



"IT Governance Helping Business Survival"




Steve Crutchley
 CEO & Founder
 Consult2Comply
www.consult2comply.com



Introduction – Steve Crutchley

- Founder & CEO of Consult2Comply
- 39 Years IT & Business Experience
- 22 Years GRC - Risk/Compliance Experience
- Recognized International Consultant
- ISO 27001, ISO 20000, BS 25999 Qualified Lead Auditor – IRCA approved
- Content expert – Regulations, Standards & Best Practices - worldwide
- ISO 27001, ISO 20000, BS 25999 Trainer and ACP
- Approved CobIT trainer - ISACA
- Experience in Government, Finance, Utilities, Pharmaceutical, Transportation (Airports) and Insurance
- Successfully ran businesses – ex CEO of a public company
- Developed Assessment Software to support the Business & Security/Risk needs
- Product architect for C2C Products
- Numerous Articles, Speaking and TV appearances related to security and security related solutions



Seminar Content?

CONSULT
COMPLY


IT Governance introduction – the why's and wherefores
Issues that cause IT Governance concerns – setting the scene
Governance Standards and Frameworks
IT Governance for Business Survival

Interactive and Questions

What is IT Governance?

CONSULT
COMPLY

- **Information Technology Governance**, IT Governance is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management.
- The rising interest in IT Governance is partly due to compliance initiatives (e.g. Sarbanes-Oxley (USA) and Basel II (Europe)), as well as the acknowledgment that IT projects can easily get out of control and profoundly affect the performance of an organization.



4

Why target IT?

CONSULT
COMPLY

In recent years, surveys have consistently revealed that 20 to 70 percent of large-scale investments in IT-enabled change are wasted, challenged or fail to bring a return to the enterprise (figure In fact, one survey on measuring costs and value found that, in many enterprises, less than 8 percent of the IT budget is actually spent on initiatives that create value for the enterprise.

A 2002 Gartner survey found that 20 percent of all expenditures on IT is wasted—a finding that represents, on a global basis, an annual destruction of value totaling about US \$600 billion.

A 2004 IBM survey of Fortune 1000 CIOs found that, on average, CIOs believe that 40 percent of all IT spending brought no return to their organizations.

A 2006 study conducted by The Standish Group found that only 35 percent of all IT projects succeeded while the remainder (65 percent) were either challenged or failed.

Reference Val IT Framework 2.0

Headlines around the world corroborate these findings:

CONSULT
COMPLY

Nike reportedly lost more than US \$200 million through difficulties experienced in implementing its supply chain software. Failures in IT-enabled logistics systems at MFI and Sainsbury in the UK led to multimillion-pound write-offs, profit warnings and share price erosion.

Tokyo Gas reported a US \$46.6 million special loss due to cancellation of a large customer relationship management (CRM) project. In the public sector, the UK Department for Work and Pensions apparently 'squandered' more than £2 billion by abandoning three major projects.

Reference Val IT Framework 2.0

Why is IT Governance important?

CONSULT
COMPLY

IT are in competition for budget – Business is beating IT to and for budget

IT needs to become a business focused discipline

IT is viewed by senior management as 'Fire Fighters' and not 'Planners or implementers'

IT is viewed as a monetary drain on business

IT needs to compete effectively at the 'C' level

Business does not perceive IT as value for money



7

7

IT Governance Discipline

CONSULT
COMPLY

The discipline of information technology governance derives from corporate governance and deals primarily with the connection between business focus and IT management of an organization.

It highlights the importance of IT related matters and states that strategic IT decisions should be owned by the corporate board, rather than by the CISO/CSO or other IT managers.



8

8

History of IT Governance Standards and Frameworks

CONSULT
COMPLY

Australian Standards – AS 8015:2005 – Corporate Governance of information and communications technology

ITGi – based on CobIT
Val IT Framework 1.0 – launched 2006
Val IT Framework 2.0 – launched 2008

ISO/IEC 38500:2008 Corporate governance of information technology – based on AS 8015:2005



