based on original research

IT GOVERNANCE INSTITUTE

AGENDA

- What makes IT Governance so important?
- What is IT Governance?
- COBIT – The IT Governance framework
- COBIT and Other Frameworks
- The COBIT Framework Evolution
  - How business drives IT
  - Value Management
  - Extended Practices
  - Supporting Products
- A Value Governance Audit Approach
- Conclusions

COBIT - The Emerging IT Governance Framework

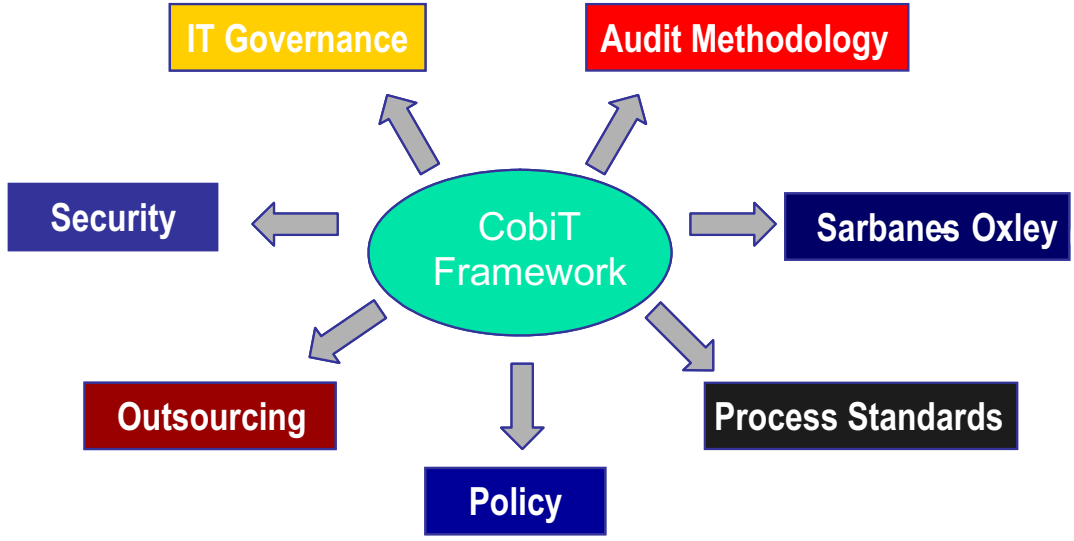


An open standard at www.isaca.org

IT GOVERNANCE INSTITUTE

COBIT - The Emerging IT Governance Framework

How is it being used?



"CobiT is a framework that gives a good overview of IT."

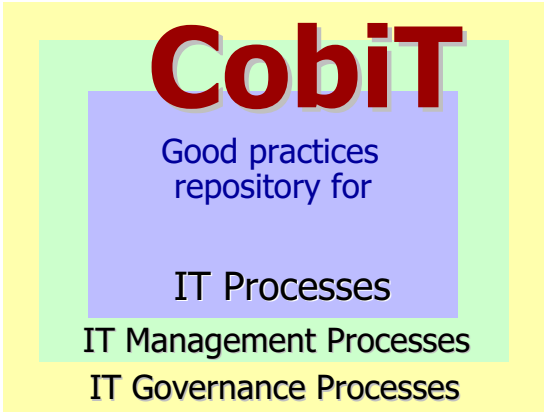
John Shapiro, CIO, Unisys

"CobiT is the framework that gives me confidence in my IT decisions."

Simon Chapin, CIO, Unisys

GOVERNANCE INSTITUTE

COBIT - The Emerging IT Governance Framework



Value

- Internationally accepted good practices, a de facto standard
- Is management oriented
- Is supported by tools and training
- Freely available
- Sharing knowledge and leveraging expert volunteers
- Continually evolves
- Maintained by reputable not for profit organisation
- Maps 100% onto COSO
- Maps strongly onto all major related standards

IT GOVERNANCE INSTITUTE

CobiT - The Emerging IT Governance Framework

Limitations

- It is a reference, a set of best practices, not an "off-the-shelf" cure
- Enterprises still to need to analyse its control requirements and customise based on its
  - Value drivers
  - Risk profile
  - IT infrastructure, organisation and project portfolio

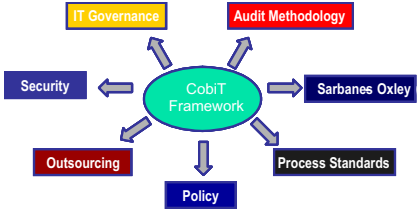
Support

- Implementation Guide, performance metrics, control practices

IT Governance Institute

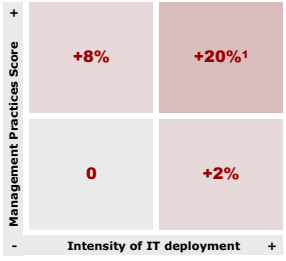
COBIT - The Emerging IT Governance Framework

- IT governance needs a control framework that
  - Is strategically aligned
  - Engages the executive level
  - Can be reused for synergy



- IT governance begins with the Board asking some tough questions about IT

- IT Governance has a high return on investment



GOVERNANCE INSTITUTE

Conclusion

Support for the CIO: World-class IT

Fortune 500 CIO's

- Aligned with the business and providing transparent value
- Top management attention through appropriate IT Governance mechanisms
- Engaged in performance measurement
- Committed to continuous improvement

COBIT : A free download at www.itgi.org

IT GOVERNANCE INSTITUTE

The 2006 European Conference of Internal Audit
Helsinki, 8 September 2006

Erik Guldentops
Advisor to the Board
The IT Governance Institute
erik.guldentops@pandora.be
eguldentops@itgi.org

For more information…

Information Systems Audit and Control Association (ISACA)
IT Governance Institute (ITGI)

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone	+1.847.253.1545 (ISACA)
	+1.847.590.7491 (ITGI)
Fax	+1.847.253.1443 (both)
ISACA E-mail	*info@isaca.org*
ISACA Web Site	*www.isaca.org*
ITGI E-mail	*info@itgi.org*
ITGI Web Site	*www.itgi.org*

IT GOVERNANCE INSTITUTE

E-3
Providing Continuous Assurance on IT Governance – Is the Internal Audit Profession up for it?

Frank Alvern (NOR)
Chief Staff Officer
IIA Norway

Providing Continuous Assurance on IT Governance: Is the Internal Audit Profession up for it?

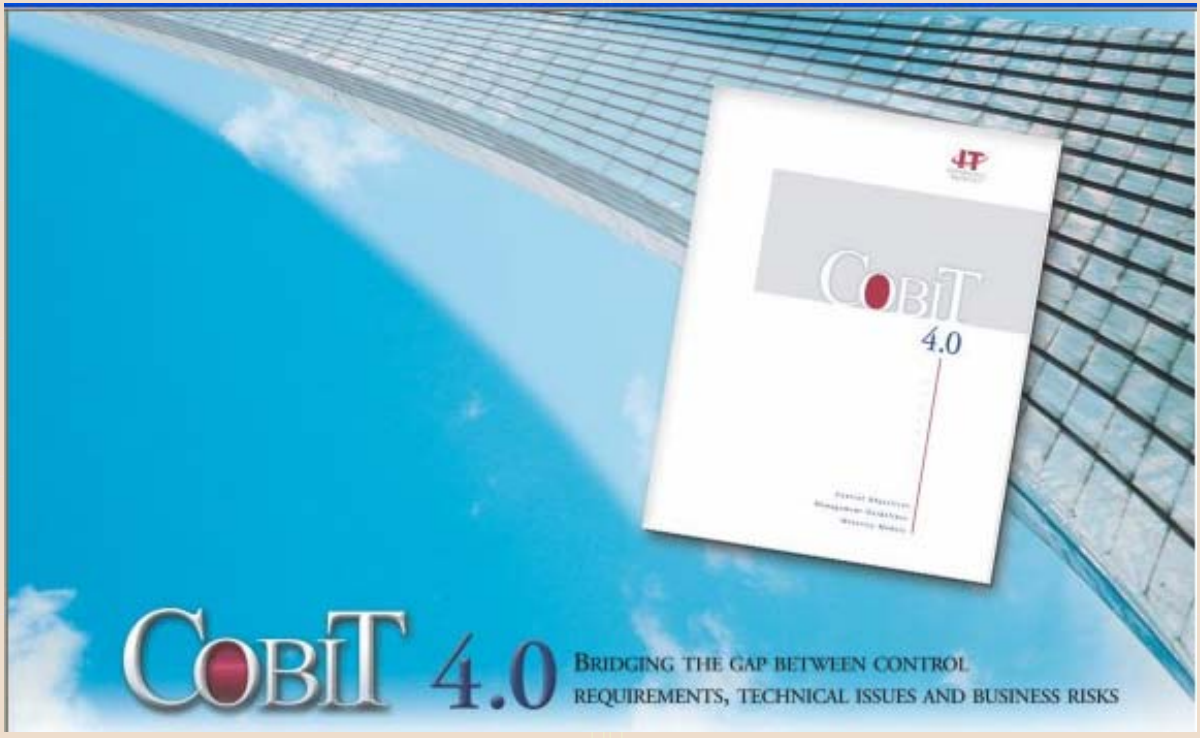
Frank Alvern CIA, CCSA, CISA

Chief Staff Officer, IIA Norway

Agenda

- Agreeing on the starting point
  - Defining IT Governance & Continuous Assurance
- Guidance from The IIA
- Examples on local IIA level: Norway
  - What we have done & plan to do next
- Investing in IA training: the Nordea case
- Q & A session

Defining IT Governance



CobiT 4.0

Executive Overview

IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

CobiT 4.0

Executive Overview

Furthermore, IT governance integrates and institutionalises good practices to ensure that the enterprise's IT supports the business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

IT Governance

Common Sense, Not Common Practice

Erik Guldentops, CISA, CISM
Executive Professor
University of Antwerp – Management School, BE
Advisor to the Board
IT Governance Institute, USA

<erik.guldentops@pandora.be>

What is IT Governance?

DOMAINS

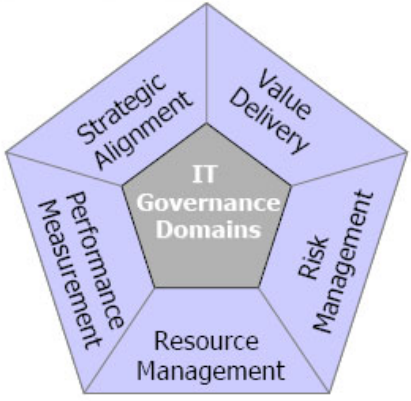
1. Strategic Alignment
aligning with the business and providing collaborative solutions

2. Value Delivery
focus on IT expenses and proof of value

3. Resource Management
knowledge, infrastructure and partners

4. Risk Management
safeguarding assets and disaster recovery

5. Performance Measurement
IT Scorecards



GOVERNANCE INSTITUTE

eg26042006-11

Defining ”continuous”

PwC Advisory
Internal Audit

PricewaterhouseCoopers 2006
State of the internal audit profession study:
Continuous auditing gains momentum*

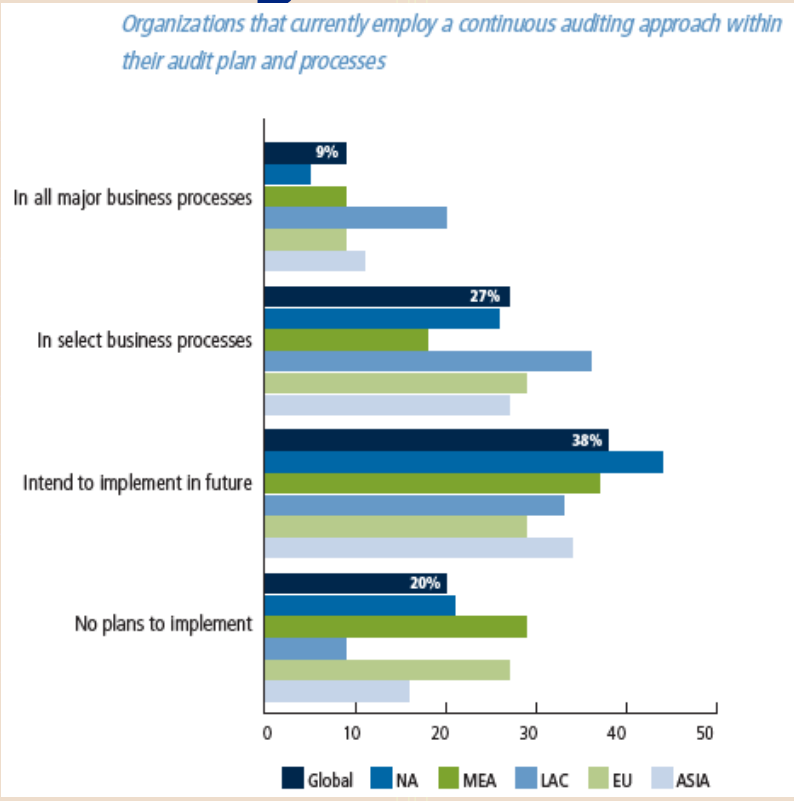
Defining "continuous"

1. Eighty-one percent of 392 companies responding to questions about continuous auditing reported that they either had a continuous auditing or monitoring process in place or were planning to develop one.
2. From 2005 to 2006, the percentage of survey respondents saying they have some form of continuous auditing or monitoring process within their internal audit functions increased from 35% to 50%—a significant gain.
3. Fifty-six percent of our respondents said their continuous auditing processes include both manual and automated elements, 41% indicated their processes are entirely manual, and 3% reported having fully automated processes.
4. The most common continuous auditing "cycle" is quarterly, with 57% of our respondents falling into this category. Another 34% focus on monthly monitoring activities, while only 9% focus on daily applications of their continuous auditing processes.

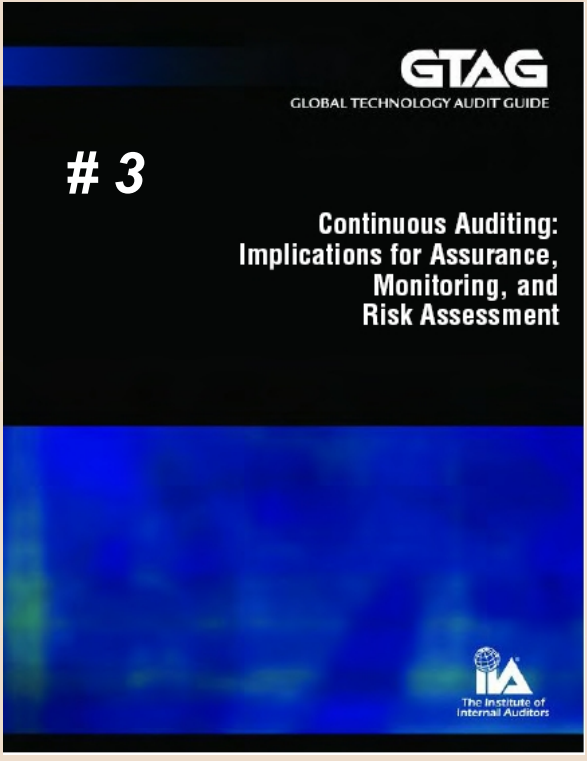
Defining ”continuous”

ACL™
Data you can trust. Results you can see.

Defining "continuous"

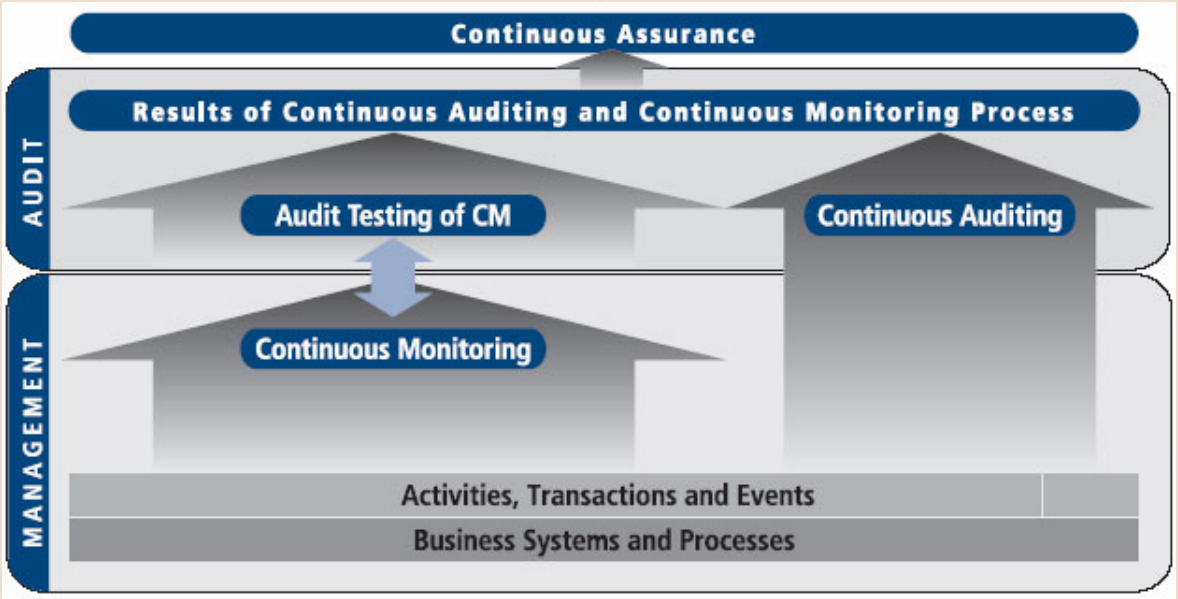


Defining ”continuous”



“Continuous auditing is a method used by auditors to perform audit-related activities on a continuous basis. Activities range from continuous control assessment to continuous risk assessment.”

From GTAG # 3



Continuous Auditing, Monitoring, and Assurance (Conceptual Model)

But, let's not kid ourselves

Common sense – YES –
but not common practice (thanks Erik!):

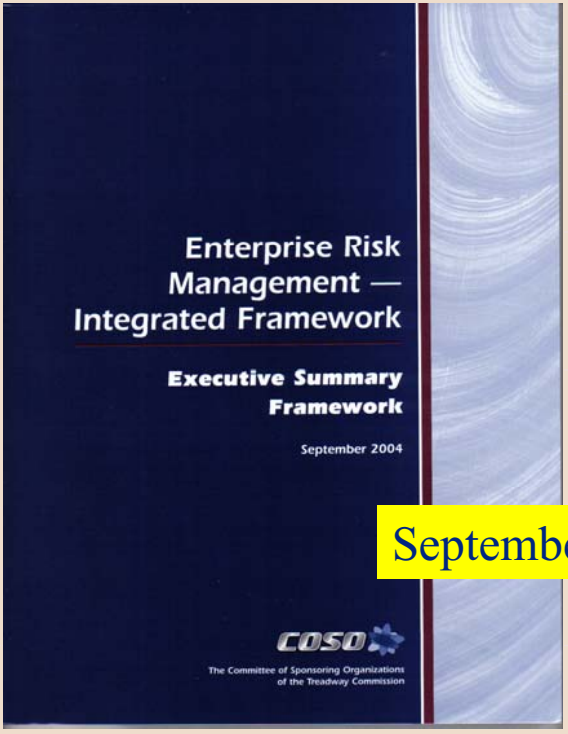
- Internal auditors need GUIDANCE
- Internal auditors need ENCOURAGEMENT
- Internal auditors need PRACTICE
- Internal auditors need SUCCESS STORIES

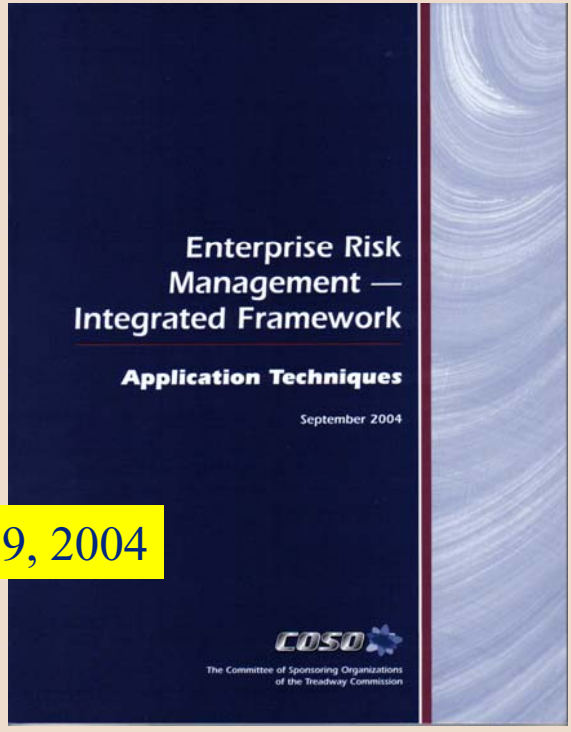
AND it will take time to master this

Agenda

- Agreeing on the starting point
  - Defining IT Governance & Continuous Assurance
- Guidance from The IIA
- Examples on local IIA level: Norway
  - What we have done & plan to do next
- Investing in IA training: the Nordea case
- Q & A session

The "foundation"...





