

IT Governance:

The role of Audit, Review and Assessment

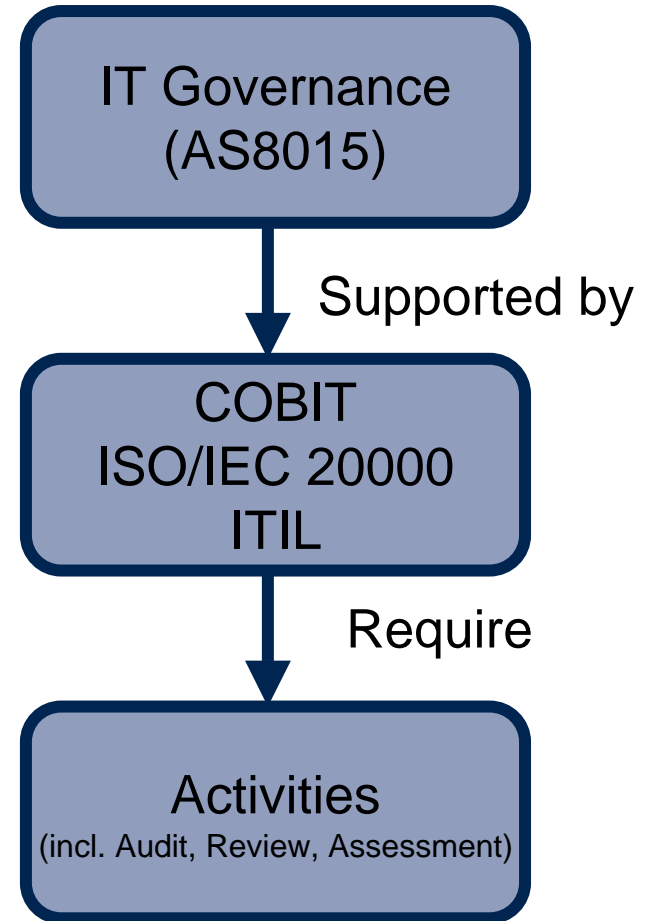
Ralph Gray
Fox IT Ltd



itSMF

Agenda

- Views of IT Governance
- Audit, Review, Assessment
 - Definition
 - Requirements
 - Activities
 - Examples, stories
 - Finding balance
- Summary and Questions
- In your notes:
 - An overview of ICT Governance Principles from AS8015



What is Governance?

Source: ITIL® v3 – Service Strategy

- Management and Governance are different disciplines.
 - Management deals with making decisions and executing processes.
 - Governance only deals with making sound decisions.
- (Governance) is the framework of decision rights that encourage desired behaviours ...
 - When companies confuse management and governance, they inevitably focus on execution at the expense of strategic decision making.
- Both are vitally important.

Three Views of IT Governance

● ITIL® v3

- Governance is ensuring that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

● ISACA / ITGI / COBIT

- IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

● AS8015:2005

- Corporate governance of ICT is the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization.

Three Views of IT Governance

1. Roles, responsibilities, organisation

● ITIL® v3

- Governance is ensuring that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

● ISACA / ITGI / COBIT

- IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

● AS8015:2005

- Corporate governance of ICT is the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization.

Three Views of IT Governance

2. Policies, strategies, plans, ...

● ITIL® v3

- Governance is ensuring that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

● ISACA / ITGI / COBIT

- IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

● AS8015:2005

- Corporate governance of ICT is the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization.

Three Views of IT Governance

3. Monitoring, evaluating, directing, ensuring, ...

● ITIL® v3

- Governance is ensuring that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