Columbus

9

9

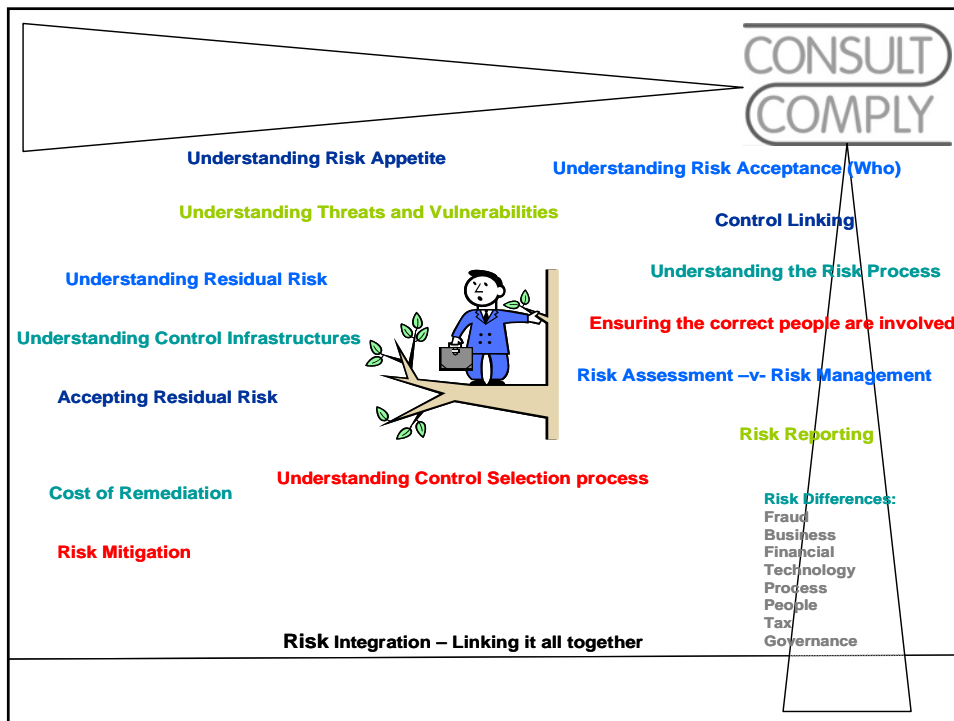
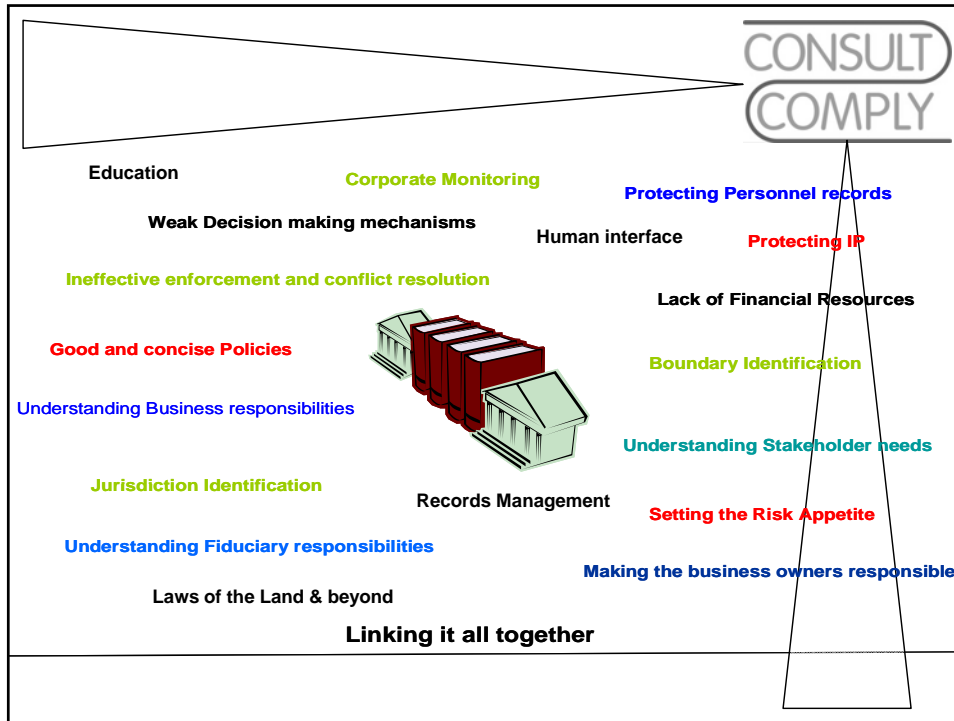
Setting the Scene