September 29, 2004

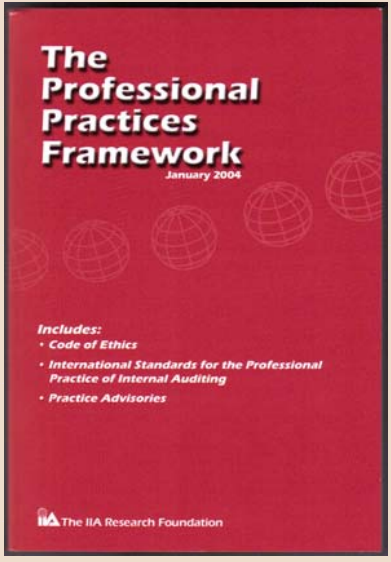
The "foundation"…

September 29, 2004

Position Statement

The Institute of Internal Auditors

The Role of Internal Audit in Enterprise-wide Risk Management



- Partners – AICPA, NACD National Association of Corporate Directors, Carnegie Mellon Software Engineering Institute, the CENTER for INTERNET SECURITY, SANS, ISSA Information Systems Security Association The Global Voice of Information Security

PROGRESS THROUGH SHARING — MORE THAN A MOTTO

THE IIA SINCERELY THANKS all the individuals who have so generously given of their time and knowledge to develop the first five editions of the Global Technology Audit Guide (GTAG) series. GTAG's overwhelming success is the result of their unparalleled expertise and unwavering commitment — making *Progress Through Sharing* more than a motto, making it a reality.

GTAG 1 - *Information Technology Controls*
David A. Richards, CIA, CPA,
The Institute of Internal Auditors

GTAG 2 - *Change and Patch Management Controls*
Jay R. Taylor, CIA, CFE, CISA,
General Motors Corp.
Julia H. Allen, Software Engineering Institute, Carnegie Mellon University
Glenn L. Hyatt, CIA, CISA, CISSP,
General Motors Acceptance Corp.
Gene H. Kim, CISA, Tripwire Inc.

GTAG 3 - *Continuous Auditing*
David Coderre,
Royal Canadian Mounted Police
John G. Verver, AGL Services Ltd.
J. Donald Warren Jr., Center for Continuous Auditing, Rutgers University
Peter Millar, AGL Services Ltd.

GTAG 4 - *Management of IT Auditing*
Michael Juergens, Deloitte & Touche LLP
David Maberry, Deloitte & Touche LLP
Eric Ringle, CISA, CISSP,
Deloitte & Touche LLP
Jeffrey Fisher, CPA, CITP, CISA,
Deloitte & Touche LLP

GTAG 5 - *Managing and Auditing Privacy Risks*
Ulrich Hahn, Ph.D., CIA, CISA, CCSA,
Switzerland/Germany
Ken Askelson, CIA, CPA, CITP,
JCPenney, USA
Robert Stiles, CISA, CFE,
Texas Guaranteed, USA

About GTAG
The IIA's GTAG series provides chief audit executives (CAEs) and audit supervisors with direction on issues relating to information technology management, control, and security. Written in straightforward business language, it arms CAEs with the knowledge to educate members of the board and audit committee, management, process owners, and others regarding technology-associated risks and recommended best practices.

Check The IIA's Web site for the latest GTAGs – www.theiia.org/technology.

PROFESSIONAL GUIDANCE
Setting the Standard


ITAUDIT
THE PREMIER INFORMATION TECHNOLOGY RESOURCE FOR INTERNAL AUDITORS
ARE YOU "WITH IT?"
ITAUDIT — THE IIA'S PREMIERE INFORMATION TECHNOLOGY (IT) RESOURCE FOR INTERNAL AUDITORS.
A free ITAudit subscription includes:
A monthly online magazine that enables auditors and IT professionals worldwide to share information and experiences.
Access to a reference library with hundreds of links to useful IT audit online resources.
A discussion board for posting questions on topics of interest and expressing your views on current issues.
SO, GET "WITH IT" — ITAUDIT — WHY NOT?
www.theiia.org/itaudit
The Institute of Internal Auditors
Progress Through Sharing
06135

The August 2006 issue

Getting a Grasp of IT

RUSSELL A. JACKSON

ILLUSTRATION BY
RICHARD TUSCHMAN

What level of technology expertise do audit leaders need to possess? Several experts share their thoughts on the systems knowledge required of CAEs.

IN HIS PAST AS A CONSULTANT, Steve Mar, now senior director of IT audit at Microsoft Corp., warned one of his clients that a costly information technology (IT) system it was considering investing in wouldn't work for the strategic goals established for it. The company executives — including the chief audit executive (CAE) — and the IT department didn't coordinate and agree on the business requirements, so testing was inadequate and a comparison of inventory records to actual inventory that should have been done was not. But the company implemented the system anyway. Its inventory management and accounting collapsed, and the entire enterprise soon went bankrupt. "Could someone have stopped that implementation?" Mar asks rhetorically. "The CAE could have, if he'd been strong

Agenda

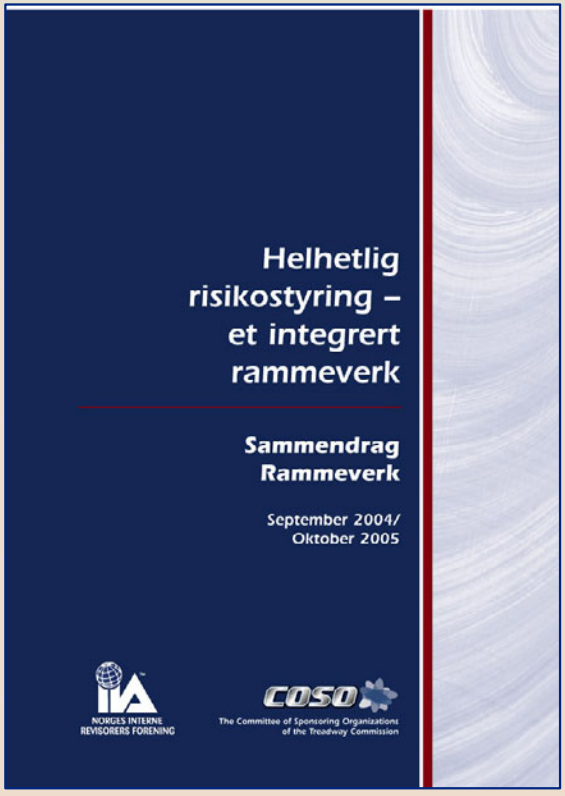
- Agreeing on the starting point
  - Defining IT Governance & Continuous Assurance
- Guidance from The IIA
- Examples on local IIA level: Norway
  - What we have done & plan to do next
- Investing in IA training: the Nordea case
- Q & A session

Seriously - what can a small, local IIA affiliate do?

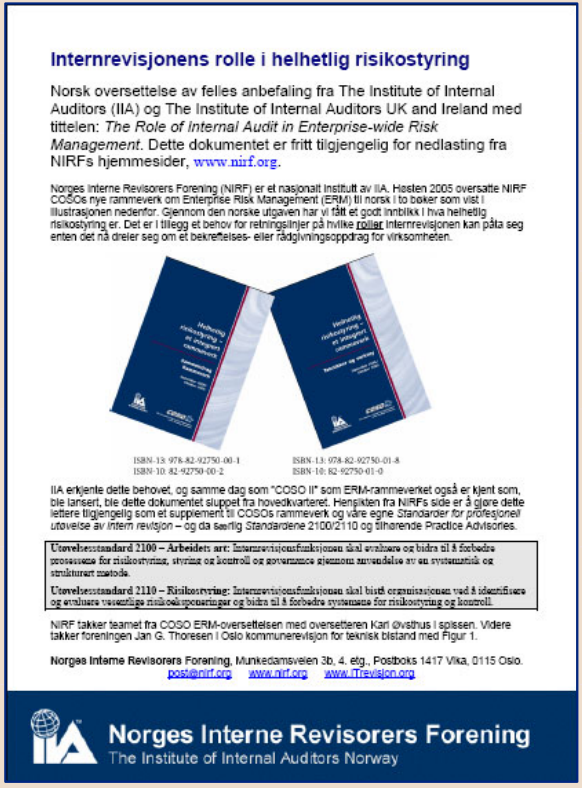
Step 1: TRANSLATE

(… and not because people can't understand English!)

Translating the ”foundations” …



Translating the "foundations" ...



Internrevisjonens rolle i helhetlig risikostyring

Norsk oversettelse av felles anbefaling fra The Institute of Internal Auditors (IIA) og The Institute of Internal Auditors UK and Ireland med tittelen: *The Role of Internal Audit in Enterprise-wide Risk Management*. Dette dokumentet er fritt tilgjengelig for nedlasting fra NIRFs hjemmesider, www.nirf.org.

Norges Interne Revisorers Forening (NIRF) er et nasjonalt Institutt av IIA. Høsten 2005 oversatte NIRF COSOs nye rammeverk om Enterprise Risk Management (ERM) til norsk i to bøker som vist i illustrasjonen nedenfor. Gjennom den norske utgaven har vi fått et godt innblikk i hva helhetlig risikostyring er. Det er i tillegg et behov for retningslinjer på hvilke roller internrevisjonen kan påta seg enten det nå dreier seg om et bekreftelses- eller rådgivningsoppdrag for virksomheten.

ISBN-13: 978-82-92750-00-1
ISBN-10: 82-92750-00-2

ISBN-13: 978-82-92750-01-8
ISBN-10: 82-92750-01-0

IIA erkjente dette behovet, og samme dag som "COSO II" som ERM-rammeverket også er kjent som, ble lansert, ble dette dokumentet sluppet fra hovedkvarteret. Hensikten fra NIRFs side er å gjøre dette lettere tilgjengelig som et supplement til COSOs rammeverk og våre egne *Standarder for profesjonell utøvelse av intern revisjon* – og da særlig *Standardene* 2100/2110 og tilhørende Practice Advisories.

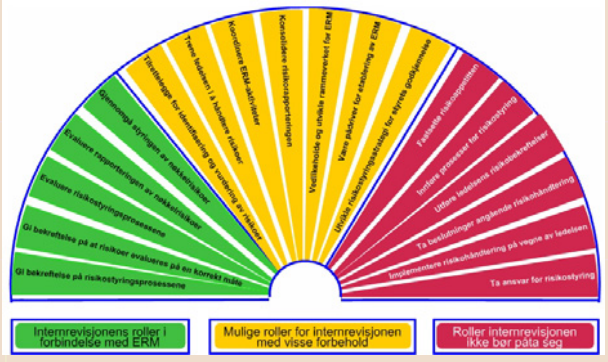
Utøvelsesstandard 2100 – Arbeidets art: Internrevisjonsfunksjonen skal evaluere og bidra til å forbedre prosessene for risikostyring, styring og kontroll og governance gjennom anvendelse av en systematisk og strukturert metode.

Utøvelsesstandard 2110 – Risikostyring: Internrevisjonsfunksjonen skal bistå organisasjonen ved å identifisere og evaluere vesentlige risikoeksponeringer og bidra til å forbedre systemene for risikostyring og kontroll.

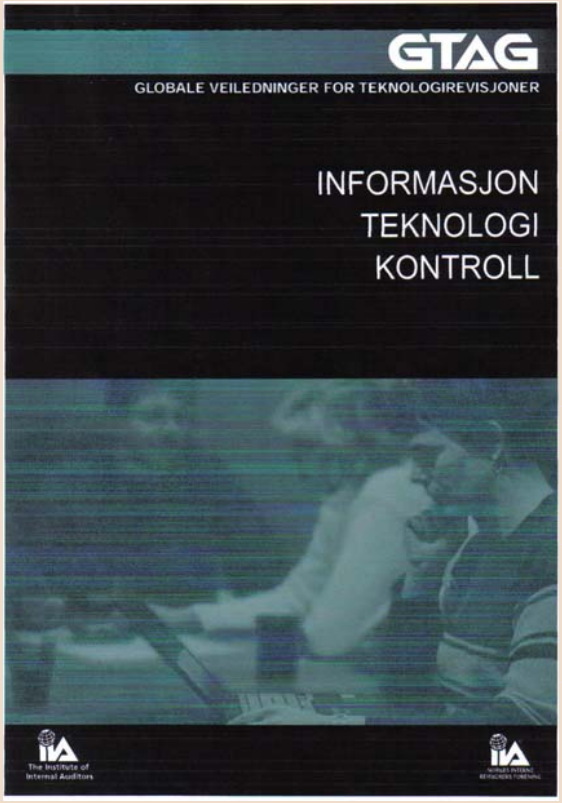
NIRF takker teamet fra COSO ERM-oversettelsen med oversetteren Karl Øvsthus i spissen. Videre takker foreningen Jan G. Thoresen i Oslo kommunerevisjon for teknisk bistand med Figur 1.

Norges Interne Revisorers Forening, Munkedamsveien 3b, 4. etg., Postboks 1417 Vika, 0115 Oslo.
post@nirf.org www.nirf.org www.ITrevisjon.org

Norges Interne Revisorers Forening
The Institute of Internal Auditors Norway



Translating the ”foundations” …



Vurdering av IT-kontroller	Forståelse av IT-kontroller	Styring, ledelse, teknisk
		Generell / applikasjon
		Forebyggeende, oppdagende, korrigerende
		Informasjonssikkerhet
	Betydningen av IT-kontroller	Pålitelighet og effektivitet
		Konkurransemessig fortrinn
		Lovgivning og regulering
	Roller og ansvarsområder	Styring
		Ledelse
		Revisjon
	Basert på risiko	Risikoanalyse
		Risikorespons
		Basiskontroller
	Overvåking og teknikker	Kontrollrammeverk
		Hyppighet
	Vurdering	Metoder
		Grensesnitt til revisjonskomité

COSO-modellen for teknologikontroller

Overvåking:

- Månedlige måltall om teknologiens ytelse
- Analyse av kostnad og ytelse for teknologien
- Periodisk vurdering av teknologiledelse
- Internrevisjon av teknologiprosjekter
- Internrevisjon av områder med høy risiko

Kontrollaktiviteter:

- Vurderingskomité for endringsledelse
- Sammenligning av teknologiinitiativer for planlegging og avkastning på investeringer
- Dokur
- Overh
- Tilslut
- Håndl

Informasjon og kommunikasjon:

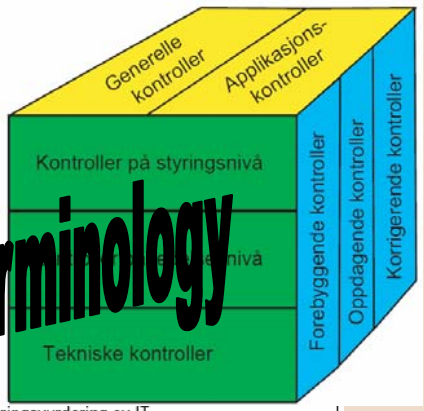
- Periodisk virksomhetsintern kommunikasjon
- Kontir
- Spørr
- IT og
- Kontir

Risikovu

- Forsikringsvurdering av IT

Kontrollmiljø:

- Ledelsen signaliserer at IT og sikkerhet betraktes som viktig
- Generelle retningslinjer for teknologi og informasjonssikkerhet
- Virksomheten har en styringskomité for teknologi
- Virksomheten har en komité for teknologiarkitektur og –standarder.
- Alle forretningsenheter er representert



Figu

Establishing a Norwegian terminology

Seriously - what can a small, local IIA affiliate do?

Step 2: TELL ABOUT IT

(and good things might actually happen…)


Nordea
Helhetlig risikostyring – et integrert rammeverk
Sammendrag Rammeverk
Helhetlig risikostyring – et integrert rammeverk
Teknikker og verktøy
Nordea
Nordea
Norges Interne Revisorers Forening
Stockholm, oktober 2005
Nordea
PricewaterhouseCoopers

Senter for statlig økonomistyring

Kundenett | Internett

Aktuelt | Økonomistyring | Konsernkonto | Statsregnskapet | Økonomitjenester | Kurs og studier

Government Agency for Financial Management

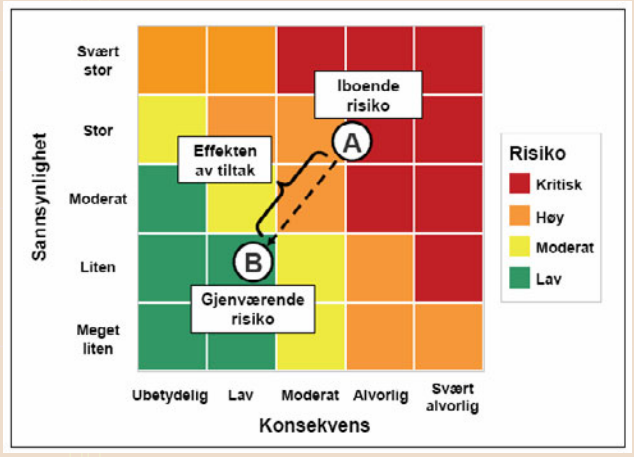
Utskrift

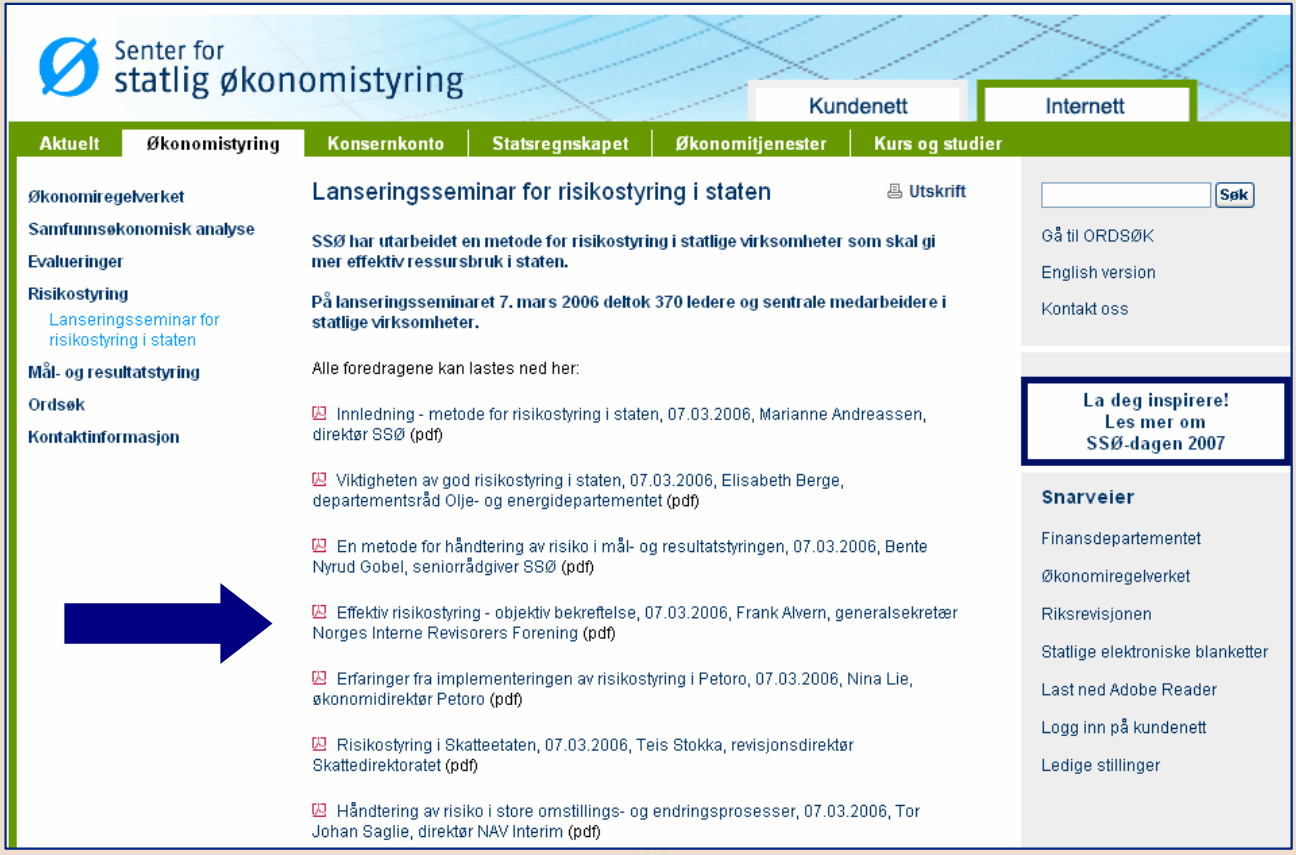
The Norwegian Government Agency for Financial Management (SSØ) was established by the Ministry of Finance on January 1, 2004. SSØ will strengthen financial management within public sector activities and improve resource efficiency within the area.