● ISACA / ITGI / COBIT

- IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

● AS8015:2005

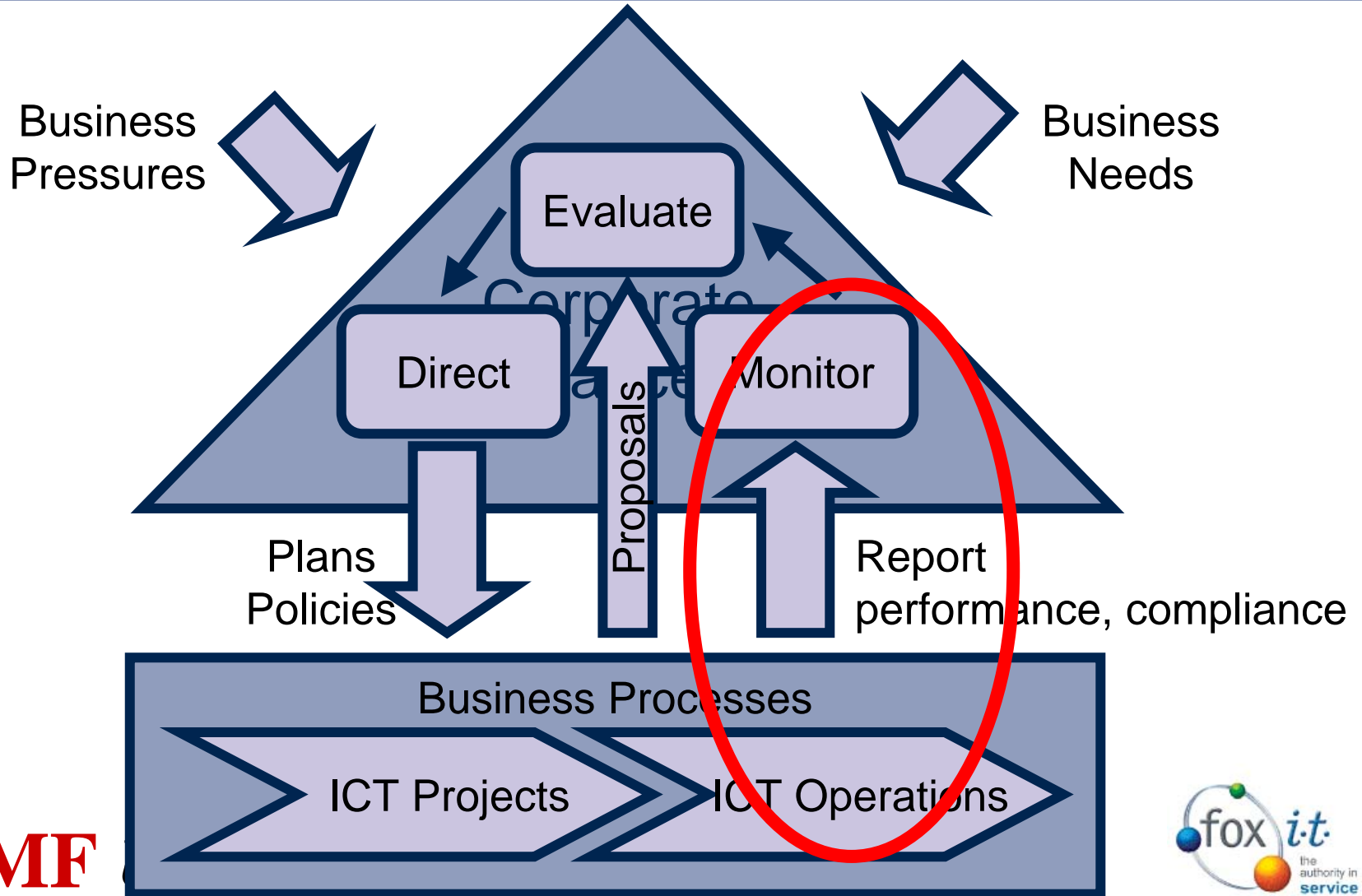
- Corporate governance of ICT is the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization.

Governance Standards

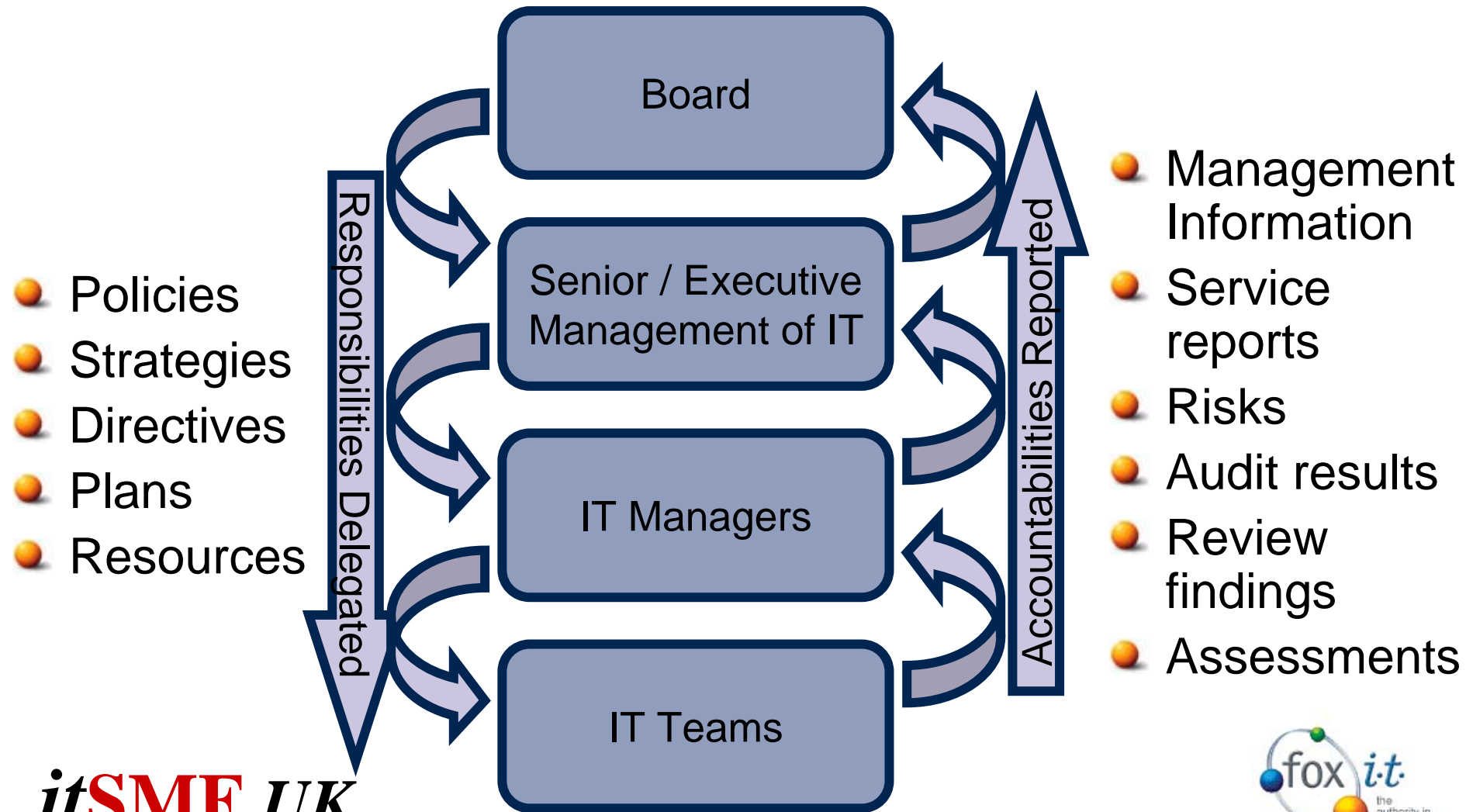
- Australian Standard AS8015-2005
“Corporate Governance of ICT”
 - The only national standard in the area of IT Governance
 - Currently being fast-tracked through the appropriate committees to become ISO/IEC 29352
- It establishes a model for governance of IT
- It defines 6 principles, with guidance for actions for each principle in the areas of:
 - Monitor
 - Evaluate
 - Direct