CONSULT
COMPLY




10


10






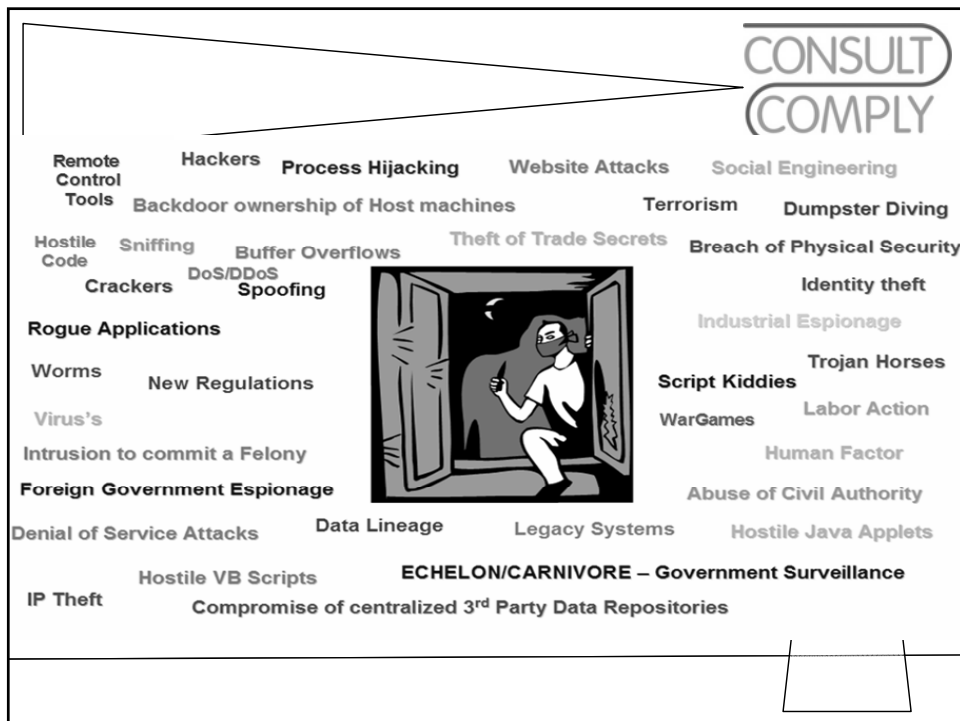
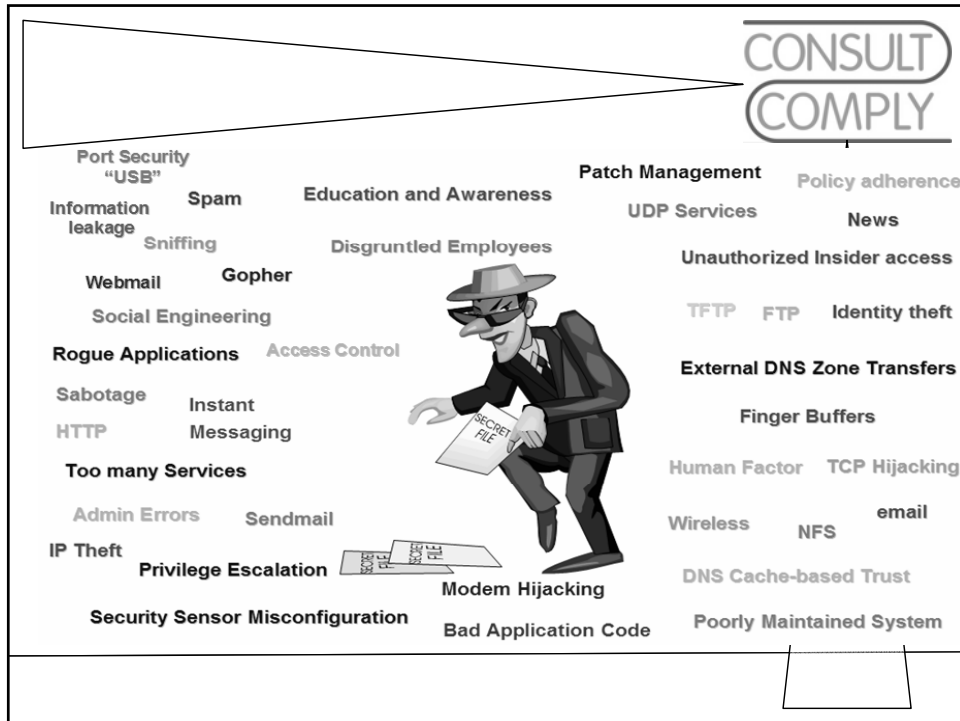
<p>PIA JSOX PCI</p> <p>FACTA</p> <p>UPA</p> <p>SB-1386 California</p> <p>Computer Security Act 1987</p> <p>Freedom of Information Act</p> <p>Digital Millennium Copyright Act 1998</p> <p>Computer Fraud and Abuse Act 1986</p> <p>Children's Online Privacy Protection Act of 1998 (COPPA)</p> <p>Sarbanes Oxley</p> <p>Foreign Corrupt Practices Act 1977</p> <p>NY Reg. 173</p>	<p>The European Union Directive on Data Protection</p> <p>Electronic Communications Privacy Act 1986</p> <p>ISO 17799</p> <p>EU Privacy Directive</p> <p>UK Data Protection Act</p> <p>21 CFR part 11</p> <p>FFIEC</p> <p>Computer Security Act 1987</p> <p>Freedom of Information Act</p> <p>Digital Millennium Copyright Act 1998</p> <p>Computer Fraud and Abuse Act 1986</p> <p>Children's Online Privacy Protection Act of 1998 (COPPA)</p> <p>Sarbanes Oxley</p> <p>Foreign Corrupt Practices Act 1977</p> <p>The Telecommunications (Data Protection and Privacy) Regulations 1999</p>		<p>Smith Report</p> <p>National Infrastructure Protection Act 1996</p> <p>NIST 800 Series Standards</p> <p>HIPAA</p> <p>EU Regulatory Framework for Electronic Communications</p> <p>Patriot Act II</p> <p>Anti-terrorism, Crime and Security Act 2001</p> <p>Homeland Security Act</p> <p>NIST</p> <p>GLBA</p> <p>Government Information Security Reform Act</p> <p>FERPA</p> <p>Foreign Corrupt Practices Act 1977</p> <p>NERC</p>	<p>BITS</p> <p>FDA</p> <p>ISO 27001</p> <p>Basel II</p> <p>Bill C-6</p> <p>PIPEDA</p> <p>Tumbull Report</p> <p>Higgs Report</p> <p>ISO 15489</p> <p>GISRA</p> <p>FISMA</p> <p>BS 7799</p> <p>DOD 5015.2</p>
--	---	---	--	---