Søk

Gå til ORDSØK

English version




Senter for
statlig økonomistyring
Kundenett
Internett
Aktuelt
Økonomistyring
Konsernkonto
Statsregnskapet
Økonomitjenester
Kurs og studier
Økonomiregelverket
Samfunnsøkonomisk analyse
Evalueringer
Risikostyring
Lanseringsseminar for risikostyring i staten
Mål- og resultatstyring
Ordsøk
Kontaktinformasjon
Lanseringsseminar for risikostyring i staten
Utskrift
SSØ har utarbeidet en metode for risikostyring i statlige virksomheter som skal gi mer effektiv ressursbruk i staten.
På lanseringsseminaret 7. mars 2006 deltok 370 ledere og sentrale medarbeidere i statlige virksomheter.
Alle foredragene kan lastes ned her:
Innledning - metode for risikostyring i staten, 07.03.2006, Marianne Andreassen, direktør SSØ (pdf)
Viktigheten av god risikostyring i staten, 07.03.2006, Elisabeth Berge, departementsråd Olje- og energidepartementet (pdf)
En metode for håndtering av risiko i mål- og resultatstyringen, 07.03.2006, Bente Nyrud Gobel, seniorrådgiver SSØ (pdf)
Effektiv risikostyring - objektiv bekreftelse, 07.03.2006, Frank Alvern, generalsekretær Norges Interne Revisorers Forening (pdf)
Erfaringer fra implementeringen av risikostyring i Petoro, 07.03.2006, Nina Lie, økonomidirektør Petoro (pdf)
Risikostyring i Skatteetaten, 07.03.2006, Teis Stokka, revisjonsdirektør Skattedirektoratet (pdf)
Håndtering av risiko i store omstillings- og endringsprosesser, 07.03.2006, Tor Johan Saglie, direktør NAV Interim (pdf)
Søk
Gå til ORDSØK
English version
Kontakt oss
La deg inspirere! Les mer om SSØ-dagen 2007
Snarveier
Finansdepartementet
Økonomiregelverket
Riksrevisjonen
Statlige elektroniske blanketter
Last ned Adobe Reader
Logg inn på kundenett
Ledige stillinger

[a·w] audit·wire
INSIGHT, ISSUES, AND INFORMATION FROM THE IIA
Volume 27 • No. 4 • July/August 2005

Norway:
IIA's First Global Technology Audit Guide Translated

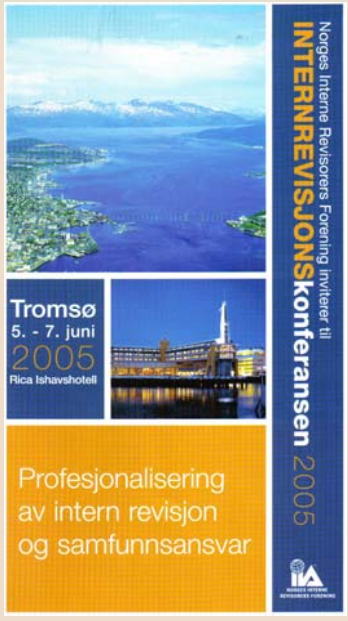
Frank Alvern, CIA, CISA, CCSA
Past President, IIA Norway

IIA Norway released the Norwegian translation of The IIA's first Global Technology Audit Guide (GTAG), *IT Controls*, with more than 200 copies purchased by participants at the 2005 Internal Audit Conference in Tromsø, Norway. "The release of the Norwegian translation of GTAG is in line with The IIA's global commitment to support its membership with relevant and timely guidance on information technology (IT), said Gerry Cox, The IIA's vice chair-professional development.

Cox upheld the proud tradition of global representation at the Norwegian annual internal audit conference, delivering a keynote address on "ERM and the Changing Role of the Auditors." Cox also introduced GTAG as part of his informative presentation entitled "What is The IIA Doing Regarding Technology?" With the release of the first guide in the series in March 2005, and three more GTAGs scheduled for release later this year, The IIA is demonstrating that it is serious about IT guidance, Cox said. "In that context, it is very satisfying to see that our affiliates support and strengthen this guidance on a local level, and IIA Norway has shown that it is possible to do this even for the smaller affiliates. "It is impressive that our national institute has been able to process and deliver the Norwegian translation today," Cox told the audience.

The group that made the GTAG translation possible is the new IT audit specialty group of IIA Norway, chaired by Stig Sunde, senior advisor with the Office of the Auditor General of Norway. In addition, the specialty group was responsible for three well-received presentations at the conference. The common message for these presentations was that IT risks and controls concern all auditors today, and the new specialty group will be an important arena for obtaining relevant knowledge for the membership.

The IT audit group is one of three specialty audit groups established by IIA Norway, including a group for financial services auditors and government auditors. The newly elected president of IIA Norway, Reidar Døli, emphasized in his inaugural speech the importance of the specialty groups, which provide an interesting and promising tool for achieving progress through sharing. "Our IT audit group demonstrated this very well at this conference," he concluded.



NORGES INTERNE REVISORERS FORENING

NETTVERKSGRUPPEN FOR IT-REVISJON

Seriously - what can a small, local IIA affiliate do?

Step 3: GET HOLD OF THE CAEs

(… they just might thank you!)

INVITASJON til

ROUNDTABLE for INTERNREVISJONSSJEFER

Tema: *DITT BEHOV FOR Å FORSTÅ IT...*

Hvorfor IT, og hvorfor nå?

Norges Interne Revisorers Forening (NIRF) ved Nettverksgruppen for IT-revisjon inviterer deg til å delta i en roundtable med fokus på informasjon – teknologi – kontroll. Den observante leser vil her gjenkjenne den norske tittelen på den første *globale veiledningen for teknologirevisjoner (GTAG)* som The Institute of Internal Auditors (IIA) lanserte tidligere i år. Nettverksgruppen har nå bearbeidet denne veiledningen videre, og er klar til å presentere den sett fra ståstedet til lederen av internrevisjonen i en norsk virksomhet.

Hvorfor Roundtable?

Foreningens motto er *Fremskritt gjennom delt kunnskap*. IIA har økt sitt fokus på IT, og revisjonssjefenes behov for å forstå IT. NIRF opplever det samme behovet i Norge. Det er imidlertid noen sentrale utfordringer knyttet til å få konkret nytteverdi ut av en global veiledning. Et slikt materiale må bearbeides og så må det knyttes direkte opp mot de behov revisjonssjefene har. Gjennom å begrense deltagelsen til maksimum 15 deltagere på hvert roundtable mener vi at forholdene ligger godt til rette for dette. NIRF og IT-nettverket har på dine vegne relatert denne generelle veiledningen opp mot norske regler, krav, forventninger og muligheter.

Hvorfor begrenset til internrevisjonssjefene?

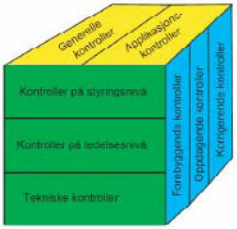
Nå tror vi at dere etter å ha vært gjennom denne dagen, vil anbefale oss å invitere deres medarbeidere til det samme! Det gjør vi gjerne på et senere tidspunkt. GTAG nr. 1 er skrevet spesifikt for dere som ledere (og noen få andre). Det å samle ledere som sitter med ansvaret for at IT risikovurderes og revideres i virksomheten i et slikt forum, mener vi har stor egenverdi. Uansett om du har dedikerte IT-revisorer eller ikke, er kommet langt i å innarbeide IT i revisjonsavdelingens arbeide eller ikke, vil du oppleve at utfordringene stort sett er de samme rundt bordet. Denne dagen skal være en kombinasjon av presentasjoner fra vår side, og diskusjoner dere i mellom. Videre vil vi vise frem de forskjellige modellene og rammeverkene GTAGen refererer til, samt aktuelle regler, forskrifter og veiledninger for Norge.

Men jeg trenger da ikke vite alt om IT-kontroller?

Nei, selvsagt ikke. Det finnes IT-kontroller på mange nivåer, og nettopp det å forstå roller og ansvar både i linjen og i internrevisjonen er en nøkkel frem mot at vi kan avgi en objektiv bekreftelse på at linjen faktisk *har kontroll*. Det er mange måter å illustrere dette på. Figuren over er hentet fra GTAGen, og fungerer bra som en ramme å diskutere dette innenfor.

Er nå egentlig IT og IT-kontroller så spesielt da?

Her er det sikkert mulighetene til gode diskusjoner! GTAGen vektlegger kontrollbegreper som er kjente og kjære for oss alle. Som figuren viser må vi også innenfor IT vurdere kontrollene i forhold til om de er forebyggende, oppdagende eller korrigerende. GTAGen deler opp "kontrolluniverset" i to: generelle kontroller og applikasjonskontroller. Det kan selvsagt også diskuteres, men igjen – det vi søker nå er noen relativt enkle begreper, rammer og knagger å henge både enkle og kompliserte saker og forhold på. For har vi først det på plass vil vi kunne gå dypere inn i materien der det er nødvendig. Da står vi også overfor spørsmålet om kompetansen finnes internt eller må kjøpes eksternt.



Skal vi nå få enda flere modeller og rammeverk å forholde oss til?

Føler du at du akkurat har nådd metningspunktet for rammeverk med kuber og pyramider du også? Et mål vi har med denne dagen er nettopp å se disse rammeverkene opp mot hverandre GTAGen har noen riktig gode vedlegg som diskuterer dette her. Hvor tar det ene rammeverket over, hvor har vi overlapp mellom dem, hva er de gode til og hva er de IKKE gode på? Og så kommer noe av det vi tror blir konkret og nyttig for deg: hvor kommer norske lover og forskrifter inn med sine krav og forventninger? Hvilke rammeverk baserer myndighetene seg på?

Hva koster denne dagen, og hva skal inntektene finansiere?

Vi har lagt oss på en pris for denne dagen på kr 5.000 per deltager. Det vi håper er at vi på den måten skal få midler til å jobbe videre med å dekke behovet for relevante veiledninger for våre medlemmer fremover også. IIA produserer disse GTAGene på løpende bånd fremover, og relevansen for oss i Norge varierer. Der hvor vi har høy relevans har vi sagt at det første steget er å oversette til norsk. Oversettelse er en krevende og kostbart affære, og i noen tilfeller er det dessuten nødvendig å sette den norske oversettelsen inn i den riktige norske sammenhengen. Forøvrig ønsker å fremskaffe gode veiledninger til medlemsmassen til en lav kostnad, og heller bruke ressursene på å bearbeide og formidle det gode budskap.

Hvem er ansvarlig for opplegget fra foreningens side?

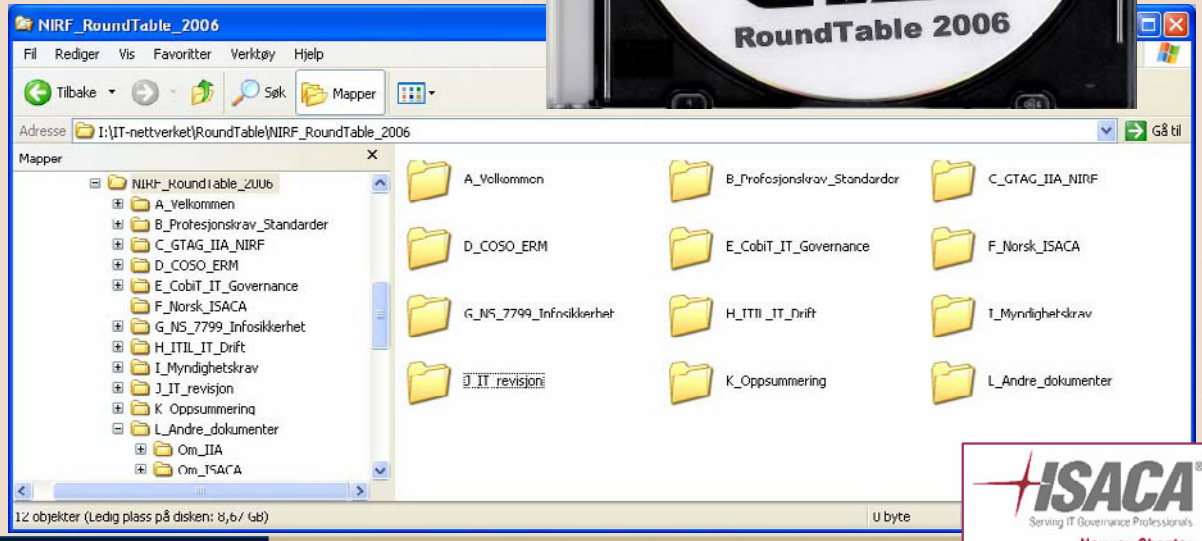
Generalsekretæren i NIRF, Frank Alvern og lederen av Nettverksgruppen for IT-revisjon, Stig J. Sunde vil sammen stå for gjennomføringen. Alvern har nå permisjon fra Nordeas internrevisjon, hvor han var medlem av ledergruppen med ansvar for kompetanse og metode. Sunde jobber i metodeseksjonen for regnskaps- og IT-revisjon i Riksrevisjonen, og har tidligere omfattende IT-revisjonserfaring fra PwC, Postbanken og kommunerevisjon. Begge to er sertifisert som Certified Internal Auditor (CIA) og Certified Information Systems Auditor (CISA), og begge er aktive medlemmer i IT-revisjonsforeningen ISACA. Dessuten er IIA's Advanced Technology Committee (ATC) en fellesnevner: Alvern satt i ATC i treårsperioden 2001-2004, og Sunde ble medlem av den samme nå i sommer. ATC er den komiteen i IIAs hyvilige apparat som står ansvarlig for utarbeidelsen av GTAGene globalt.

Ta kontakt med Alvern i dag på frank.alvern@nirf.org eller på telefon 9281 1774!

NETTVERKSGRUPPEN FOR IT-REVISJON

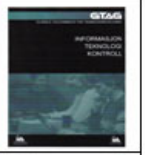

Velkommen til RoundTable:
Ditt behov for å skjønne IT!
Fremskritt Gjennom Delt Kunnskap
www.nirf.org
RoundTable 2006
Nettverksgruppen for IT-Revisjon
www.ITRevisjon.org

3 separate events in January 2006 - a total of 25 CAEs



ISACA Serving IT Governance Professionals Norway Chapter

NIRFs forsøk på et oversiktsbilde på sammenhengen mellom koder, standarder, retningslinjer og rammeverk innenfor IT

NIVÅ 0: Faglige standarder	      
NIVÅ 1: Helt overordnede	        
NIVÅ 2: Litt mer detaljerte	        
NIVÅ 3: Spesifikke områder	        
NIVÅ 4: Spesifikke leverandører m.v.	    

Seriously - what can a small, local IIA affiliate do?

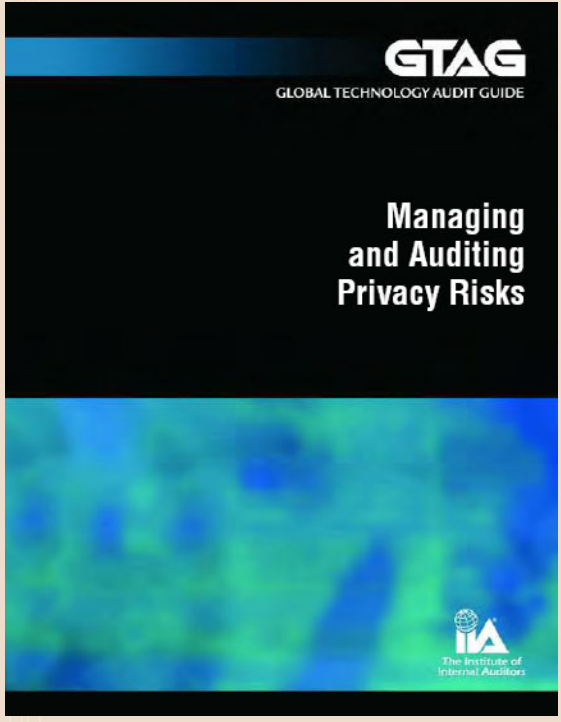
Step 4: KEEP AT IT WITH THE CAEs

(… don't you let go now, Frodo!)

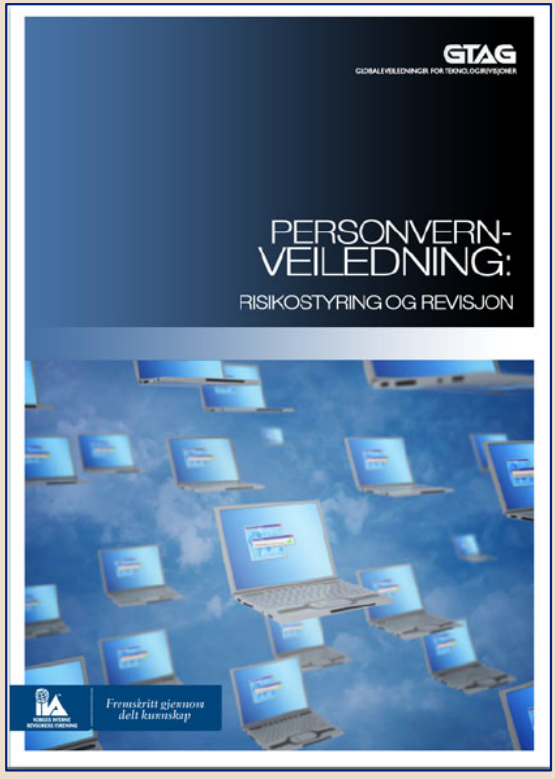
If necessary, localize the guidance

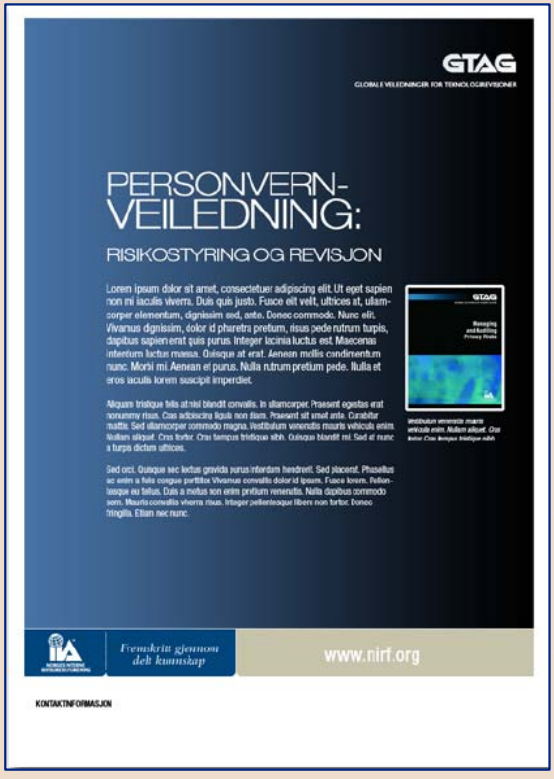
September 4, 2006 in Oslo:

One-day seminar on Privacy – "the Norwegian way" (based on GTAG # 5) by invitation only.



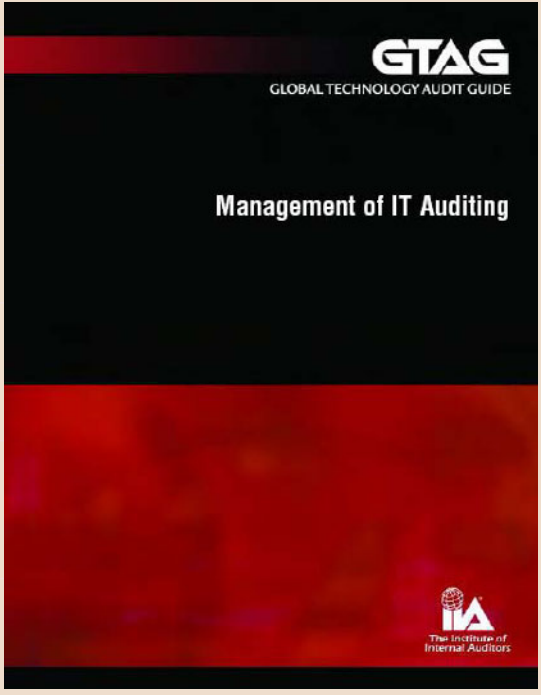
If necessary, localize the guidance

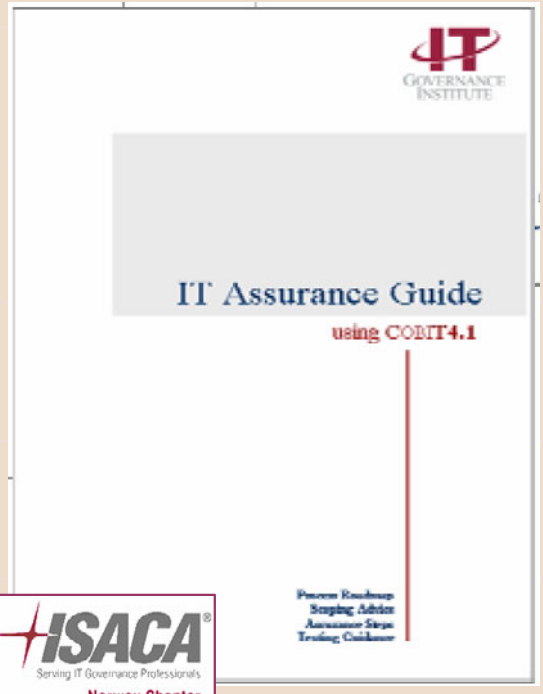





English - Datatilsynet - Microsoft Internet Explorer
Fil Rediger Vis Favoritter Verktøy Hjelp
Adresse http://www.datatilsynet.no/templates/Page____194.aspx
Datatilsynet personvern - din rett til å velge
Annual reports | Guidelines | Contact
You are here: Front page
.: TO NORWEGIAN PAGE
.: ENGLISH
>Annual reports
>Guidelines
>Contact
NEWSLETTER FROM DATATILSYNET
Read more and order(in norwegian)>>
English
Print
About The Data Inspectorate
The Data Inspectorate, an independent administrative body under the Norwegian Ministry of Labour and Government Administration, was set up in 1980 to ensure enforcement of the Data Register Act of 1978, now made obsolete by the commencement of the Personal Data Act of 2000. The purpose of this Act is to protect persons from violation of their right to privacy through the processing of personal data. The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.
Personal Data Act (pdf, new window)
Personal Data Regulations (pdf, new window)Personal Health Data Filing System Act (new window)
The Data Inspectorate shall:
keep a systematic, public record of all processing that is reported or for which a licence has been granted
deal with applications for licences, receive notifications and
?
Sitemap>>

Coming up:
another IT RoundTable for CAEs





ISACA
Serving IT Governance Professionals
Norway Chapter

Agenda

- Agreeing on the starting point
  - Defining IT Governance & Continuous Assurance
- Guidance from The IIA
- Examples on local IIA level: Norway
  - What we have done & plan to do next
- Investing in IA training: the Nordea case
- Q & A session

We need to train our auditors – even those ”less enthusiastic”

This is my own history as Head of Competence & Development Centre, Internal Audit Activity, Nordea

Innovative: Frank Alvern's involvement with the Institute of Internal Auditors (IIA) provides Nordea with an opportunity to closely follow developments within internal auditing.