Corporate Governance of ICT

Source: AS 8015:2005

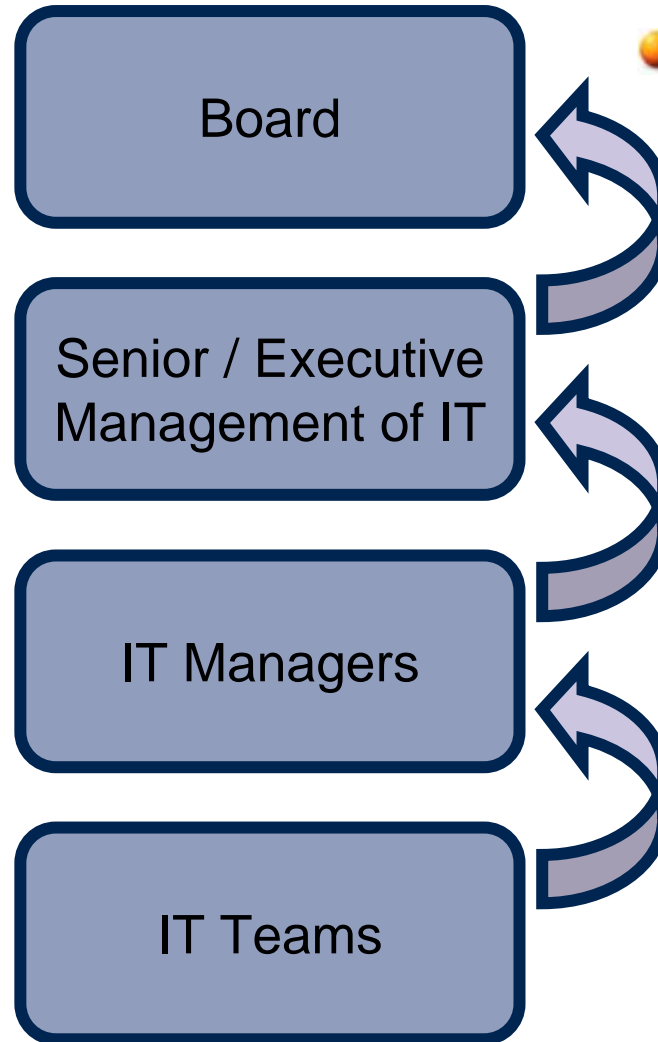


Who does IT Governance apply to?



How can audit, review and assessment help?

• They provide mechanisms that can be used by IT managers to report upwards in a structured, systematic way



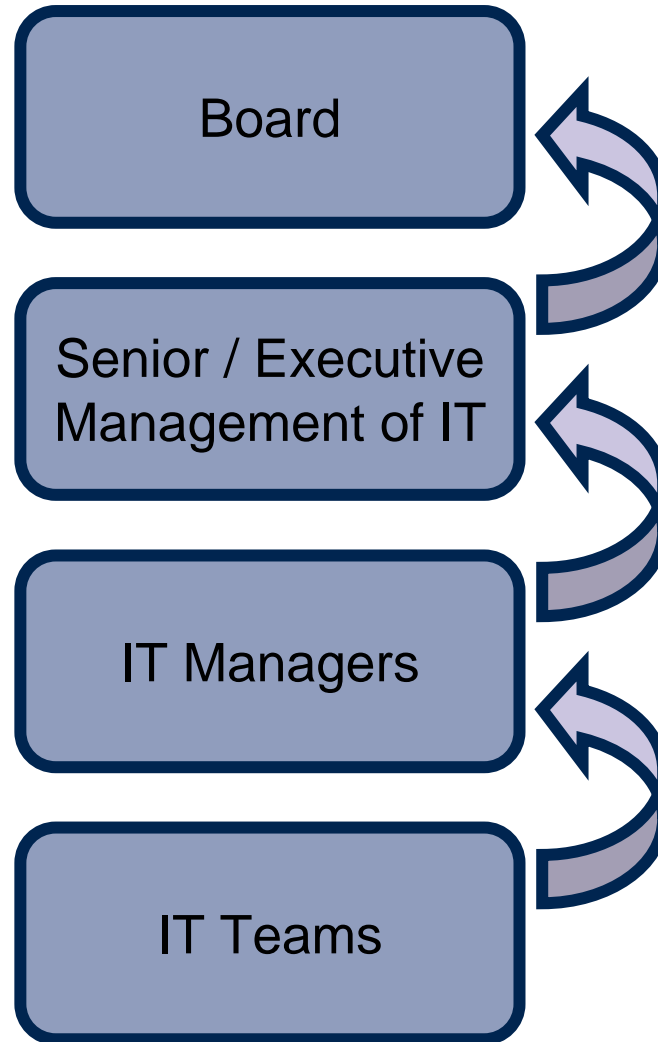
• They provide the information for senior management to execute their responsibilities to:

- monitor
- evaluate and
- direct

How can audit, review and assessment help?