13



<p>Intrusion Protection</p> <p>Mobile Computing</p> <p>Data Exchange</p> <p>Domain Security</p> <p>Webmail</p> <p>Platform Security</p> <p>Risk Analysis</p> <p>Secure Email</p> <p>Corporate Governance</p> <p>Event Monitoring</p> <p>PKI Infrastructures</p> <p>Security Policies and Procedures</p>	<p>Data Classification</p> <p>Security in Enterprise Architectures</p> <p>HR Policy</p> <p>Event Correlation</p> <p>Legal/Regulatory</p> <p>Risk Assessments</p> <p>Intrusion Detection</p> <p>The Human Factor</p> <p>Encryption</p> <p>Security Frameworks</p> <p>Users</p> <p>Vulnerabilities</p> <p>Privacy</p>		<p>Security Management</p> <p>Network Forensics</p> <p>Security Measurement</p> <p>Disaster Recovery</p> <p>Privilege Management</p> <p>Training</p> <p>Control Standards</p> <p>Content Management</p> <p>Firewalls</p> <p>Asset Classification</p> <p>Security Integration</p> <p>Security Baselines</p> <p>Data Lineage</p>	<p>Security Health Checks</p> <p>Portal Security</p> <p>Security Infrastructure</p> <p>Legacy Systems</p> <p>Collaboration/Partners</p> <p>Malware</p> <p>Computer Forensics</p> <p>Wifi</p> <p>Security Awareness</p> <p>Virus</p> <p>PKI Readiness Reviews</p> <p>Consultants</p> <p>Incident Management</p> <p>Mainframe Security</p>
---	---	---	--	--

Business Continuity Planning





Cable Security

Express Kidnapping

Snooping

Access Control

Booms

Contracts

Building Security

Escorting

Entry/Exit Points

Raised Flooring

Fireproof Safes

Physical Layouts

Building Management

Perimeter Security

Surveillance

Wireless

Elevators

Parking Lots

CCTV

Alarms

Reception

Evacuation


Health & Safety

Landlords

Proximity Security

First Aid

Eavesdropping



Disposal Services

Business Continuity

Physical Protection

Office Erection

Emergency Exits

Fire-resistant and tamper-resistant storage facilities

Anti-theft measures

Trash collection

Maintenance

Protection (People)

Utilities – Power and Water

Communications

Smoking/Smoke Areas

Bugs & Probes

Keycards

Transportation


Counter Surveillance

Turnstiles

Plants

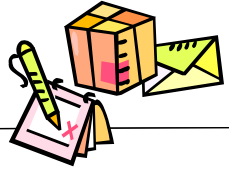
Disaster Recovery

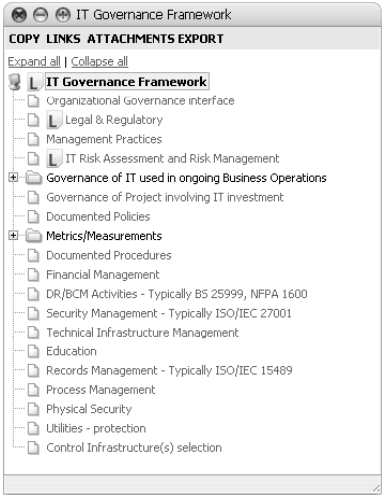
Anti-vandal measures



What should Information Technology Governance Deliver?