Enthusiast combines hobby with work

Frank Alvern was appointed head of the IAA (Internal Audit Activity) competence centre in Nordea. He also runs the Norwegian branch of the Institute of Internal Auditors. For Nordea it is such an important job that he is allowed to pursue his hobby during working hours.

Nordea's 170 internal auditors have been assigned to implement the new concepts reflected in the change in strategy. One of the people with additional responsibilities is Frank Alvern. As head of the Norwegian branch of the IIA, the Institute of Internal Auditors, he has first-hand knowledge of the latest developments in internal auditing worldwide. The IIA has 80,000 members in more than 150 countries worldwide, and is the profession's centre for research, education, certification and professional standards.

– Relative to its population, few countries have contributed more to the profession's progress than Norway, says Frank Alvern, who was appointed last summer.

– Major efforts by many over several years, where Norway has sometimes been the only European country represented, means we are frontrunners in the profession. The IIA is the driver of new ideas, whereby the role of auditors is transformed from guard dogs arriving after the fact with an "I got you" attitude, to becoming agents contributing added value to the organisation through the active pursuit of better management and control mechanisms at all levels.

– My work for the IIA is something that I pursue out of pure interest, but Nordea regards it as important enough to allow me to do some of this work during working hours. Nordea's interests lie with whatever is best and represents the cutting edge right now – guidance from the IIA. Nordea is among the first companies in the world to adopt the new standards of the IIA, explains Frank Alvern, who besides heading the Norwegian branch also sits on the IIA's international Advanced Technology Committee.

– This is an excellent way to promote Nordea. It shows that we are on the alert and assume responsibility for the profession's future progress. For Nordea, having people in central positions within the IIA means access to all new thinking at an early stage. We have our finger on the pulse, and Nordea's auditors are also represented on the national committees in Denmark and Sweden, says Frank Alvern.

His manager, Dag Andresen, who also picked Frank Alvern to be head of IAA's competence centre in Nordea, praises him for his work achievements, past and present.

– Frank is a professional and ideally suited to head the competence centre in Nordea, says Dag Andresen.

Text and photo:
Lars Richard Bache

2005 Course Catalogue

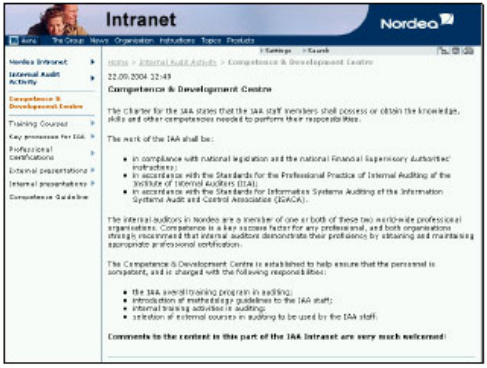
Competence & Development Centre

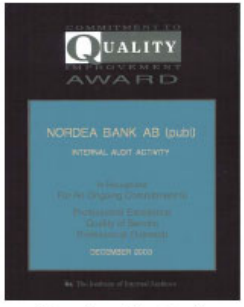
Nordea

Internal Audit Activity

IAA Competence & Development Centre – Course Catalogue 2006

Please stay updated by checking out the 'Training Courses' area on the CDC intranet!





Honouring our Commitment!

Nordea

Internal Audit Course Catalogue

Summary by quarter 2005

January - March

- IT and IT Governance in Nordea (week 2)
- Welcome to IAA (week 3)
- Auditing the IT Providers and auditing general IT controls (week 11)

April - June

- An introduction to Basel II (week 17)
- The Nordea way - version 2.0 (weeks 24+25)
- Communicating - Phase II (weeks 24+25)

July - September

- Auditing business applications (weeks 33+34)
- Auditing development activities (week 38)

October - December

- Using SAP in auditing (week 43)
- An introduction to Leadership (week 47)
- Introduction to COSO ERM (week 50)

Nordea

2005 Course Catalogue - by location

	Course name	Participants	Helsinki	Copenhagen	Stockholm	Oslo
1	IT and IT Governance in Nordea	Mandatory	13 January	12 January	11 January	14 January
2	Welcome to IAA	By invitation only	not planned	not planned	19-21 January	not planned
3	Auditing the IT providers and auditing general IT controls	Mandatory for business auditors	17 March	14 March	16 March	15 March
4	An introduction to Basel II	Mandatory	21 + 22 April	28 + 29 April	18 + 19 April	25 + 26 April
5	The Nordea way - version 2.0	Mandatory	16 June	13 June	9 June	6 June
6	Communicating - Part II	Mandatory	17 June	14 June	10 June	7 June
7	Auditing business applications	Mandatory	18 + 19 August	25 + 26 August	15 + 16 August	22 + 23 August
8	Auditing development activities	SAMs and AiCs	not planned	22 + 23 September	19 + 20 September	not planned
9	Using SAP in auditing	Open	not planned	27 October	24 October	26 October
10	An introduction to Leadership	By invitation only	23 November	24 November	22 November	not planned
11	An introduction to COSO ERM	Open	14 December	12 December	13 December	15 December

NB: changes to this schedule will be communicated on the IAA Intranet (CDC)

Content topic: Specialties

Subject: Auditing Information Systems and Related Technology

Linkage to the IIA *Standards*

Attribute Standard 1200
Proficiency and Due Professional Care
Engagements should be performed with proficiency and due professional care.

Attribute Standard 1210
Proficiency
Internal auditors should possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Implementation Standard 1210.A3
Internal auditors should have knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

Overall objective of the training in this subject
Training in auditing IS/IT will target both the business auditors and the IT auditors. A comprehensive seven days training program will be offered over five separate sessions.

The primary objective of this programme is to facilitate the decided division of responsibilities between the IT Audit group and all the other (business) auditors.

To reach this objective, the training programme will

(1) first ensure that everybody is up-to-date with Nordea's IT situation
(2) then ensure that the contents and implications of the *IT Audit Service Catalogue* is understood by all, and finally
(3) support the necessary competence development of the auditors in fulfilling their prescribed roles.

Session	IT Audit Programme overview	Days
1	IT and IT governance in the Nordea Group	1
2	Auditing the IT providers and auditing general IT controls (with case)	1
3	Auditing business applications (with case)	2
4	Auditing development activities (with case)	2
5	Using SAP in auditing	1

Auditing Information Systems and Related Technology

Session 1: IT and IT governance in the Nordea Group

WHO SHOULD ATTEND

Mandatory one-day course for all business auditors and IT auditors alike.

COURSE OBJECTIVE

- To provide the necessary background and understanding for this training programme in auditing IS/IT in Nordea
- To provide an overview of the way we have decided to manage IT in Nordea (based on the upcoming *Nordea IT Governance Handbook*)
- To familiarise all auditors with the current IT situation in Nordea following the sourcing strategy (Nordic Processor etc)

COURSE CONTENT

1. The division of responsibilities within Internal Audit Activity
   - Introducing this training programme
   - Introducing the *IT Audit Service Catalogue*
2. IT governance in Nordea
   - Introducing key player # 1: The Board
   - Introducing key player # 2: Group Executive Management
   - Introducing key player # 3: The Business Areas
   - Introducing key player # 4: Group IT
   - Introducing key player # 5: Other GPT units
   - Introducing key player # 6: Nordic Processor
   - [illegible] importance
   - [illegible] / expertise / flow
   - [illegible]
   - Processes
   - Brief introduction to [illegible] chnical architecture
   - Introducing our key business systems
   - Important IT development activities

Group IT Mgmt

PREPARATIONS

Familiarise yourself with the contents of the *IT Audit Service Catalogue, version 1.0*, and bring your own copy with you. This document will be downloadable from CDC's intranet pages prior to the course starts.

LANGUAGE: English.

PROVIDER	CPE POINTS
Senior Group IT personnel will cover items 2 and 3, and CDC will cover item 1	The exact CPE points will be communicated when the detailed course agenda has been finalised. The current estimate is: CIA / CCSA / CFSA / Dipl. I.R. = 6 CISA = 6

TIME AND PLACE

Oslo:	11 March 2005	Stockholm:	8 March 2005
Copenhagen:	9 March 2005	Helsinki:	10 March 2005

Standard format (can be deviated from): Day 1 from 09:30 to 16:30.

In closing, I think …

- The concept of ”governance” is still growing on our profession – and IT Governance is an important part
- The frameworks are just in, and further alignments and reconciliations between them will surely help:
  - COSO ERM appropriately placing IT risks
  - CobiT 4 as the IT Governance mgmt model
- ”Continuous” assurance is another challenge

In closing, I think …

- Global IIA is working on it – and local IIA affiliates need to step up to the plate too
  - inspirational examples from IIA Norway?
- There are no quick fixes here – CAEs must demand that internal auditors need to buckle up for the ride
  - Commitment to invest and continuously improve
  - Nordea example shows the importance of bringing IT management into the training of our internal auditors

Agenda

- Agreeing on the starting point
  - Defining IT Governance & Continuous Assurance
- Guidance from The IIA
- Examples on local IIA level: Norway
  - What we have done & plan to do next
- Investing in IA training: the Nordea case
- Q & A session

Providing Continuous Assurance on IT Governance: Is the Internal Audit Profession up for it?

Frank Alvern *CIA, CCSA, CISA*
Chief Staff Officer, IIA Norway
frank.alvern@nirf.org

NORGES INTERNE REVISORERS FORENING
Fremskritt gjennom delt kunnskap

The Institute of Internal Auditors Finland 1956–2006

F-1
How to look bigger than you are?

Hans Nieuwlands (NED)
Audit Manager; Nuon Netwerk Services / Asset management
Vice President of ECIIA

8 September 2006

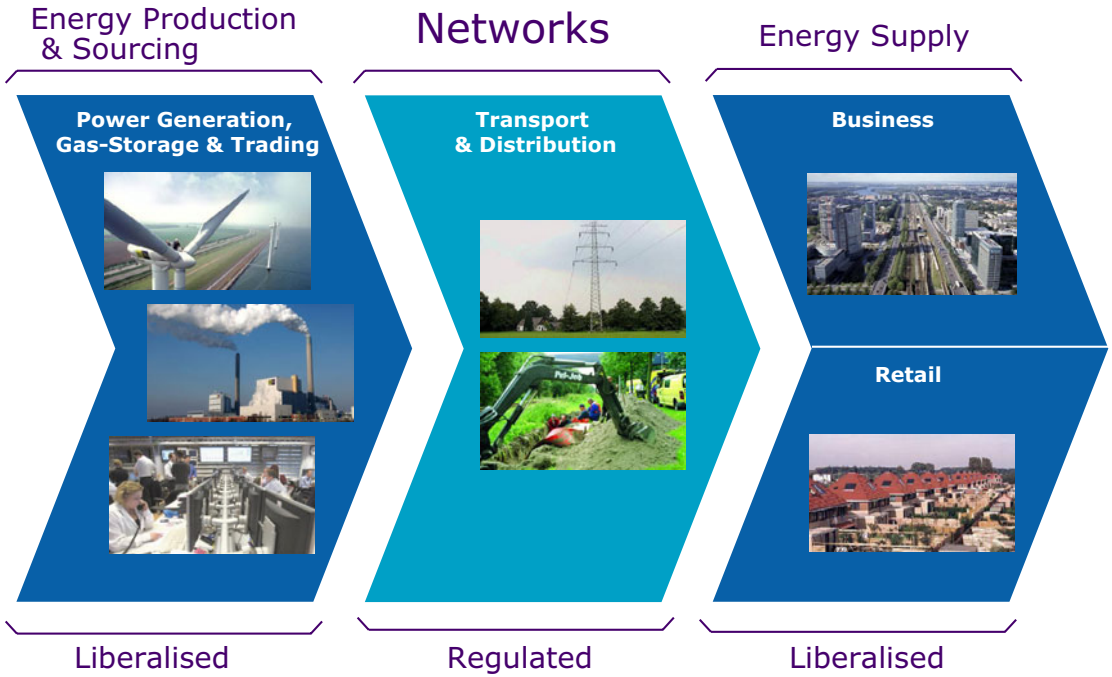
How to look bigger than you are

Hans Nieuwlands RA CIA CCSA CGAP

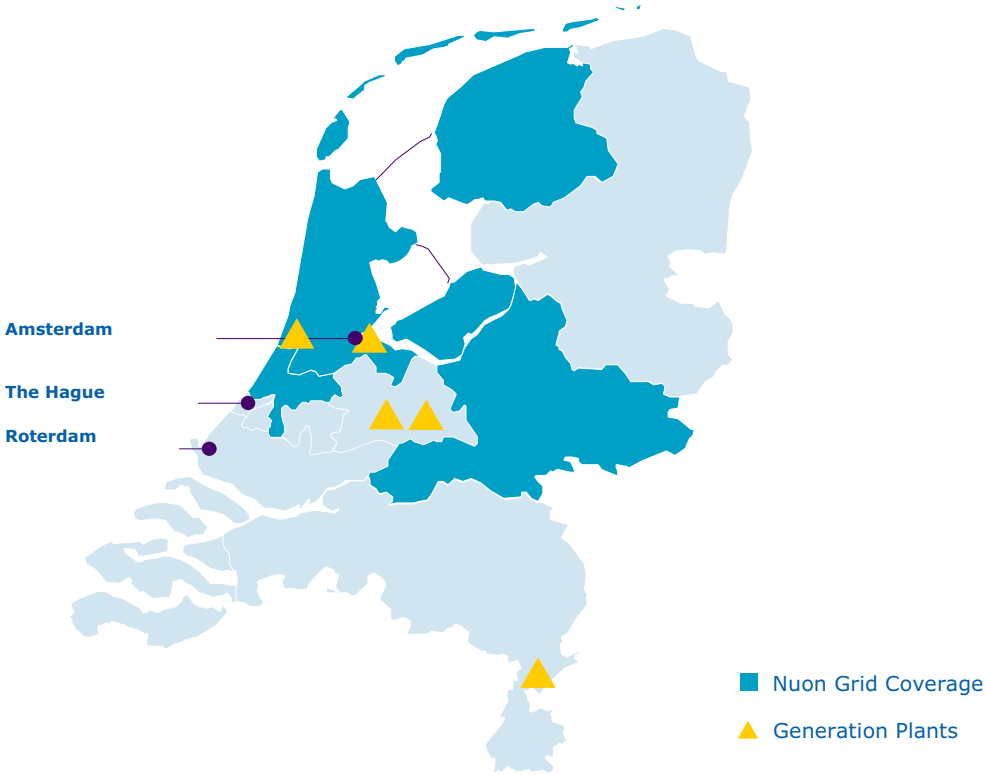
Outline

- Background of Nuon
- Critical Success Factors
- Staffing issues
- Types of work
- Reporting
- Customer Satisfaction
- Quality Assessment
- Communication
- Conclusion

Nuon Energy value chain

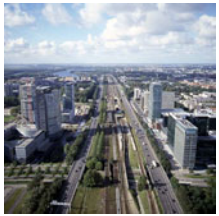
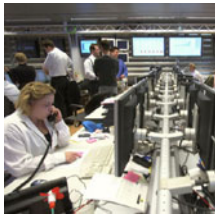


Main Network Regions in the Netherlands



Nuon Company profile (2005)

- Net turnover of € 5 Bn
- Operational Profit € 1,1 Bn
- Total assets € 11.2 Bn
- Power generation capacity 4000 MWe
- Generated electricity 14 GWh
- Generated heat 6.8 TJ
- Employees 9665 FTE
- Corporate auditors 10 FTE
- Network Services auditors 6 FTE


Critical Success Factors

- Quality of work
- Staffing
- Add value
- Positioning
- Visibility
- Open mind
- Creativity
- Communication
- Customer Satisfaction
- Demonstrate successes
- Follow up on recommendations

Staffing Issues

- Recruit only experienced auditors
- Ensure every uses the same reference (IIA-Professional Practices Framework)
- Have a right mix of knowledge and skills in the team
- Look for the unusual in the résumé (hidden talents)
- All auditors should be excellent communicators
- Encourage thinking outside the box
- Create a team spirit

Staff Qualifications

- Certified Internal Auditor
- Certificate in Control Self Assessment
- Certified Government Auditing Professional
- Quality Management Systems Lead Auditor (ISO 9001)
- Environmental auditor (ISO 14001)
- Safety auditor
- Operational auditor
- Chartered Accountant
- ICT
- …

Staff Satisfaction

- Assignment of audits in line with the interest of staff members
- Empower the auditor
- Encourage open communication
- Praise them for a job well done
- Meet bi-weekly to discuss any issues
- Discuss results of Corporate employee satisfaction survey
- Agree a challenging personal development scheme
- Discuss progress on personal development formally
- Recognise achievements in staff magazines
- Encourage to write articles for internal and external magazines
- Encourage networking in/outside the company

Use in house experts

- Engineers
- Experts on environmental regulations
- Operational regional managers to work in another region
- Safety experts
- Trainers
- Limited time

- Experienced auditor has the lead
- Write report jointly

Type of Audits

- Operational
- Technical
- Safety
- Environmental
- Reliability of reporting
- Project evaluations

Type of Consultancy

- Advise on the impact of the Dutch Corporate Governance Code
- Support development of Enterprise Risk Management System
- Advise on Operational Improvements
- Advise on reviews by non experienced auditors
- Mediation

Other Activities

- Organise workshops/seminars
- Facilitate ERM sessions
- Assist in set up of environmental self scan
- Mediation
- Facilitate Self Assessments on strategic directions of ICT, long term sick leave, technical improvements, innovations
- …

Annual Audit Planning

- Meet with Management to discuss input/concerns
- Agree on in sourcing of experts
- Include consultancy
- Include facilitating self assessments
- Make a realistic plan
- Be flexible with updates
- Align with corporate values

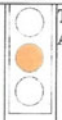
Audit Plan Align with Corporate values

- Safety
- Quality of Services
- Sustainability (environment)
- Legal aspects
- Financial performance
- Image
- Compliance with specific Utility Regulations

Reporting

- Agree draft reports with customer
- Be clear about distribution list (in draft version)
- Include management's comments and action plan
- Issue reports timely
- Report interim when needed (oral or in writing)
- Ensure excellent writing
- Make sure that recommendations are very clear
- Include photo's, graphs, drawing when feasible

Audit reports: Quick glance on results

Nr	Proces	Oordeel		Toelichting
	MANAGEMENTPROCES			
MGT1.01	Besturingsproces		**T: 0** **A: 1**	- het in de procedure beschreven vergelijkingsdocument bestaat niet - activiteiten van MT-leden in dit proces zijn niet beschreven
MGT1.02	Directiebeoordeling en evaluatie		**T: nvt** **A: nvt**	- procedure is nog niet in praktijk uitgevoerd
	PROCES CONTRACTEREN			
CT2.01	Opstellen P&D portfolio AM		**T: 0** **A: 1**	- afstemming met processen van Standaardisatie & Normalisatie is niet geregeld.
CT2.02 CT2.03	'Reactieve' acquisitie klant en Onderhandelen klant		**T: 0** **A: 1**	- risico's door concentratie van werkzaamheden bij één medewerker zonder aanwezigheid van werkinstructies.
CT2.04 CT2.05 CT2.06	Acquisitie externe leverancier; Onderhandelen externe leverancier; Verstrekken van opdrachten intern		**T: 3** **A: 2**	- processen zijn niet ingevoerd en ook een plan ontbreekt - DVO/SLA met Infraservices niet geregeld; geen versiebeheer - onvolkomenheden in procesbeschrijvingen

Audit reports: Use of photos

NUON
Asset management
Audit

en of fabrikaten mogen niet door elkaar gebruikt worden. De monteurs
n van hetzelfde type en fabrikaat.

vuil worden afgevoerd. Lege
l en weggegooid met het overige

nen deze doorgeprikt te worden en te
n luchtinsluitingen worden er
rder kan stromen. Deze worden

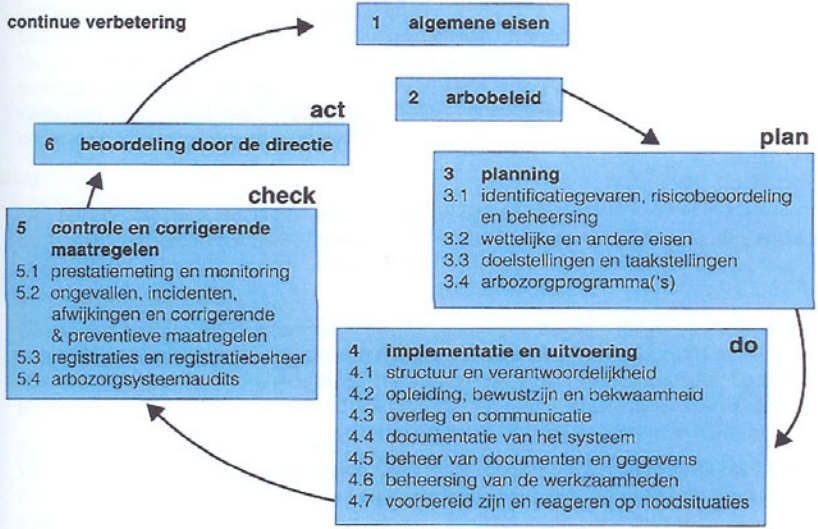
etaped. Het inspuitventiel wordt in 2 (AA, AP) van de 3 gevallen

met aanwezige grond en na een half uur (aannemer) tot drie kwartier
id.