Source: ISO/IEC 20000

- “The objective of service management reviews, assessments and audits shall be recorded ...



... together with the findings of such audits and reviews and any remedial actions identified.

- Any significant areas of noncompliance or concern shall be communicated to relevant parties.”

Review

Source: ISO 9000:2005

Definition:

An activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives



itSMF

Review - Requirements

- ISO/IEC 20000 (extracts)
 - Management shall ... conduct **reviews** of service management, at planned intervals, to ensure continuing suitability, adequacy and effectiveness.
 - The SLAs shall be maintained by regular **reviews** by the parties to ensure that they are up-to-date and remain effective over time.
 - The process for a major incident should include a **review** which will inform a plan for improving the service.
- Reviews can also be actions related to:
 - Analyse ...
 - Investigate ...

Reviews - Activities

- Reviews can be
 - Targetted, e.g.
 - a major incident review
 - An SLA or contract review with a client or supplier
 - Informal
 - “let’s discuss this latest set of figures”
 - Structured
 - Scheduled in a regular management meeting

Review – a true story

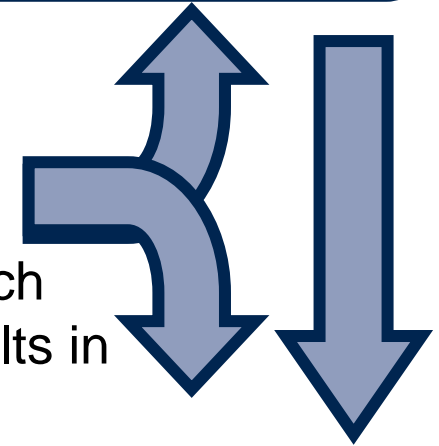
Major Incident



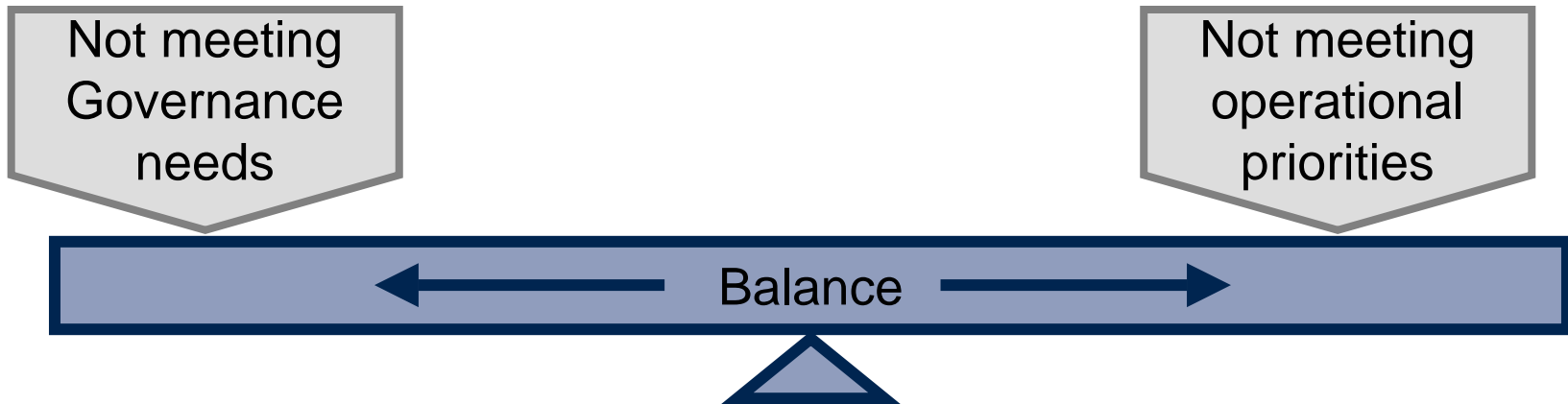
Escalation

Which results in

Actions



Achieving Balance in Service Reviews



- Too few reviews
- Poorly structured
- Results not documented
- Recommendations not followed up
- Not integrated with day-to-day activities

- Too much time spent reviewing
- Bureaucratic practices
- Can become overwhelmed with recommendations and actions

Audit

Source: ISO 9000:2005

Definition:

A systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled



itSMF

Audit - Requirements

● ISO 9001

- The organization shall conduct internal audits at planned intervals ...
- An audit programme shall be planned ...
- The management responsible for the area being audited shall ensure that actions are taken without undue delay ...