Executives should focus on Information Technology Governance, which when properly implemented should provide the following:





```

IT Governance Framework
├── Organizational governance interface
├── Legal & Regulatory
├── Management Practices
├── IT Risk Assessment and Risk Management
├── Governance of IT used in ongoing Business Operations
│   ├── Governance of Project involving IT investment
│   └── Documented Policies
├── Metrics/Measurements
│   ├── Documented Procedures
│   ├── Financial Management
│   ├── DR/BCM Activities - Typically BS 25999, NFPA 1600
│   ├── Security Management - Typically ISO/IEC 27001
│   ├── Technical Infrastructure Management
│   ├── Education
│   └── Records Management - Typically ISO/IEC 15489
├── Process Management
├── Physical Security
├── Utilities - protection
└── Control Infrastructure(s) selection
    
```

18

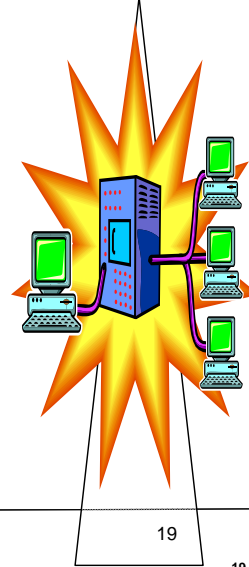
What are the IT Governance Characteristics?

CONSULT
COMPLY

A general theme of IT Governance discussions is that the IT capability can no longer be something the business doesn't understand and that IT must also understand the business and its needs.

Handling of IT has always been an issue for board-level executives because of the technical nature of IT, therefore, key decisions were left to IT professionals. IT Governance implies a system in which all stakeholders, including the board, internal customers and related areas such as finance, have the necessary input into the decision making process.

This will prevent a single stakeholder, typically IT, being blamed for poor decisions. It also prevents users from later complaining that the system does not behave or perform as expected – very important for IT



19

19

What are the IT Governance Characteristics (2)?

CONSULT
COMPLY

Most importantly - The board needs to understand the overall architecture of its company's IT applications portfolio ... The board must ensure that management knows what information resources are out there, what condition they are in, and what role they play in generating revenue...



20

20

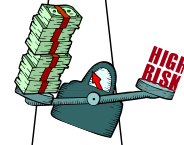
IT Governance Goals

CONSULT
COMPLY

The primary goals for Information Technology Governance are:

- (1) assure that the investments in IT generate business value
- (2) mitigate the risks that are associated with IT.

This can be done by implementing an organizational structure with well-defined roles for the responsibility for information, business processes, applications, infrastructure that's well communicated across the organization.

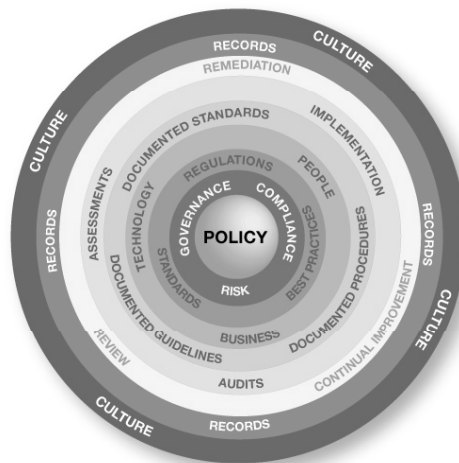


21

21

C2C's GRC Model view – supporting IT Governance

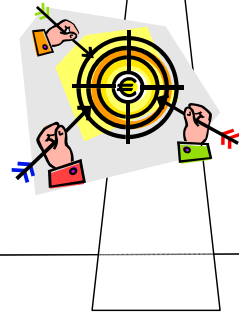
CONSULT
COMPLY



Who is this aimed at?

Senior Management
CIOs
IT Managers
It staff
And
IT centric organizations

CONSULT
COMPLY



What are the
Frameworks or
Standards?

CONSULT
COMPLY

CONSULT
COMPLY

Overview of ISO/IEC 38500 and Val IT 2.0

What is the objective of IT Governance?