Audit reports: Use recognized paradigms

t milieu geen onderdeel is van deze audit. "

audit heeft zich gericht op de keten CN-AM-Aanleg/S&O. De conclusies en bevindingen van deze audit zijn naar rwachting Nuon-breed van toepassing. De insteek van de audit was primair de inrichting van een iligheidsmanagementsysteem en niet de effectiviteit van bestaande veiligheidsmaatregelen op de werkvloer. Niet derzocht is op welke wijze er met veiligheidsaspecten rekening wordt gehouden bij het ontwerpen van tallaties door AM.



guur 1. OHSAS 18001

Communication: Audit reports

Don’t forget:

This is your main product !

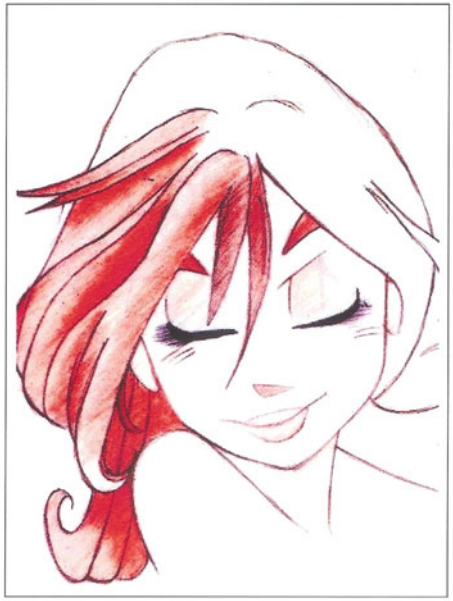
Customer Satisfaction

- Agree Audit approach with customer
- Have interim meetings when needed
- Inform customer timely about delays
- Submit evaluation form after completion for audit and consultancy work
- Discuss form with customer when needed
- Monitor overall satisfaction with kpi
- Analyse results of surveys and take preventative measures

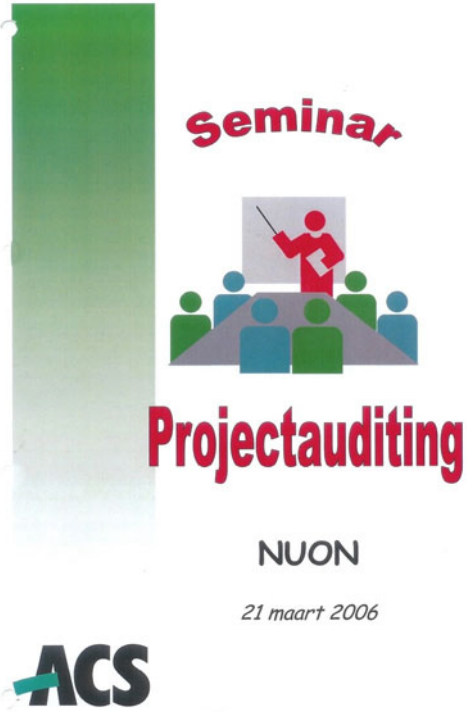
Customer Satisfaction: Evaluation form

1. Purpose and Scope were clearly communicated with me
2. Through put time of the audit was acceptable
3. My concerns with operational aspects have been taken into account adequately
4. Communication on the progress and findings of the audit was timely and adequate
5. The auditors have satisfactory expertise
6. The auditors showed respect
7. The auditors met promises
8. Results of the audit were clearly communicated and put in the right perspective
9. Audit recommendations are constructive and feasible
10. The audit added value to my department

Organise Workshops/seminars

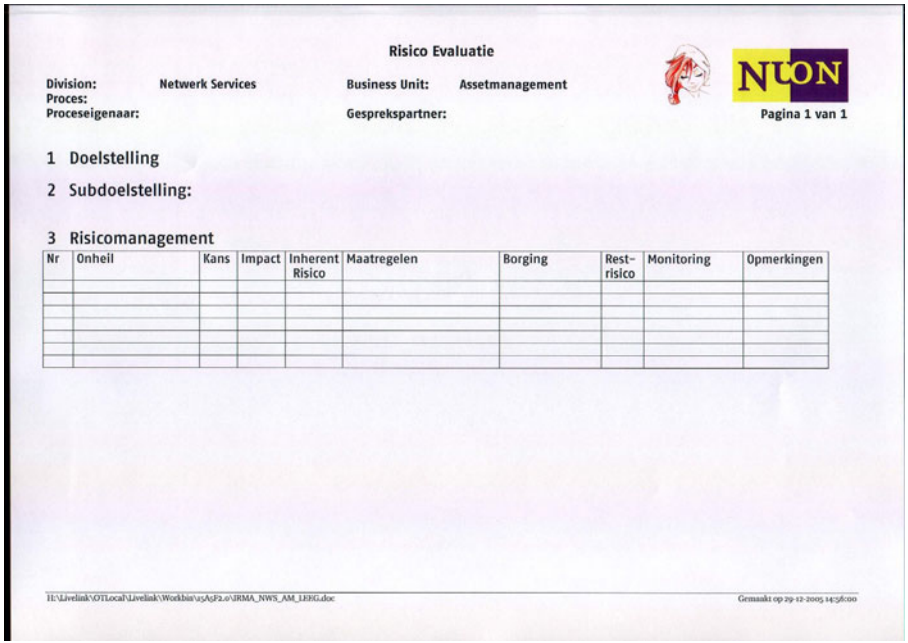


IRMA
NWS Workshop
Integraal Risicomanagement



Workshop Risk Management

- Create own Materials



Risico Evaluatie

Division: Netwerk Services Business Unit: Assetmanagement
Proces:
Proceseigenaar: Gespreksparter: Pagina 1 van 1

1 Doelstelling

2 Subdoelstelling:

3 Risicomanagement

Nr	Onheil	Kans	Impact	Inherent Risico	Maatregelen	Borging	Rest-risico	Monitoring	Opmerkingen

H:\Livelink\OTLocal\Livelink\Workbin\u5A5F2.0\IRMA_NWS_AM_LEEG.doc Gemaakt op 29-12-2005 14:56:00

Workshop Risk Management: Books

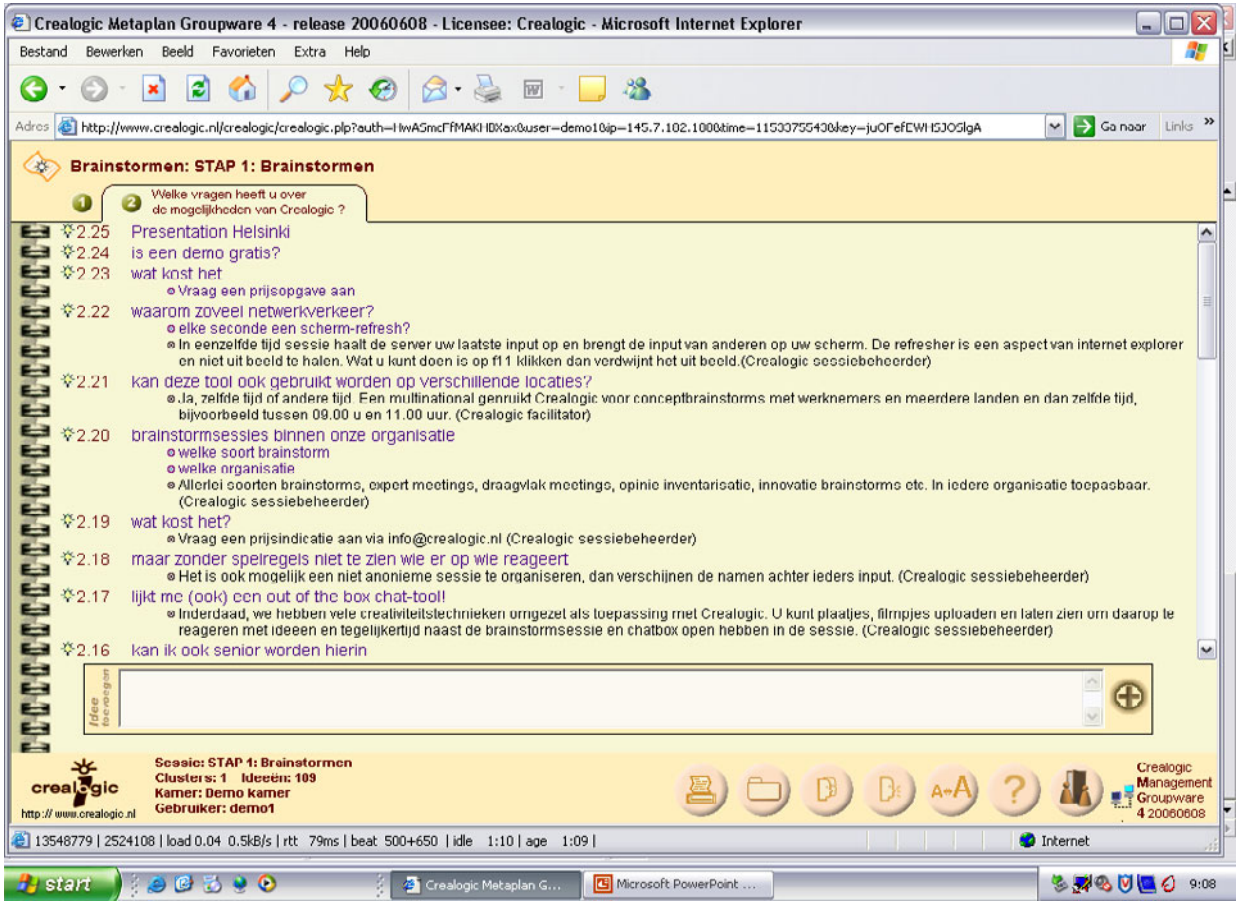
- Give away books

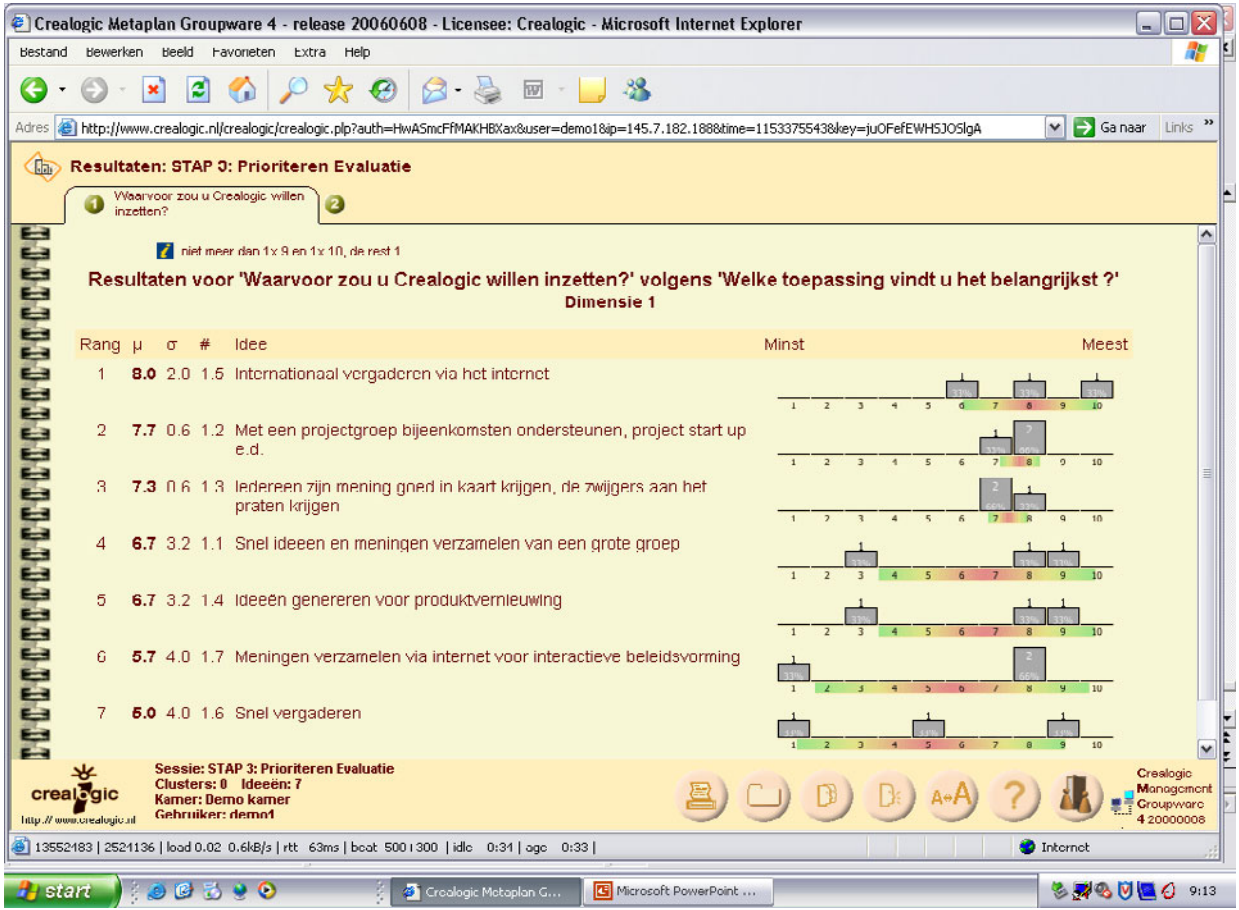
Seminar Project Audit

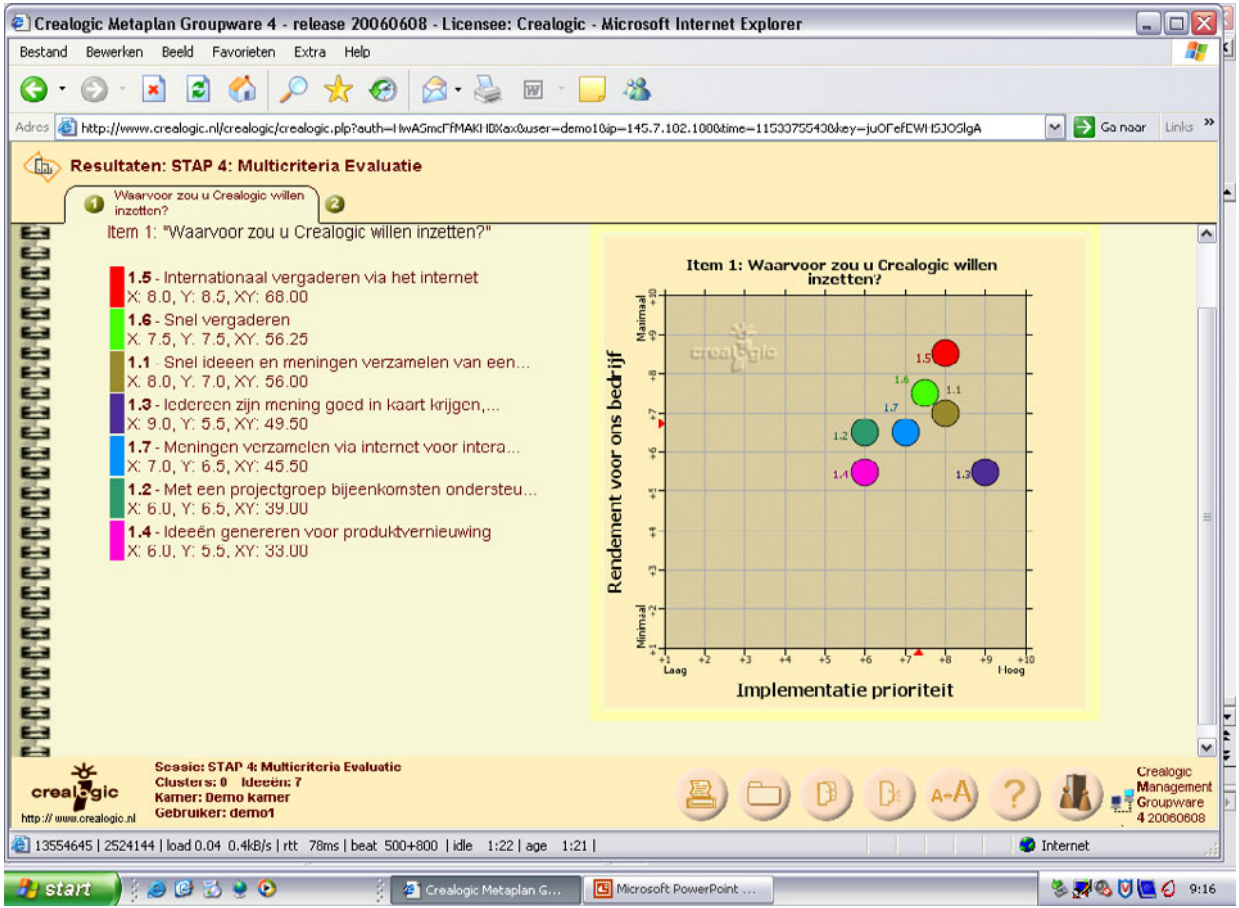
- Starting point: existing IIA seminar
- Third party provider: ACS
- Taylor made, focussing on project development standards used by Nuon
- Limited preparation time
- Marketing also outside own environment
- Several project managers attended
- Created good network
- Created new opportunities: to include audit as a standard phase in the project life cycle.

Other services: Facilitate CSA Sessions

- Invest in preparing CSA sessions with customer
- Start with "comfort zone" subject (e.g. Internal Controls)
- Expand gradually with related topics (e.g. Risk Management)
- Be responsive to new requests, even outside the comfort zone
- Evaluate each sessions with the customer
- Familiarise with Groupware software
- Produce session reports very quickly (software allows to print during the session)
- Enjoy the fun!