● ISO/IEC 20000

- (almost identical)

● COBIT (3rd Edition)

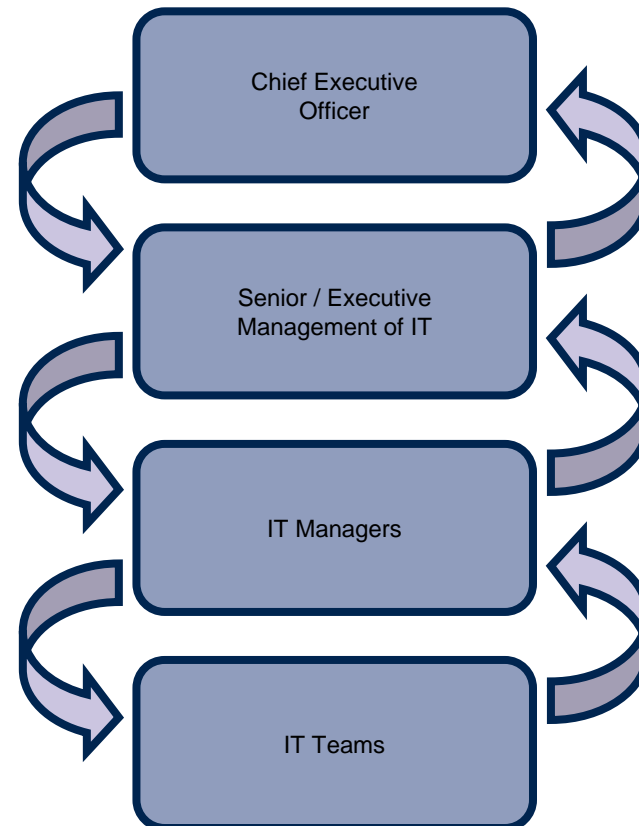
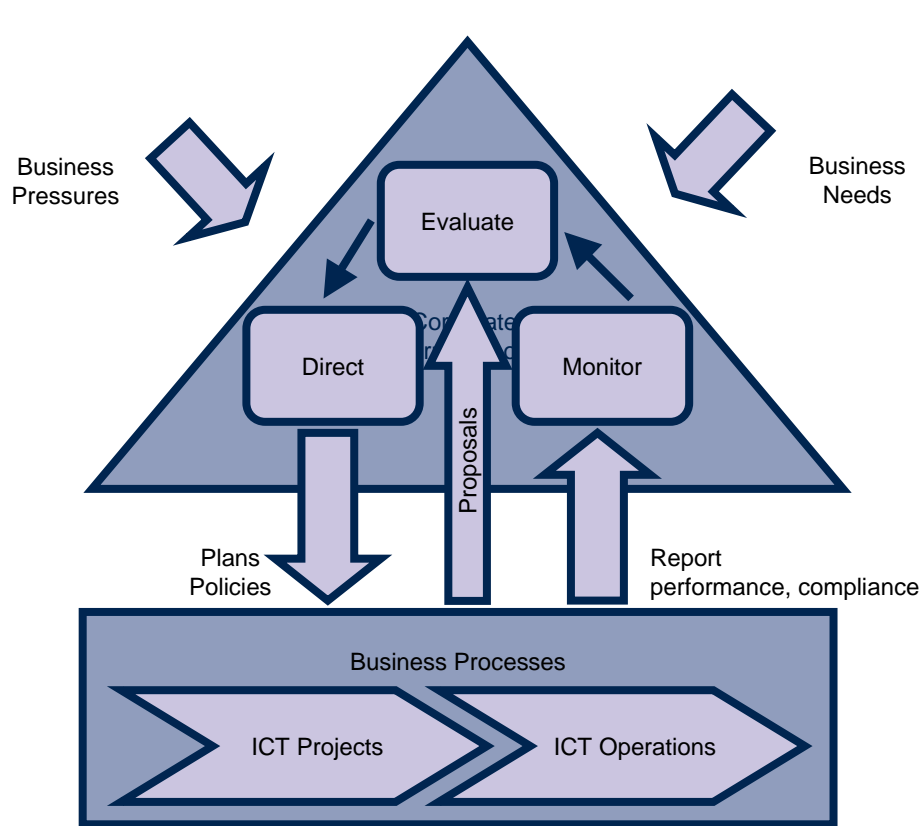
- Management should obtain independent
 - assurance ...
 - certification/accreditation ...
 - evaluation ...