CONSULT
COMPLY

Strategic alignment of *IT* with the *Business* with emphasis on Business Governance

Conformance of the organization to Security, Privacy - Trade Practices, IPR, Records Management, Legislation and Regulations (Laws of the Land) and alignment to Best Practices to reduce and streamline costs improve revenues.

CONSULT
COMPLY

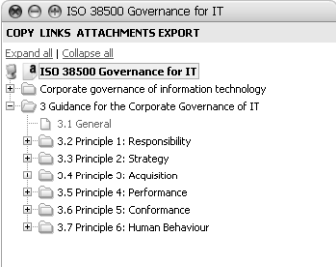

ISO/IEC
38500:2008



CONSULT
COMPLY

What is a framework?

A **framework** is a basic conceptual structure used to solve or address complex issues – something like ISO/IEC 38500 – Governance for IT

But it should have processes that are effective.

ISO/IEC 38500 Structure

CONSULT
COMPLY

Principle 1: Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.

Principle 2: Strategy

The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.

Principle 3: Acquisition

IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

ISO/IEC 38500 Structure

CONSULT
COMPLY

Principle 4: Performance

IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

Principle 5: Conformance

IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Principle 6: Human Behavior

IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

ISO/IEC 38500 Responsibility

3.2 Principle 1: Responsibility – extracts

Evaluate

Directors should evaluate the options for assigning responsibilities in respect of the organization's current and future use of IT.

Direct

Directors should direct that plans be carried out according to the assigned IT responsibilities.

Monitor

Directors should monitor that appropriate IT governance mechanisms are established.

ISO/IEC 38500 Strategy

3.3 Principle 2: Strategy - extracts

Evaluate

Directors should evaluate developments in IT and business processes to ensure that IT will provide support for future business needs.

Direct

Directors should direct the preparation and use of plans and policies that ensure the organization does benefit from developments in IT.

Monitor

Directors should monitor the progress of approved IT proposals to ensure that they are achieving objectives in required timeframes using allocated resources.

ISO/IEC 38500 Acquisition

CONSULT
COMPLY

3.4 Principle 3: Acquisition - extracts

Evaluate

Directors should evaluate options for providing IT to realize approved proposals, balancing risks and value for money of proposed investments.

Direct

Directors should direct that IT assets (systems and infrastructure) be acquired in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided.

Monitor

Directors should monitor IT investments to ensure that they provide the required capabilities.

ISO/IEC 38500 Performance

CONSULT
COMPLY

3.5 Principle 4: Performance - extracts

Evaluate

Directors should evaluate the means proposed by the managers to ensure that IT will support business processes with the required capability and capacity. These proposals should address the continuing normal operation of the business and the treatment of risk associated with the use of IT.

Direct

Directors should ensure allocation of sufficient resources so that IT meets the needs of the organization, according to the agreed priorities and budgetary constraints.

Monitor

Directors should monitor the extent to which IT does support the business.

ISO/IEC 38500 Conformance

CONSULT
COMPLY

3.6 Principle 5: Conformance - extracts

Evaluate
Directors should regularly evaluate the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.

Direct
Directors should direct those responsible to establish regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.

Monitor
Directors should monitor IT compliance and conformance through appropriate reporting and audit practices, ensuring that reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the business.