Crealogic Metaplan Groupware 4 - release 20060608 - Licensee: Crealogic - Microsoft Internet Explorer
Bestand Bewerken Beeld Favorieten Extra Help
Brainstormen: STAP 1: Brainstormen
Welke vragen heeft u over de mogelijkheden van Crealogic ?
2.25 Presentation Helsinki
2.24 is een demo gratis?
2.23 wat kost het
Vraag een prijsopgave aan
2.22 waarom zoveel netwerkverkeer?
elke seconde een scherm-refresh?
In eenzelfde tijd sessie haalt de server uw laatste input op en brengt de input van anderen op uw scherm. De refresher is een aspect van internet explorer en niet uit beeld te halen. Wat u kunt doen is op f11 klikken dan verdwijnt het uit beeld.(Crealogic sessiebeheerder)
2.21 kan deze tool ook gebruikt worden op verschillende locaties?
Ja, zelfde tijd of andere tijd. Een multinational gebruikt Crealogic voor conceptbrainstorms met werknemers en meerdere landen en dan zelfde tijd, bijvoorbeeld tussen 09.00 u en 11.00 uur. (Crealogic facilitator)
2.20 brainstormsessies binnen onze organisatie
welke soort brainstorm
welke organisatie
Allerlei soorten brainstorms, expert meetings, draagvlak meetings, opinie inventarisatie, innovatie brainstorms etc. In iedere organisatie toepasbaar. (Crealogic sessiebeheerder)
2.19 wat kost het?
Vraag een prijsindicatie aan via info@crealogic.nl (Crealogic sessiebeheerder)
2.18 maar zonder spelregels niet te zien wie er op wie reageert
Het is ook mogelijk een niet anonieme sessie te organiseren, dan verschijnen de namen achter ieders input. (Crealogic sessiebeheerder)
2.17 lijkt me (ook) een out of the box chat-tool!
Inderdaad, we hebben vele creativiteitstechnieken omgezet als toepassing met Crealogic. U kunt plaatjes, filmpjes uploaden en laten zien om daarop te reageren met ideeen en tegelijkertijd naast de brainstormsessie en chatbox open hebben in de sessie. (Crealogic sessiebeheerder)
2.16 kan ik ook senior worden hierin
Idee toevoegen
Sessie: STAP 1: Brainstormen
Clusters: 1 Ideeën: 109
Kamer: Demo kamer
Gebruiker: demo1
Crealogic Management Groupware 4 20060608
Internet
start
Crealogic Metaplan G...
Microsoft PowerPoint ...
9:08


Crealogic Metaplan Groupware 4 - release 20060608 - Licensee: Crealogic - Microsoft Internet Explorer
Bestand Bewerken Beeld Favorieten Extra Help
Adres http://www.crealogic.nl/crealogic/crealogic.plp?auth=HwASmcFfMAKHBXax8user=demo18ip=145.7.182.1888time=1153375543&key=juOFefEWH5JOSlgA
Ga naar Links
Resultaten: STAP 3: Prioriteren Evaluatie
Waarvoor zou u Crealogic willen inzetten?
niet meer dan 1x 9 en 1x 10, de rest 1
Resultaten voor 'Waarvoor zou u Crealogic willen inzetten?' volgens 'Welke toepassing vindt u het belangrijkst ?'
Dimensie 1
Rang μ σ # Idee Minst Meest
1 8.0 2.0 1.5 Internationaal vergaderen via het internet
2 7.7 0.6 1.2 Met een projectgroep bijeenkomsten ondersteunen, project start up e.d.
3 7.3 0.6 1.3 Iedereen zijn mening goed in kaart krijgen, de zwijgers aan het praten krijgen
4 6.7 3.2 1.1 Snel ideeen en meningen verzamelen van een grote groep
5 6.7 3.2 1.4 Ideeën genereren voor produktvernieuwing
6 5.7 4.0 1.7 Meningen verzamelen via internet voor interactieve beleidsvorming
7 5.0 4.0 1.6 Snel vergaderen
crealogic
http:// www.crealogic.nl
Sessie: STAP 3: Prioriteren Evaluatie
Clusters: 0 Ideeën: 7
Kamer: Demo kamer
Gebruiker: demo1
Crealogic Management Groupware 4 20000008
13552183 | 2521136 | load 0.02 0.6kB/s | rtt 63ms | bcat 500 | 300 | idle 0:34 | age 0:33 |
Internet
start
Crealogic Metaplan G...
Microsoft PowerPoint ...
9:13


Crealogic Metaplan Groupware 4 - release 20060608 - Licensee: Crealogic - Microsoft Internet Explorer
Bestand Bewerken Beeld Favorieten Extra Help
Resultaten: STAP 4: Multicriteria Evaluatie
Waarvoor zou u Crealogic willen inzetten?
Item 1: "Waarvoor zou u Crealogic willen inzetten?"
1.5 - Internationaal vergaderen via het internet
X: 8.0, Y: 8.5, XY: 68.00
1.6 - Snel vergaderen
X: 7.5, Y: 7.5, XY: 56.25
1.1 - Snel ideeen en meningen verzamelen van een...
X: 8.0, Y: 7.0, XY: 56.00
1.3 - Iedereen zijn mening goed in kaart krijgen,...
X: 9.0, Y: 5.5, XY: 49.50
1.7 - Meningen verzamelen via internet voor intera...
X: 7.0, Y: 6.5, XY: 45.50
1.2 - Met een projectgroep bijeenkomsten ondersteu...
X: 6.0, Y: 6.5, XY: 39.00
1.4 - Ideeën genereren voor produktvernieuwing
X: 6.0, Y: 5.5, XY: 33.00
Item 1: Waarvoor zou u Crealogic willen inzetten?
Rendement voor ons bedrijf
Implementatie prioriteit
Minimaal
Maximaal
Laag
Hoog
Sessie: STAP 4: Multicriteria Evaluatie
Clusters: 0 Ideeën: 7
Kamer: Demo kamer
Gebruiker: demo1
Crealogic Management Groupware 4 20060608
Internet
start
Crealogic Metaplan G...
Microsoft PowerPoint ...
9:16

Quality Assessment

- Self assessment QMS (ISO 9001)
- Peer review by other internal QMS auditors
- External audit by accredited ISO auditors
- External review by IIA-Netherlands

Quality Management System (ISO 9001)

- Strives for continuous improvement
- Pilot for a QMS for the whole division
- Hence, increased visibility for the audit function
- Fully external certified 3 years ago
- Re-certified in 2006
- Three staff auditors are trained ISO auditors
- Documents processes
- Structured approach
- Mandatory internal and external audits

Communication/visibility

- Develop a communication plan
- Include all available channels
- Define topics to communicate
- Match the topics with the best available channels
- Include graphs/photo's/cartoons
- Look for new technologies (webcasts, mp3, polls)
- Make sure the info on intranet is current and links are working

Communication Plan:Channels

- Internal magazines in print
- External magazines (o.a. IIA)
- Digital Newsletters

- Regular meetings
- BUs/Division gatherings
- Masterclasses
- Introduction Programs
- General Training Programs

- Intranet

Audit

Organisatie
Netwerk Services
Assetmanagement
AM afdelingen
Planning
Realisatie
AIV
Business Control
HRM
Audit
Secretariele en Algeme...

Audit

Internal Auditing is een onafhankelijke, objectieve "assurance" (geven van zekerheid) en consulting (geven van advies) activiteit met de bedoeling waarde toe te voegen aan en verbetering te brengen in de operaties van een organisatie.

Internal Auditing helpt een organisatie om haar doelen te verwezenlijken door een methodische, ordelijke benadering om de effectiviteit van risicomanagement, controle en beheersingsprocessen te evalueren en verbeteren.

Dit is vastgelegd in het **Internal Audit Charter**.

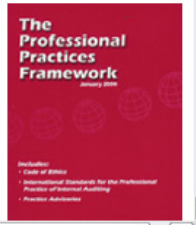
Audit:

- **doelstellingen en producten**

Contact:
Kunt u opnemen via Assetmanagement.Audit@nuon.com of met één van de onderstaande medewerkers. Heeft u vragen, klachten of opdrachten m.b.t. de verantwoordelijkheden binnen de afgesloten contracten met klanten en/of leveranciers dan kunt u dit melden via het Klachtenformulier AM.

Zoeken
Trefwoord
ZOEK ›

Gerelateerd
- mail naar Audit
- Audit Charter
- Doelstelling, Producten en Taken
- Klachtenformulier AM
- FAQ Audit



Communication: Website links

- General mailbox address
- Audit Charter
- Complaint form
- Mission/products/responsibilities
- IIA Professional Practices Framework
- Frequently asked questions

Communication: Website FAQ

- What is an audit ?
- How much time will it cost me ?
- Is cooperation mandatory ?
- Do I have to drop everything to help the auditor ?
- What happens with the information I provide ?
- What are the consequences for me ?
- What are the results of an audit ?
- Where can I find more information ?

Communication: Topics

- Certification ISO system
- Internal ISO audits
- Summary of audit findings
- Risk Management
- Feedback from Workshops/seminars
- Report on CSA sessions
- Corporate Governance
- Environmental issues
- Safety aspects
- Audit process
- Follow up monitoring
- …

Newsletter

Preventief gaslekzoeken

De afdeling Audit van Nuon Assetmanagement verricht, op verzoek van Continuon, een onderzoek naar de systematiek van het lekzoeken en het nakomen van de gemaakte afspraken. Daarbij wordt ook gekeken naar de borging van het daadwerkelijk verhelpen van de lekkages en het behalen van de planning.

Vlnr: Pieter de Jonge - Monteur, Rijk Pleiter - Teamleider S&O, Floor Karnebeek - Auditor

'Look in another man's kitchen'

Audit of Realization processes started

Joint audit by Regional managers and auditors

info: Audit Department

Attire Audit

Next Friday the Audit department will perform observation audits on the tidiness of employees' cloths.

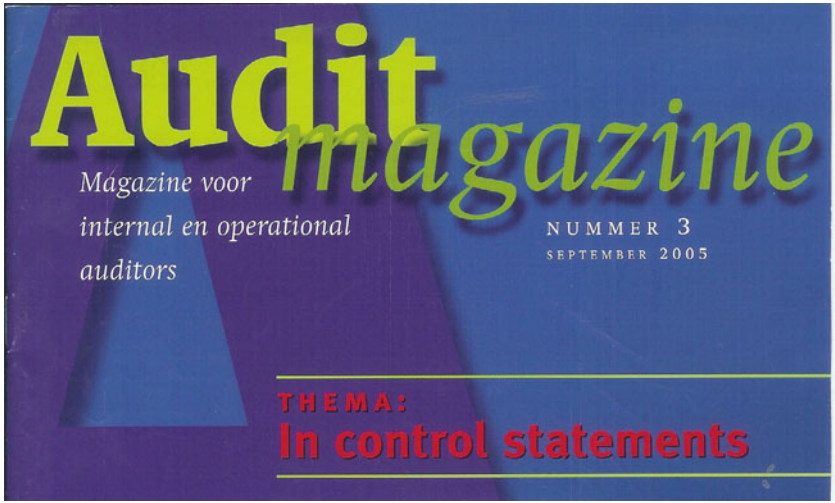
This is based on the paragraph decency and respect from the Corporate Code of Conduct.

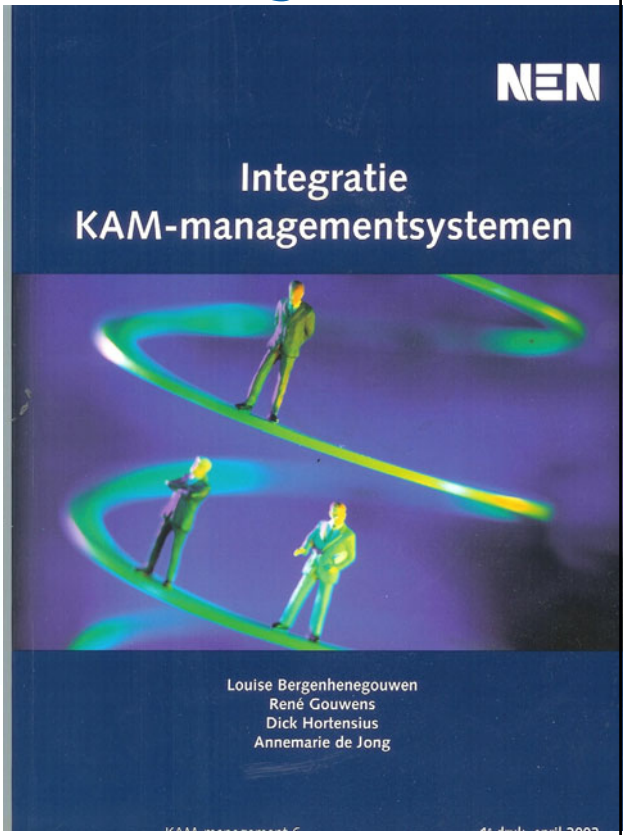
Attire Audit

Next Friday the Audit department will perform observation audits on the tidiness of employees' cloths.

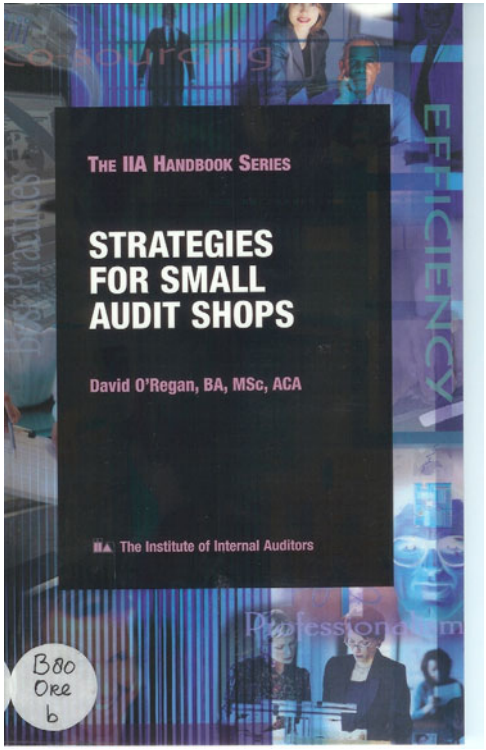
This is based on the paragraph decency and respect from the Corporate Code of Conduct.

Visibility: Distribute books and magazines





More information: www.theiia.org



Conclusion: To look bigger than you are:

- Add value
- Provide Quality
- Demonstrate Proficiency
- Be Visible, Proactive, Creative
- Communicate
- Enjoy your job !

You can look bigger than you are !

Questions/Suggestions/Comments ?

Hans Nieuwlands RA CIA CFE CCSA CGAP
Audit Manager

NUON

Netwerk Services / Assetmanagement

P.O. Box 9039, 6800 EZ Arnhem, The Netherlands
Utrechtseweg 68, Arnhem
Fax +31 26 844 27 62
Mobile +31 6 5538 7512
hans.nieuwlands@nuon.com

F-2
Quality Assurance in Small Internal Audit Departments

Dominique Vincenti (FRA)
Chief Officer
The IIA Research Foundation

Quality Assurance in Small Internal Audit Departments

The ECIIA Conference
Helsinki 2006

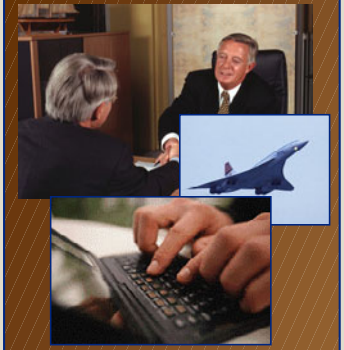
Dominique Vincenti, CIA
Chief Officer, Professional Practices, Certification & Quality,
Executive Director of The IIA research Foundation
IIA Global Head Quarters

The Institute of Internal Auditors

QUALITY
Ensuring Excellence

Presentation Objectives

What is quality & What do the quality standards require?



What does n quality assessment entail, and how can you prepare?

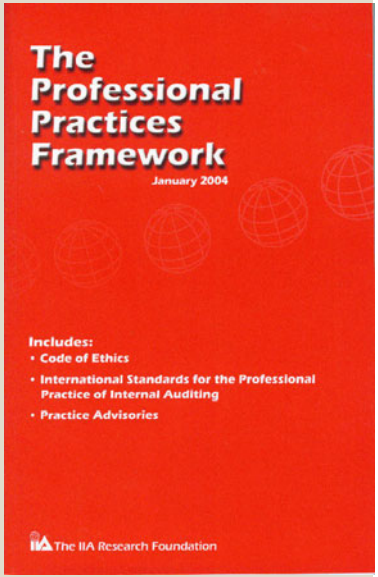
What are some common problems observed by QAR teams?

Quality Assessment

- The process of evaluating the efficiency and effectiveness of an internal auditing organization through a comprehensive, qualitative review of audit procedures, leading to recommendation for improving controls, reducing risk, and the introduction of successful innovative best practices. It should also ensure compliance with the *Standards for the Professional Practice of Internal Auditing* and other relevant organizational and departmental policies and procedures.

Quality Assurance: 7 New Standards

- Quality Assurance and Improvement Program *(1300)*
- Quality Program Assessments *(1310)*
- Internal Assessments *(1311)*
- External Assessments *(1312)*
- Reporting on the Quality Program *(1320)*
- Use of "Conducted in Accordance with the Standards" *(1330)*
- Disclosure of Noncompliance *(1340)*



Standard 1300
Quality Assurance & Improvement Program

- Includes both ongoing and periodic internal quality assessments.
- Includes an external quality assessment at least once every five years, the results of which are communicated to the Board of Directors (BOD) through the Audit Committee of the Board of Directors.

Standard 1310
Quality Program Assessments

- "The internal audit activity should adopt a process to monitor and assess the overall effectiveness of the quality program. The process should include both internal and external assessments."

- The assessment process is the same for internal and external assessments – the difference is that an external assessment requires the involvement of an independent team leader or validator.

Standard 1311
Internal Assessments

- Includes both ongoing and periodic reviews - point in time reviews of specific sections of the *Standards* using the tools from The IIA Quality Assessment Manual 5th Edition*:*
  - Preparation and planning – tool 1
  - Self Assessment Guide – tool 2A
  - Client and Staff Surveys – tools 4 & 5
  - Interviews – tools 6 - 11
  - Review Activities – tools 12 - 17
  - Evaluation – tool 18 & 19
  - Reporting and Follow-up – tool 20B

Standard 1312
External Assessments

- Two methods:
  - Self assessment with independent validation (SAIV)
  - Independent assessment with independent validation (QA)

Self-Assessment with Independent Validation

- This process must have the following features:
  - Comprehensive and fully documented self-assessment process
  - Independent on-site validation by qualified reviewer
  - Economical time and resource requirements

Self-Assessment with Independent Validation

- Self-Assessment is performed by a team under the direction of the CAE.
- Independent reviewer validates the results and expresses an opinion on compliance with the *Standards* by:
  - Conducting a few interviews of Senior Executives.
  - Performing limited tests of Self-Assessment.
- Includes a final report

Self-Assessment with Independent Validation

- Intended to expand External Assessment process to a wider range of internal audit activities.
- Focuses on basic expectations to ensure fulfillment of mission.
- Provides compliance review
- Time and cost reduced.
- Intended for small companies

Self-Assessment with Independent Validation

Does not offer in-depth recommendations regarding:

- Economies and Efficiencies
- Governance
- Consulting Services
- Advanced Technology

Self Assessment or external assessment: A practical approach

Conducting a quality assessment:

- Planning
- Tools and analysis
- Reporting

Conducting a QA - Planning

- Begin the process:
  - Reserve the time for the assessment!
    - Planning = 100 hours
    - Execution = 200 hours
    - Reporting = 20 hours
    - Total = 320 hours

Conducting a QA - Planning

- Engage Audit Committee and senior management in the process:
  - Budget and contract negotiation is required; the self assessment will be validated by an external party.
- Assign a lead person and IA staff to the project.

TOOL 1
PREPARATION AND PLANNING

Activity

1. Agree to lead the review and reserve time.
2. Negotiate, review, and sign contract with client specifying the timing and duration of the review.
3. Review inquiry form, proposal letter, and proposed time frames for details and any special objectives and schedules.
4. Determine status of surveys. (**Tools 4 & 5)**
5. Contact CAE to set up onsite or telephone preliminary meeting.
6. Receive self-assessment and review. (**Tool 2)**
7. Conduct preliminary meeting visit with CAE**.** Obtain completed CAE Questionnaire. **(Tool 3) (See administrative checklist for preliminary visit.)**
8. Send preliminary visit report to QA team members and CAE, if appropriate.
9. Establish team assignments. Contact team members for welcome and initial expectations.
10. Receive GAIN and review.
11. Review initial customer survey and staff survey data. **(Tools 4 & 5)**
12. Prepare for on-site: forms, electronic formats, etc.

Conducting a QA - Tool 2A

Complete the Self Assessment – Tool 2A:

I. POSITIONING

A. Background of the Organization
B. Risk Management, Governance, Accountability, and Oversight
C. Background of the Internal Audit Activity (IA activity)
D. Internal Audit Practice Environment (including Support, Authority, and Scope)
E. Relationship of the IA Activity with Senior Management and the Board (Audit Committee)

II. PROCESSES

A. Internal Audit Activity Documentation
B. Internal Audit Activity Effectiveness and Performance Measurements
C. Planning

III. PEOPLE

Conducting a QA - Tool 2A

- Tool 2A – Positioning:

  Determine if the internal audit activity is strategically positioned within the organization to enable it to contribute to the organization's objectives.

Conducting a QA - Tool 2A

- Tool 2A – People:

  Does the internal audit activity have the right people to deliver the approved audit objectives and annual audit plan?

Conducting a QA - Tool 2A

- Tool 2A – Processes:

  Does the internal audit activity processes enable achievement of their objectives and audit plan and allow the activity to be responsive to the changing needs of the organization?

Conducting a QA - Tools 4 and 5

Plan for the surveys – Tool 4 and 5:

- Who will receive the client surveys?
- Will the staff survey be used?
- When will the surveys be sent out?

The objective of the surveys is to gather valuable feedback from key stakeholders on the effectiveness and “value add” of internal audit.

Conducting a QA - Tools 4 and 5

- The client surveys should be sent to a broad cross section of managers in the organization who have interaction with internal audit. The goal is to obtain feedback from various levels in the organization, not just the senior executives.
- Staff surveys should be sent to all members of the internal audit activity.
- The surveys should be anonymous and protect the confidentiality of the respondent.

Conducting a QA - Tools 6 - 11

- Decide who to interview:
  - Tool 6 – Audit Committee Chair
  - Tool 7 – Executive to Whom CAE Reports
  - Tool 8 – Senior and Operating Management
  - Tool 9 – Chief Audit Executive
  - Tool 10 – Internal Audit Staff
  - Tool 11 – External Auditor
- The interviews are optional for a self assessment – in the case of a SAIV, the validator will conduct key interviews as part of the validation.

Conducting a QA - Tools 6 - 11

- Interviews provide valuable feedback from key stakeholders that can assist in the analysis conducted in Tools 12 – 17.
- Any preliminary observations from interviews should be substantiated with additional analysis of documentation.