Audit Activities

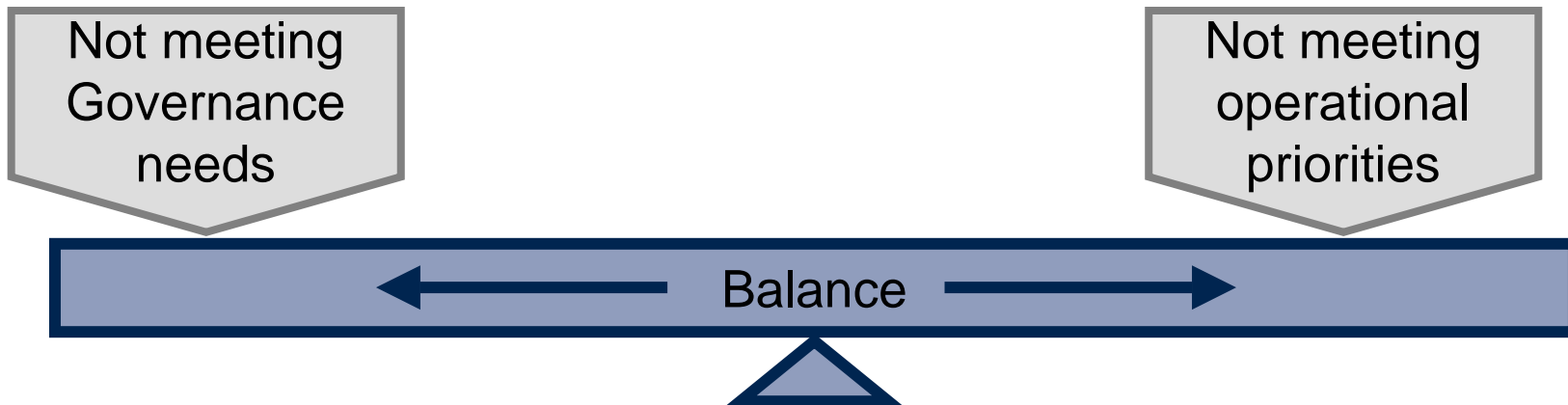
Source: ISO 19011:2005

- Plan the audit programme
 - Set objectives, scope, responsibilities
 - Consider all levels of audit in an audit programme
 - 1st party audits (aka internal audits)
 - 2nd party audits (generally related to supply chain)
 - 3rd party audits (aka external audits)
- Implement the audit programme
 - Evaluate and select auditors
 - Conduct audits
 - Conduct audit activities
 - Report audit results
 - Conduct audit follow-ups
- Monitor the audit programme
- Improve the audit programme

Governance at work – a true audit story



Achieving Balance in Audits



- Don't do them
- Fear of audits - resistance
- Poor skills and method
- Lack of commitment from management and staff
- Focus becomes on meeting the "auditor's requirements"

- Too many, not integrated
 - Internal
 - "Internal" audit branch
 - Using COBIT
 - External
 - ISO20000
 - ISO9000
 - ISO27001
- Can be expensive – time and money

Assessment

Source: ISO 9000:2005

Definition:

A comprehensive and systematic review of the organization's activities and results referenced against a model



itSMF

Assessment Requirements

● ISO/IEC 20000

- The service provider shall perform activities to ... collect and analyse data to baseline and benchmark the service provider's capability ...

● COBIT

- Evaluate the completeness and effectiveness of management's control over IT processes, policies and contracts through a continuing programme of self-assessment.

ISO 20000 Baseline Assessment

(semi-fictitious example)

Process	Hatfield	Woking	Reading	London
Availability & Continuity Management	85	90	88	100
Business Relationship Management	86	100	81	86
Budgeting & Accounting for IT Services	88	83	86	88
Capacity Management	90	92	71	80
Change Management	93	97	80	44
Configuration Management	68	92	75	68
Incident Management	86	65	70	63
Information Security Management	65	68	69	65
Management System	63	68	47	63
New and Changed Services	53	57	61	53
Planning and Implementing	56	61	63	42
Problem Management	51	63	55	51
Release Management	58	37	67	56
Risk Management	57	57	57	43
Service Level Management	74	50	16	45
Service Reporting	50	31	50	50
Supplier Management	28	50	24	32

Legend	Score
Fully conformant	100
Mostly conformant	85 – 99
Non-conformant – moderate effort required	66 – 84
Non-conformant – major effort required	55 – 65
Significantly non-conformant – major concerns	0 – 54

🍊 The management of this organisation thought they had a single management system !!

ITIL Baseline Assessment – a true story

UNIT	← ITIL SERVICE SUPPORT →						← ITIL SERVICE DELIVERY →				
	SERVICE DESK	INCIDENT MGMT.	PROBLEM MGMT.	CONFIG. MGMT.	CHANGE MGMT.	RELEASE MGMT.	SERVICE LEVEL MGMT.	FINANCIAL MGMT.	CAPACITY MGMT.	SERVICE CONTINUITY MGMT.	AVAILABILITY MGMT.
IS Unit 1	1.5	1.5	1	1	2	2.5	1	1	1	0	1
IS Unit 2	1.5	1	0	1	2	1	1	2.5	1	1	1
IS Unit 3	1.5	1.5	1	2	2.5	1.5	2	2.5	1.5	1.5	2
IS Unit 4	2	2	2	1	1	1	1	1	1	1	1
IS Unit 5	2.5	2.5	2.5	1.5	1.5	1.5	2	2	1.5	2	2.5
IS Unit 6	2.5	2.5	2	2	1	1	1	2	2	2	2
IS Unit 7	2	2	2	1	2.5	1	1	2	1	1	2
IS Unit 8	1	2	0	1	2.5	1	1	1	1	1	1
IS Unit 9	1	1	1	1	1	1	1.5	1	1	1	1
IS Unit 10	0	0	1	0	1	1	1	1	0	1	1
IS Unit 11	1	1.5	1.5	0	1	1.5	1	2	1	1	1