ISO/IEC 38500 Conformance

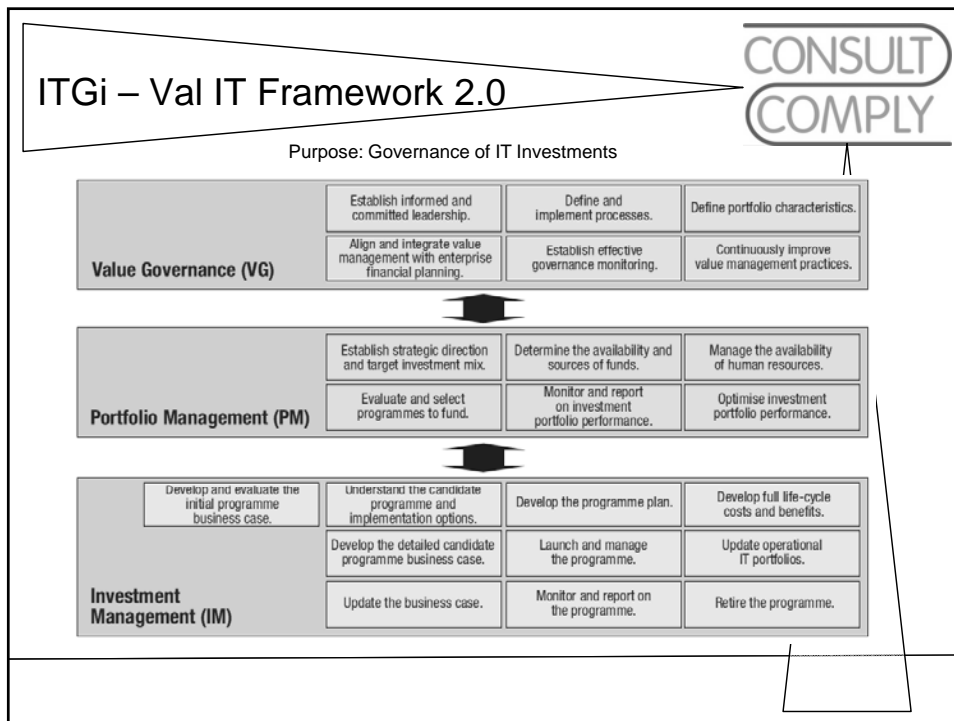
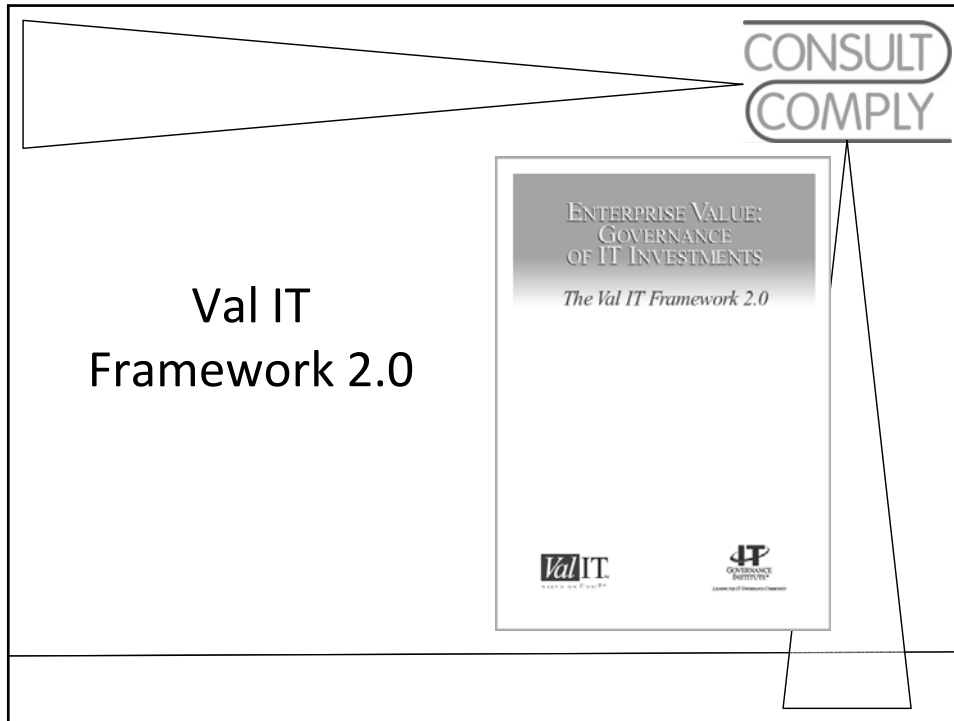
CONSULT
COMPLY