Conducting a QA - Tools 6 - 11

- Interviews should be scheduled as far in advance as possible to allow access to key stakeholders with limited availability.
- Interviews should take 30 – 45 minutes each with the exception of the Tool 9 – Chief Audit Executive – which may take up to 90 minutes.

Conducting a QA - Tool 12

THE CHIEF AUDIT EXECUTIVE REPORTING LINES AND QUALITY ASSURANCE RESPONSIBILITY

- Procedures (Standards 1000, 1110, 1310, 1340, 2060)
- The objectives of this module are to evaluate whether the CAE:
  - Reports to a level within the organization that allows the internal audit activity to accomplish its responsibilities,
  - Maintains effective audit committee relationships,
  - Maintains a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness.

Conducting a QA - Tool 12

Evidence to Examine:

- Minutes of the Board
- IA Activity Charter
- Organization Charts
- Audit Committee Charters
- Budget and Staffing of IA Activity
- IA Policies and Procedures
- Performance Indicators
- Formal Results of Assessments Performed
- External Assessment Report

Conducting a QA - Tool 13

RISK ASSESSMENT AND AUDIT PLANNING

- Procedures (Standards 2010, 2010.A1)
- The objectives of this module are to assess whether the IA activity's planning process considers the organization's enterprise risk framework, management control environment, and accountability processes, as well as the organization's strategic and technology plans and significant business activities to arrive at the annual and longer-term plan. The risk assessment and planning process should involve four stages: risk assessment, audit plans, staff analysis, and budgeting.

Conducting a QA - Tool 13

- Evidence to Examine:
  - Annual Audit Plan
  - Formal Risk Assessment
  - Strategic Plan of the Organization
  - Formal Opinions of Senior Management [considered in the process]
  - Board Minutes

Conducting a QA - Tool 14

STAFF PROFESSIONAL PROFICIENCY

- Procedures (Standards 1210, 1210.A1, 1210.A2, 1210.A3, 1210.C1, 1220, 1230, 2020, 2030, 2340)
- The objectives of this module are to appraise the recruitment, development, and assignment of the right mix of staff skills to achieve the internal audit activity's mission/goals.

Conducting a QA - Tool 14

- Evidence to Examine:
  - Job Descriptions
  - Hiring and Selection Procedures
  - Training Plans
  - Annual and Engagement Performance Evaluations
  - Resumes of Staff
  - Work Paper Reviews
  - Professional Activities
  - Certifications of Staff
  - Staffing Analysis and Annual Operating Plan
  - Staff Utilization Ratios
  - IA Policies and Procedures

Conducting a QA - Tool 15

INFORMATION TECHNOLOGY

- Procedures – (Standards 2010, 2010.A1, 1210.A3, 1220.A2)
- The objectives of this module are to review and evaluate the IT audit processes/activities in the following key result areas:
  - Risk identification
  - Audit coverage
  - Staff expertise/training
  - Prospective risk-based auditing focus
  - Use of CAATS (Computer-assisted Audit Tools)

Conducting a QA - Tool 15

- Evidence to Examine:
  - Annual Audit Plan
  - Formal Risk Assessment
  - Strategic Plan of the Organization
  - Formal Opinions of Senior Management [considered in the process]
  - Board Minutes
  - Job Descriptions
  - Hiring and Selection Procedures
  - Training Plans
  - Annual and Engagement Performance Evaluations
  - Resumes of Staff
  - Work Paper Reviews

Conducting a QA - Tool 16

ASSESSING PRODUCTION AND VALUE ADDED

- Procedures (Standards 2030, 2400, 2060)
- The objectives of this module are to evaluate activity reports and determine how the internal audit activity (IA activity) monitored program accomplishment and added value to the organization.

Conducting a QA - Tool 16

- Evidence to Examine:
  - Staffing Analysis and Annual Operating Plan
  - Annual Audit Plan
  - On-time Performance of Audit Engagements Monitored
  - Board Minutes
  - CAE Board Presentation
  - Status of Action Plan from Audit Observations
  - Work Program, Objectives and Scope of the Engagement
  - Procedures for Validating and Reporting Audit Results
  - Engagement Communications
  - Audit Reports

Conducting a QA - Tool 17

PLANNING AND CONDUCTING THE ENGAGEMENT, WORKPAPER REVIEW, AUDIT REPORT, AND MONITORING PROGRESS

- Procedures (*Standards* 2200, 2201, 2201.A1, 2210, 2210.A1, 2210.A2. 2220, 2220.A1, 2220.A2, 2230, 2240, 2240.A1, 2300, 2310, 2320, 2330, 2330.A1, 2330.A2, 2340, 2400, 2410, 2410.A1, 2410.A2. 2410.A3, 2420, 2421, 2430, 2440, 2440.A1, 2440.A2, 2500, 2500.A1)

- The objectives of this module are to assist the QA team members in evaluating work papers. This review is to determine whether the IA activity staff and management are complying with The IIA's *Standards* and the policies of the activity.

Conducting a QA - Tool 17

- Evidence to Examine:
  - Audit Engagement Letter
  - Audit Work Program
  - Audit Work Papers
  - Evidence that Fraud is Considered
  - Elements of criteria, condition, cause, effect and recommendation considered
  - IA Policies and Procedures
  - Approval Documents
  - Evidence of Supervision
  - Organization and Regulatory Requirements
  - Assessment of Risk to the Organization
  - Audit Reports
  - Audit Report Distribution
  - Board Minutes
  - Formal Follow up Procedure

Conducting a QA - Tool 18

- Observations and Issues Worksheet
  - All observations resulting from the previous analysis steps are documented on Tool 18 – one Tool 18 for each observation.
  - A recommendation is also provided in the Tool 18
  - Both the observation and recommendation are discussed with the CAE prior to inclusion in the report.

Conducting a QA - Tool 19

- After completing all of the tools in The IIA Quality Assessment Handbook, 5th Edition, Tool 19, should be used to provide an overall assessment of the organizations conformance with the *Standards*.

Conducting a QA - Tool 19

- Consider each section of the *Standards* (numbers ending in "00") and conclude as to the degree of conformity by the activity to each section taken as a whole, based on conclusions reached for the related individual *Standards* in the section and on other relevant observations made during the QA. If all underlying *Standards* are non-conforms then the overall *Standard* is does not conform. Otherwise, the team must make a judgment based on the number of non-compliant and the specific conditions present as to whether the overall rating is does not conform or partially conforms.

- On the same basis as for sections of the *Standards*, conclude as to the degree of conformity by the activity to the major categories of the *Standards* (ATTRIBUTE and PERFORMANCE); then make an overall evaluation as to the activity's conformity to the *Standards* as a whole.

Conducting a QA - Tool 19

- **GC – "Generally Conforms"** means the evaluator has concluded that the relevant structures, policies, and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual *Standard* or element of the Code of Ethics in all material respects. For the sections and major categories, this means that there is general conformity to a majority of the individual *Standards* or elements of the Code of Ethics, and partial conformity to the others, within the section/category. There may be significant opportunities for improvement, but these should not represent situations where the activity has not implemented the *Standards* or the Code of Ethics, is not applying them effectively, or is not achieving their stated objectives.

Conducting a QA - Tool 19

- **PC – "Partially Conforms"** means the evaluator has concluded that the activity is making good-faith efforts to comply with the requirements of the individual *Standard* or element of the Code of Ethics, section, or major category, but falls short of achieving some major objectives. These will usually represent significant opportunities for improvement in effectively applying the *Standards* or Code of Ethics and/or achieving their objectives. Some deficiencies may be beyond the control of the activity and may result in recommendations to senior management or the board of the organization.

Conducting a QA - Tool 19

- **DNC – "Does Not Conform"** means the evaluator has concluded that the activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many/all of the objectives of the individual *Standard* or element of the Code of Ethics, section, or major category,. These deficiencies will usually have a significant negative impact on the activity's effectiveness and its potential to add value to the organization. They may also represent significant opportunities for improvement, including actions by senior management or the board.

Conducting a QA - Tool 20B - Reporting

Report should include:

- Executive Summary
- Background
- Results:
  - Successful Practices Currently in Effect
  - Opinion on Conformance with the Standards
  - Items for Consideration by Senior Management
  - Items for Consideration by the Internal Audit Management
  - Suggestions for Improvements in Efficiency and Effectiveness of the Internal Audit Activity.
  - Suggestions for Additional Successful Practices

Common Observations in QAs

- Out-of-date charters for internal audit activity
  - Internal audit activity's consulting responsibilities
  - Reflection of consulting in the mission and charter
- Client perception of inadequate audit staff knowledge
- Lack of a formalized risk assessment process
- Inadequate IT coverage or technical skills
- Audit Universe not fully developed

Quality Assessment Resources
http://www.theiia.org/quality

- Quality Assessment Manual 5th Edition, chapters 1 - 4
- Frequently Asked Questions about Quality
- Providers of external QA services
- List of organizations that have undergone external QAs
- Becoming a quality assessment team member volunteer

Quality Assessment Resources http://www.theiia.org/quality

- Sample request for a QA proposal
- Advanced preparation document
- Audit customer (client) survey
- Internal audit staff survey
- Self assessment guide
- Models - Audit Committee Charter, Internal Audit Activity Charter, Model Management Control Policy

Questions?

Contact information:

Mary L. Radley, CIA
Director, Quality
IIA Global Headquarters
E-mail: mary.radley@theiia.org

Guidance tools and information:
www.theiia.org/quality

F-3
Leveraging CAATs in Small Audit Departments

Juan Morales (CAN)
Master Trainer
ACL Services Ltd.

BUSINESS ASSURANCE ANALYTICS

Leveraging CAATs in Small Audit Departments

ECIIA
September 2006

Juan Morales
ACL Services Ltd.

ACL™
Data you can trust. Results you can see.

Today's Agenda

- Internal Audit – new challenges, new opportunities
- New role for data analytic technology
- Challenges to data access and analysis
- Analytical tools
- Continuous auditing/monitoring for integrated assurance
- Case study examples
- Key success factors
- Summary
- Q&A

New Challenges, New Opportunities

- SOX created new demands/opportunities
- Internal Audit viewed as internal controls experts – now responsible for change and discovery
- Key role in achieving compliance with SOX – overall role of IA shifting
- Greater demands without increased resources
- Compliance is an ongoing issue – not a one-time event

New Role for Data Analytics

- In Internal Audit
  - → Extend use beyond technical users or specialists
  - → Increase frequency of controls testing and scope at the transaction level
  - → Use during audit planning stages for maximum benefit
- In Management
  - → Embed technology solutions in critical business processes

Applications of Data Analytics

- General examples
  - → Travel & entertainment: expense claims, merchant analysis
  - → Asset management: depreciation, value calculations
  - → Salaries and payroll: overtime, bonuses
  - → General ledger: account reconciliation, financial ratios
  - → Accounts receivable: credit limits, discounts
  - → Inventory control: turnover rates, price/cost variance

Areas for Data Analytics

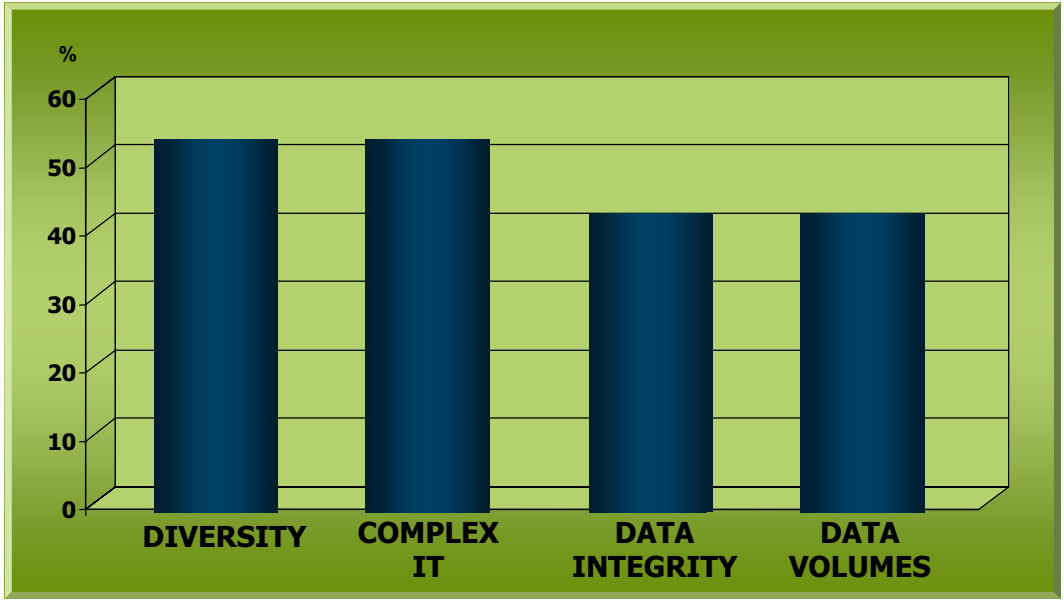
- Industry-specific examples
  - → Banking: loan reviews, portfolio analysis
  - → Education: grants compliance, financial aid
  - → Government: tax compliance, purchasing management
  - → Healthcare: patient billing, charges and claims
  - → Insurance: claims processing, investment securities
  - → Retail: gift card fraud, inventory shrinkage

Challenges for Internal Audit

Outcome	Current Challenges
Timeliness	Audit results are needed faster
Efficiency	Audit must do more – more often
Visibility	Source data resides on diverse systems
Volume	Large volumes of data must be analyzed
Accuracy	Data quality & completeness must be assured
Security	Maintaining corporate data security essential

Internal Auditors Survey

Significant challenges to data analysis:



From June 2005 poll of over 1,000 internal auditors, 96% of whom were using some form of data analytics technology.

Audit Technology Requirements: A Checklist

Outcome	Technology Requirements
Timeliness	α Direct data access α Powerful analytics α Leveraging server platforms
Efficiency	α Purpose-built for audit analysis α Efficient repeatability of audit tests
Visibility	α All data – from a single point of view α Seamless data access α Cross-platform analytics α Full audit trail for evidence, attestation
Volume	α Unlimited data populations α 100% coverage
Accuracy	α Independent of underlying systems α Read-only data analysis at the source
Security	α Co-exist within existing IT security protocols

Use of Spreadsheets

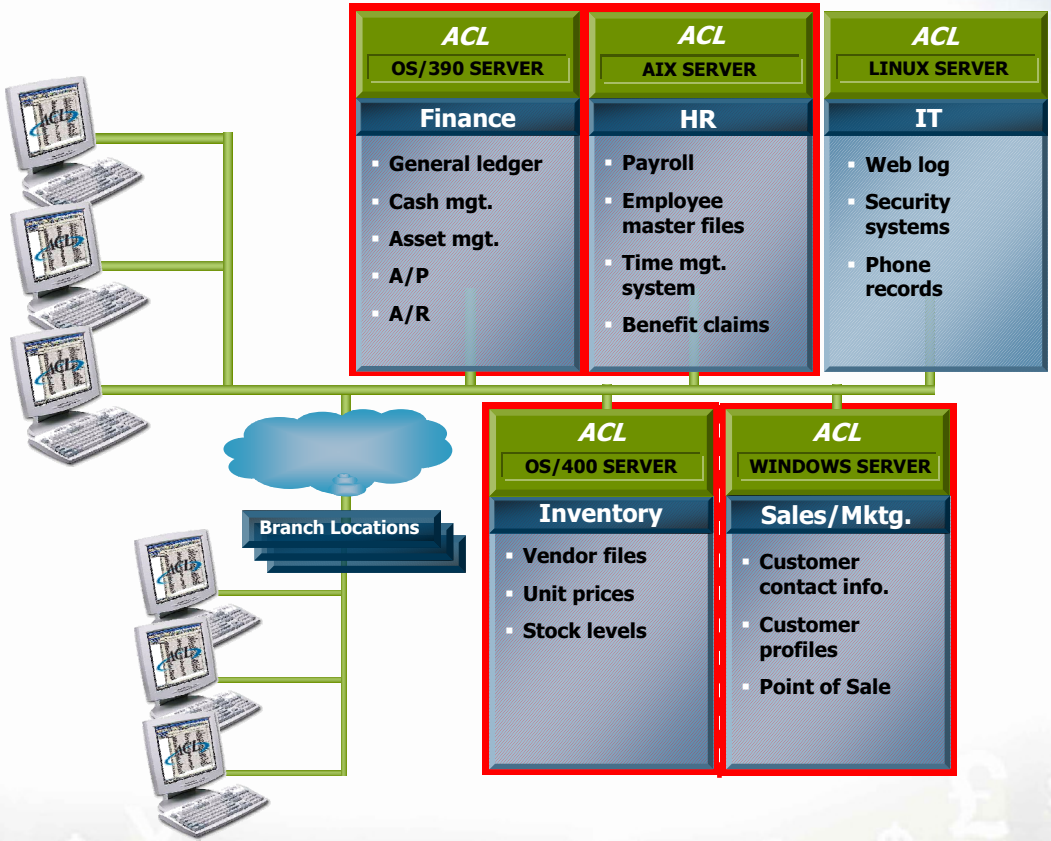
- Categories of use
  - → Financial
  - → Operational
  - → Analytical
- Risk considerations
  - → Complexity and size
  - → Purpose and use
  - → Number of users
  - → Frequency and extent of changes
  - → Potential for error
- Risk of error
  - → Recent audits of 54 spreadsheets found that 91% had errors*
  - → 30-90% of spreadsheets suffer from at least one major error*

"The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act," PwC, July 2004

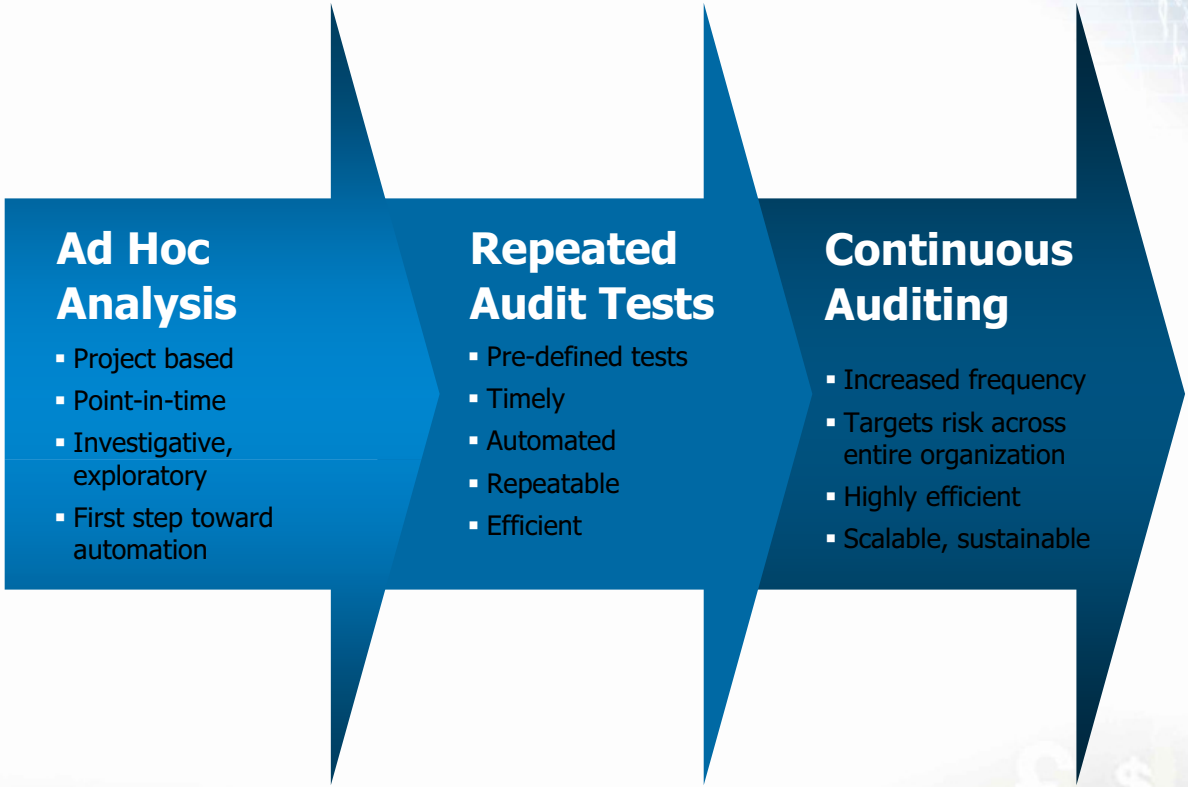
Specialized Data Analysis Software

- Review 100 percent of transactions
- No limit on file size
- Compare data from different applications & systems
- Perform tests that are designed for audit and control purposes
- Conduct tests proactively
- Ability to automate high-risk areas to catch fraud before it escalates
- Maintain comprehensive logs of all activities performed