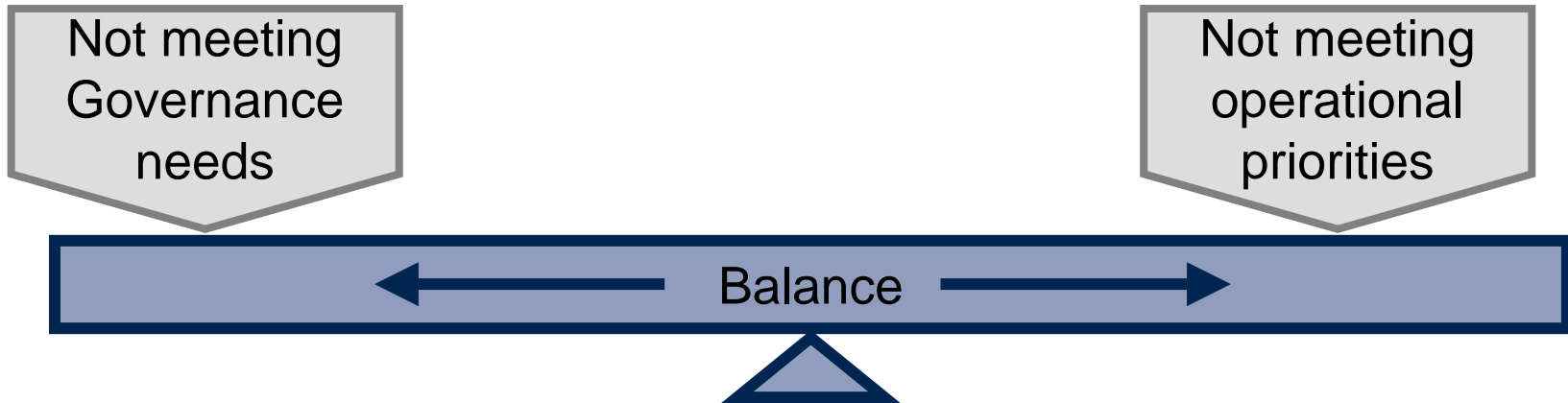
IS SUMMARY SCORES	SERVICE DESK	INCIDENT MGMT.	PROBLEM MGMT.	CONFIG. MGMT.	CHANGE MGMT.	RELEASE MGMT.	SERVICE LEVEL MGMT.	FINANCIAL MGMT.	CAPACITY MGMT.	SERVICE CONTINUITY MGMT.	AVAILABILITY MGMT.
AVERAGE	1.5	1.6	1.3	1.0	1.6	1.3	1.2	1.6	1.1	1.1	1.4
LOWEST	0	0	0	0	1	1	1	1	0	0	1
HIGHEST	2.5	2.5	2.5	2.0	2.5	2.5	2.0	2.5	2.0	2.0	2.5

ITIL Baseline Assessment – a true story

UNIT	← ITIL SERVICE SUPPORT →						← ITIL SERVICE DELIVERY →				
	SERVICE DESK	INCIDENT MGMT.	PROBLEM MGMT.	CONFIG. MGMT.	CHANGE MGMT.	RELEASE MGMT.	SERVICE LEVEL MGMT.	FINANCIAL MGMT.	CAPACITY MGMT.	SERVICE CONTINUITY MGMT.	AVAILABILITY MGMT.
IS Unit 10	0	0	1	0	1	1	1	1	0	1	1

The “worst” assessment
Maturity = 0.6

Achieving Balance in Assessments



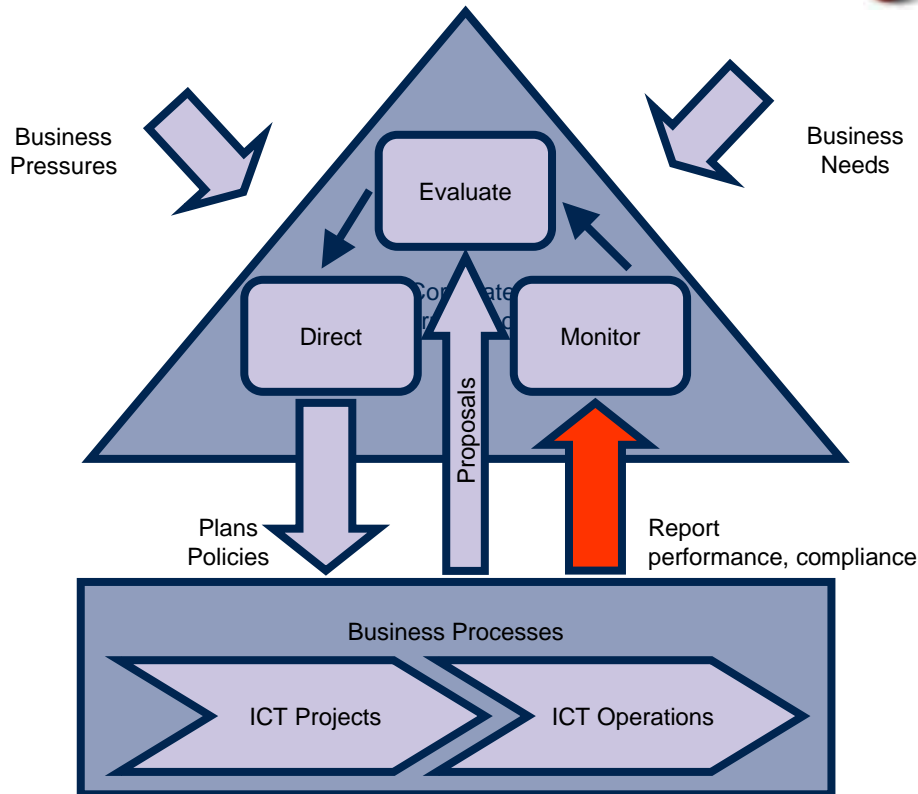
- Not doing any
- Doing it only once
- Poor tools and models
- Recommendations not developed
- Focus on “the score”, rather than improvement
- Too much time spent on complex assessment models
- If benchmarking over time, may become locked in to a method