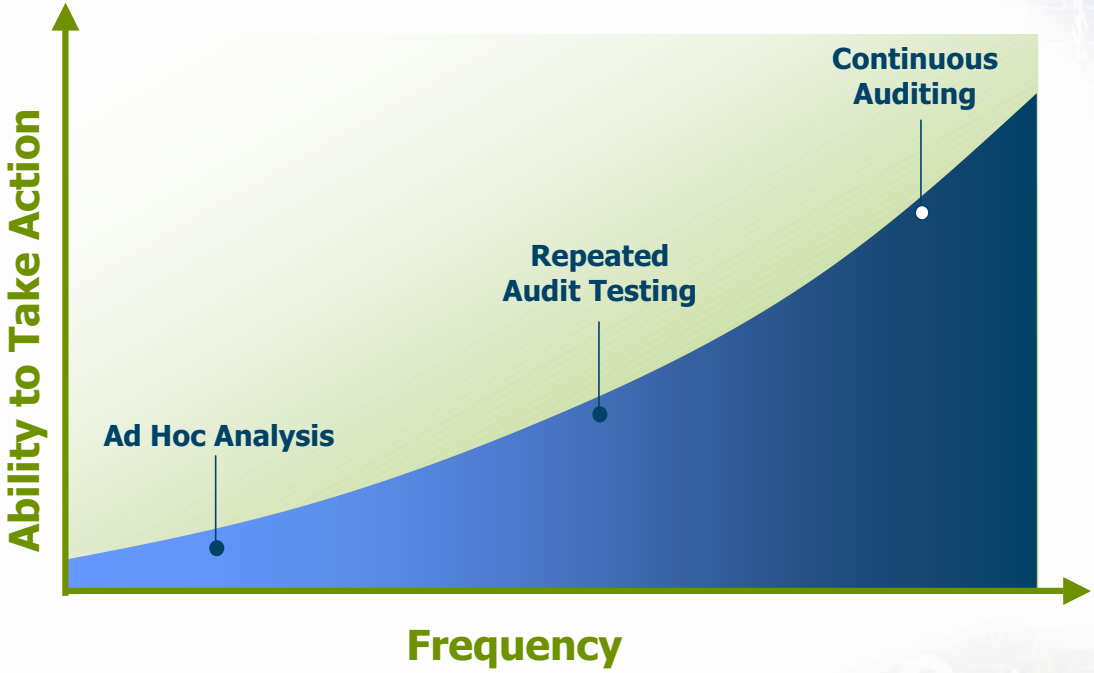
Accessing Data for Enhanced Productivity



Data Analytics Approaches



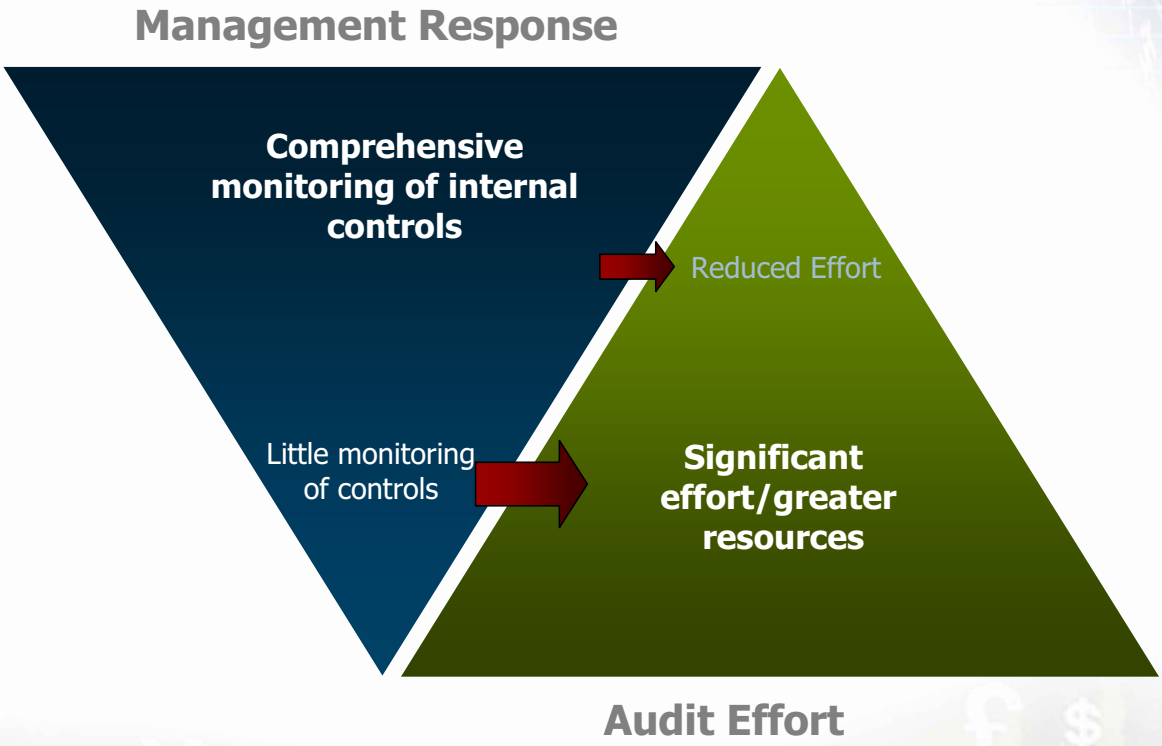
Continuous Auditing



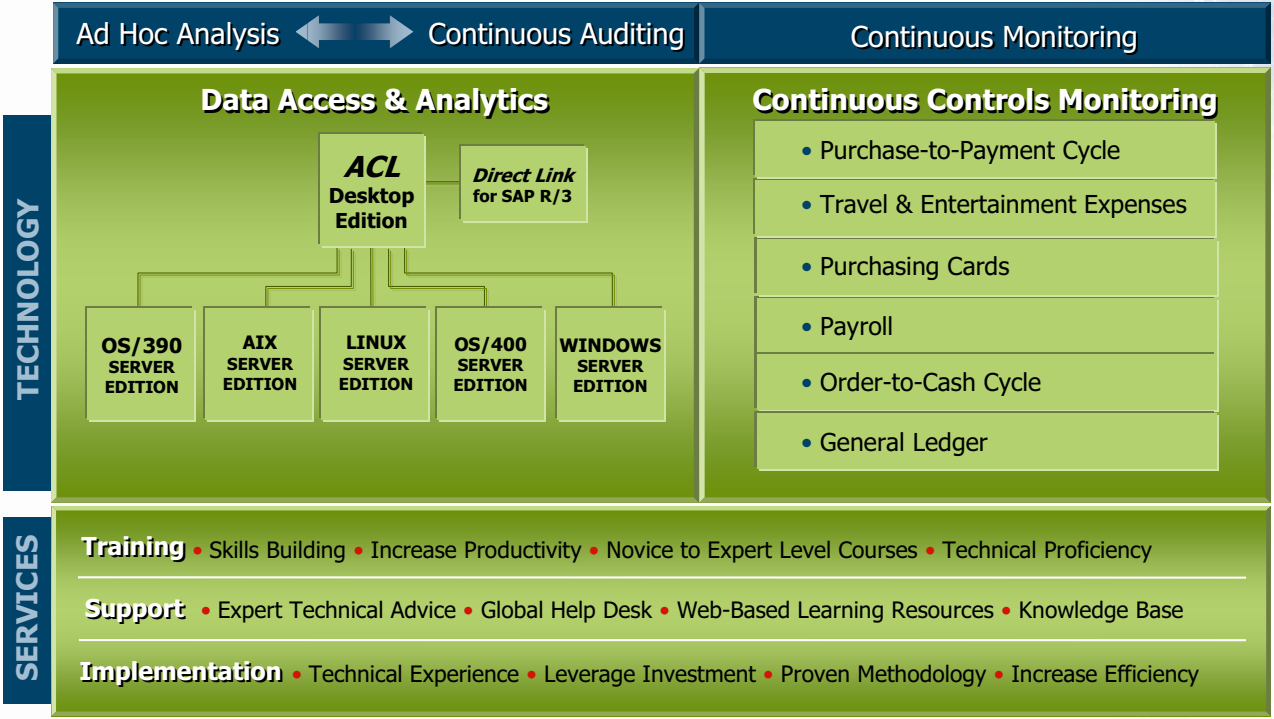
Continuous Auditing Benefits

- Key to ensuring internal controls are in place and operating effectively
- Exposes control weaknesses to prevent fraud
- Reveals anomalies close to time they occur to detect fraud early
- Existence is a deterrent

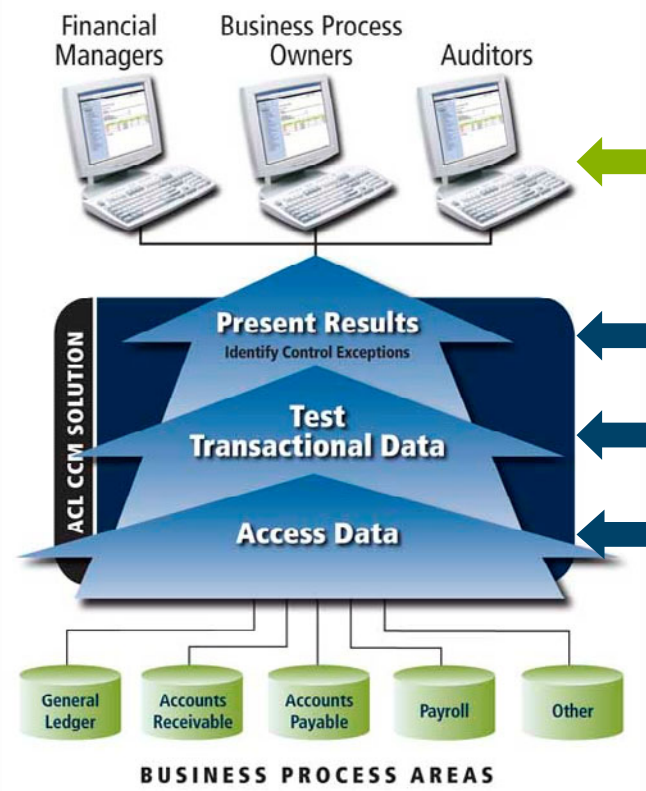
Internal Controls: Roles and Effort



Continuous Assurance



CCM Process



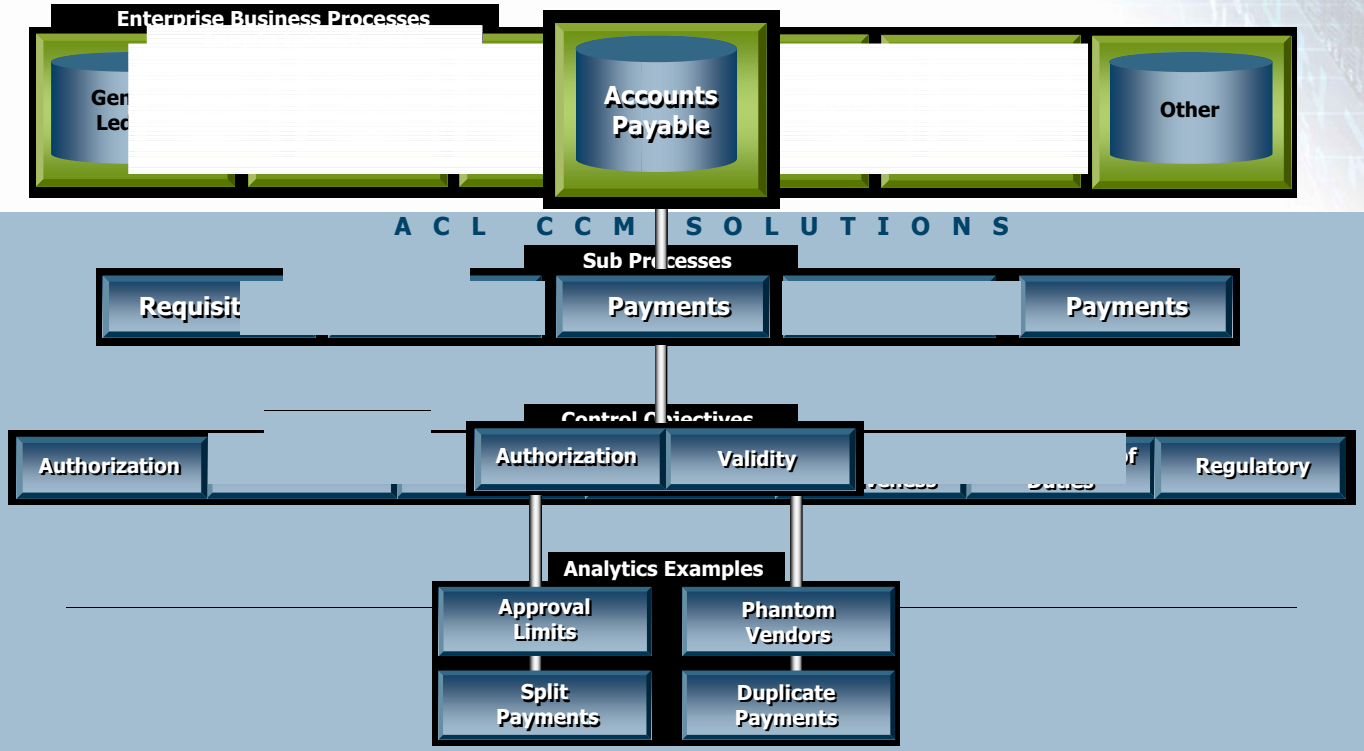
Provides visibility into controls health to all stakeholders

Presents quantified control exceptions

Applies automated tests to critical control points

Review 100% of transactions across all systems & platforms

Enterprise Business Processes



The Audit Cycle

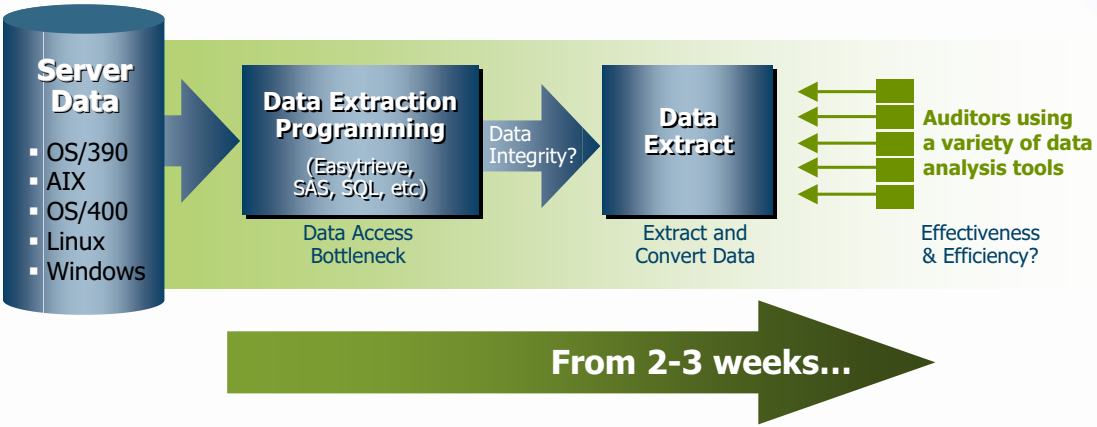
Planning

- Audits traditionally done on rotational basis
- Applying data analysis technology:
  - → Use ad-hoc testing to determine areas of greatest risk
  - → Use findings to plan audit
- Benefits
  - → Allows audits to focus on areas of highest priority and risk
- Case study
  - → Food Lion (Delhaize Group)

Preparation

- Typically make requests for data from IT
  - → Extracts can take weeks
  - → May not be what you needed, or may not be complete
  - → Requires new requests

Challenges in Data Extraction



- Time-consuming
- Issues of data integrity
- Quality of audit may suffer

Client/Server System

- Direct access across the enterprise
- Time savings, more efficient
- Quality of data and of audit higher

Substantive Testing

- Traditionally done by sampling or spot checks
- Using data analysis technology:
  - → 100% of data for more complete, accurate testing
  - → Full range of approaches to suit type of analysis
    - → Ad hoc
    - → Periodic
    - → Continuous auditing

Continuous Auditing

- Goal
  - → Need for timely, ongoing assurance over risk management and the overall control environment
- Role of continuous auditing
  - → Provides more frequent, more timely, analyses to better manage control deficiencies and risk
- Application areas
  - → Continuous control assessment
    - → Identification of control deficiencies
    - → Identification of fraud, waste, abuse
  - → Continuous risk assessment
    - → Examination of consistency of processes
    - → Development of enterprise audit plan
    - → Support to individual audits
    - → Follow-up on audit recommendations

Continuous Auditing Benefits

- Key to ensuring internal controls are in place and operating effectively
- Exposes control weaknesses to prevent fraud
- Reveals anomalies close to time they occur to detect fraud early
- Existence is a deterrent

Peer Review

- Typically manual, limited process
- Made far easier with ACL audit trail
  - → Historical record
  - → Each step is captured
- Promotes collaboration
- Enhances quality of overall audit department
- Supports professional development among team members

Report Findings

- Without the use of audit tools
  - → May be incomplete
  - → May require re-keying of findings
  - → Time-consuming
- With data analysis technology, reporting is streamlined
  - → Cut and paste charts, graphs into audit report
  - → Incorporate context of findings
  - → Export to standard working paper or reporting packages
  - → Complete, accurate and defensible findings

Small Audit Shop Case Study

BlueCross BlueShield of South Carolina

- Mutual insurance company serving over 21 million customers

Challenges

- Contain and manage internal expenses
- High volumes of transactions (6 billion in 2002)
- Urgent data requests and tight reporting deadlines

Solution Results

- Extend reach into enterprise data for marked improvements in productivity & efficiency
- Mitigate time pressures through fast responses to data requests
- Identify controls weaknesses & identify errors & fraud

Seven Steps to Success

1. Obtain **executive commitment** to data analytics
2. Select the **right solution** to meet all requirements
3. **Use strategically** by incorporating into audit plan
4. Develop a **data access strategy**
5. Enable **multiple users** for maximum impact
6. Ensure users are **well trained**
7. Apply a **continuous audit approach**

In Summary

Integrated data analytic technologies can benefit small audit departments by:

- Increasing efficiencies and shorten the audit cycle
- Providing broader, deeper coverage
- Providing increased assurance of accuracy of findings
- Ensuring independence
- Driving corporate performance through detection of
  - → Fraud
  - → Revenue leakage
  - → Business process inefficiencies
- Supporting regulatory compliance

Contact

BUSINESS ASSURANCE ANALYTICS

General Session 4
Internal Audit – The Challenge

Stephen Goepfert (USA)
Staff Vice President – Internal Audit, Continental Airlines &
Chairman of the IIA

Internal Audit –The Challenge "Tell the World"

Steve Goepfert, CIA, CPA
2006-2007 IIA Chairman of the Board
Staff Vice President – Internal Audit, Continental Airlines
ECIIA Conference
Helsinki, Finland

September 8, 2006

Our Role — Our Responsibility

- Adding Value
- Serving as advocate
  - Organizational governance
  - Internal audit profession
- Creating and sharing best practices
- Developing professional *Standards*
- Administering certification programs

Our Role — Our Responsibility

- Providing resources for world-class departments
- Expanding the global reach of the profession
- Marketing internal auditing as a long-term career choice
- Sharing the Vision for Our Future

The IIA & the Profession

- Experiencing phenomenal growth
- Garnering high visibility
- Enjoying credibility with management and the board

Adding value by . . .

- Identifying critical areas of risk and concern
- Keeping abreast of changing developments in accounting and internal control requirements
- Recruiting and retaining the best employees

Advocating for governance and the profession through . . .

- Participation with SEC / PCAOB
- Participation with COSO
- Participation with IFAC

Professional guidance . . .

- Professional Practices Framework
- Position papers and responses
- Research Foundation studies
- Quality

Professional certifications . . .

- Certified Internal Auditor (CIA)
- Certification in Control Self Assessment (CCSA)
- Certified Government Auditing Professional (CGAP)
- Certified Financial Services Auditor (CFSA)

Share best practices . . .

Identify programs and processes that enhance your department or organization.

Resources for world-class departments . . .

- Leading-edge conferences and seminars
- Webcasts and e-learning opportunities
- Benchmarking Network
- Award-winning publications

Expanding the global reach of the profession . . .

- Membership of more than 120,000
- Half of membership is outside North America
- 246 affiliates in 100 countries
- Members from 160 countries

Enhancing the rewarding career experience . . .

- Global academic development strategy
- Internal audit internships
- On-campus networking
- Student involvement with local chapters

Sharing the vision . . .

- Strategically growing the profession
- Creating additional educational products
- Advancing testing methods, such as computer-based testing

Providing valuable resources . . .

- Educational products and research
- Guidance
- Leadership available at meetings
- Training through sessions
- Web site and e-communications
- Academic Relations

Be enthusiastic about the profession!

- Be engaged!
- Be excited!
- Be proud to be an internal auditor!

"Tell the World!"

Thanks to Our Conference Sponsors

PLATINUM

Deloitte.

GOLD

ACL™

STANDARD

KPMG

PRICEWATERHOUSECOOPERS

ERNST & YOUNG

MIS TRAINING

ارامكو السعودية
Saudi Aramco

The Institute of Internal Auditors
Finland
1956–2006

IIA Finland
Itämerenkatu 5, FI-00180 Helsinki, Finland
Tel. +358-9-4730 3151
Fax. +358-9-4730 3152
E-mail: sisaiset.tarkastajat@theiia.fi
www.theiia.fi