Summary

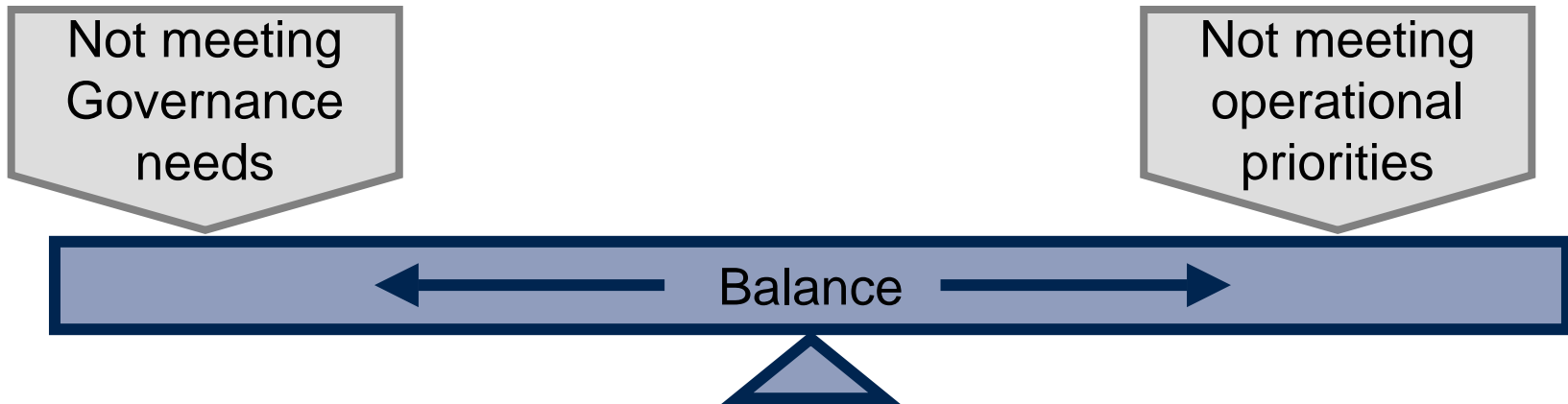
Audits, reviews and assessments

Provide the feedback necessary to allow managers and executives to:

- Monitor performance and progress of IT operations and projects
- Monitor compliance with policies and strategies
- Evaluate the situation
- Issue appropriate directives



Summary



- ... but you need to get the balance right
 - Invest enough in skills, tools, methods
 - Don't over-invest
 - Provide adequate and appropriate feedback
 - Don't overwhelm
 - Through structured accountabilities and responsibilities

Summary

- AS8015 (to be ISO/IEC 29352)
 - Provides principles for ICT Governance

- ITIL, ISO20000 and COBIT (and other frameworks)
 - Provide guidance on how and when to use audit, review and assessment

End of formal presentation

Following slides on AS8015 principles

Any questions?



itSMEF

ICT Governance Principles

Source: AS 8015:2005

- The following slides describe each the six principles:
 - Establish clearly understood responsibilities
 - Plan ICT to best support the organization
 - Acquire ICT validly
 - Ensure that ICT performs well, whenever required
 - Ensure ICT conforms with formal rules
 - Ensure ICT use respects human factors
- and gives examples as to how the principle is supported by
 - ITIL
 - ISO20000 and/or
 - COBIT

Principle 1 - Establish clearly understood responsibilities for ICT

- This principle ensures that individuals and groups within the organization understand and accept their responsibilities for ICT.
- Audits and assessments under ISO20000 will ensure that:
 - All service management roles and responsibilities shall be defined and maintained ...
 - Top management shall ensure that its employees are aware of the relevance and importance of their activities ...

Principle 2 - Plan ICT to best support the organization

- This principle ensures that ICT plans fit the current and ongoing needs of the organization and that the ICT plans support the corporate plans.
- Reviews required under ITIL and ISO20000 will ensure that:
 - A post implementation review comparing actual outcomes against those planned shall be performed ...
 - The SLAs shall be maintained by regular reviews by the parties to ensure that they are up-to-date and remain effective over time.

Principle 3 - Acquire ICT validly

- This principle ensures that ICT acquisitions are made for approved reasons in the approved way; on the basis of appropriate and ongoing analysis. Ensure that there is appropriate balance between costs, risks, long term and short term benefits.
- COBIT controls will ensure that the service provider will:
 - Verify that the process requires the business sponsor to approve and sign off on business functional and technical requirements and feasibility study reports at predetermined key stages. The business sponsor should make the final decision with respect to the choice of solution and acquisition approach.

Principle 4 - Ensure that ICT performs well, whenever required

- This principle ensures that ICT is fit for its purpose in supporting the organization, is kept responsive to changing business requirements, and provides support to the business at all times when required by the business.
- Audits under ISO20000 will ensure that
 - Management shall
 - ... ensure that customer requirements are determined and are met with the aim of improving customer satisfaction ... and
 - conduct reviews of service management, at planned intervals, to ensure continuing suitability, adequacy and effectiveness.

Principle 5 - Ensure ICT conforms with formal rules

- This principle ensures that ICT conforms with all external regulations and complies with all internal policies and practices.
- COBIT says:
 - Identify ... laws, regulations, and other external requirements that must be complied with ...
 - Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.
 - Obtain and report assurance of compliance and adherence to all internal policies derived from ... external legal, regulatory or contractual requirements ...

Principle 6 - Ensure ICT use respects human factors

- This principle ensures that ICT meets the current and evolving needs of all the ‘people in the process’.
- ISO20000 (Part 2) says ...
 - The SLM process should ensure that the service provider remains focused on the customer throughout the planning, implementation, and ongoing management of service delivery.
 - The service provider should be given adequate information to enable them to understand their customer’s business drivers and requirements.

Thank you for attending this itSMF Seminar

IT Governance:

The role of Audit, Review and Assessment

Ralph Gray
Principal Consultant
www.FoxIT.net



itSMF