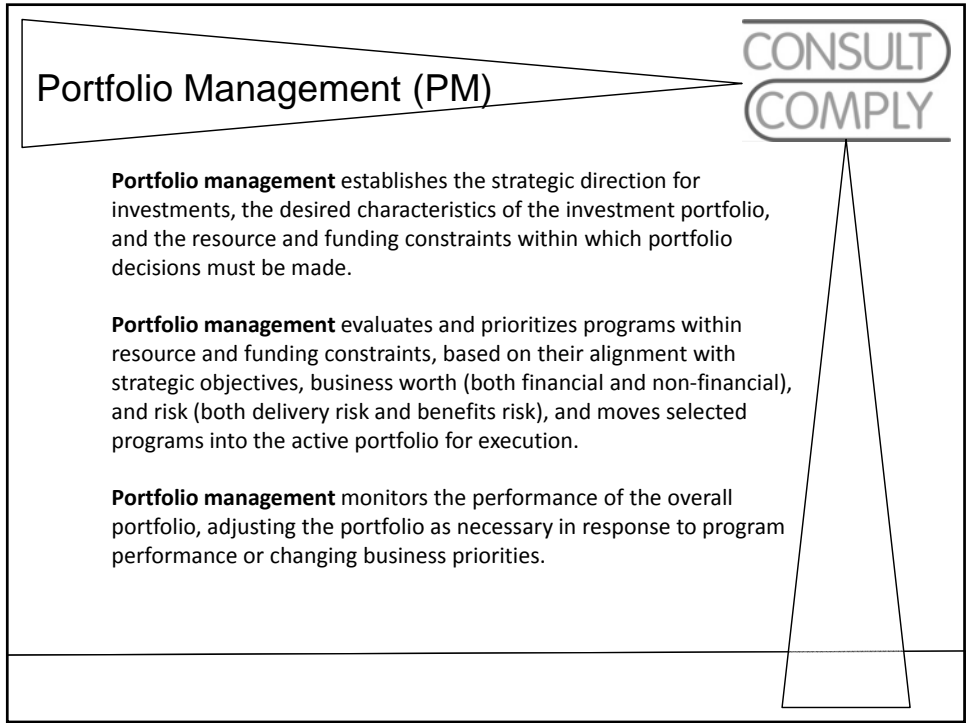
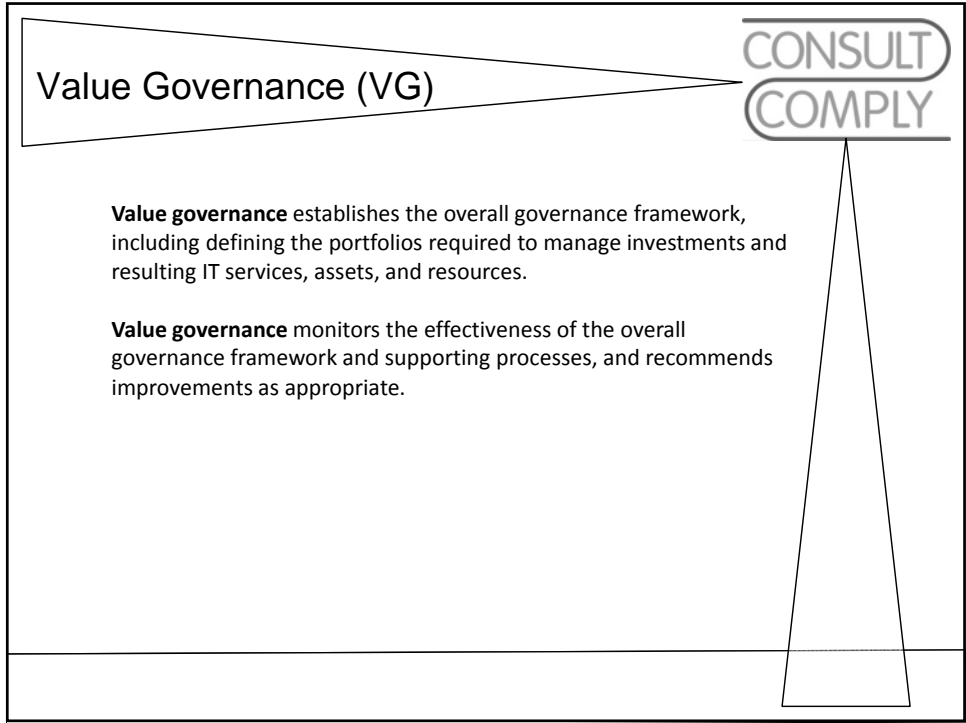
3.7 Principle 6: Human Behavior - extracts

Evaluate
Directors should evaluate IT activities to ensure that human behaviors are identified and appropriately considered.

Direct
Directors should direct that IT activities are consistent with identified human behavior.

Monitor
Directors should monitor IT activities to ensure that identified human behaviors remain relevant and that proper attention is given to them.





Investment Management (IM)

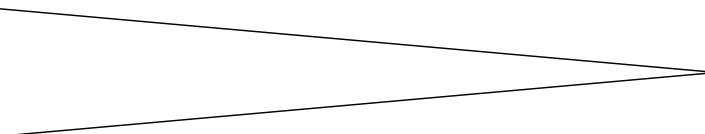
CONSULT
COMPLY

Investment management defines potential programs based on business requirements, determines whether they are worthy of further consideration, and develops and passes business cases for candidate investment programs to portfolio management for evaluation.

Investment management launches and manages the execution of active programs, and reports on performance to portfolio management. Investment management moves resulting IT services, assets and resources to the appropriate operational IT portfolio(s) and continues to monitor their contribution to business value.

Investment management retires programs when there is agreement that desired business value has been realized, or when retirement is deemed appropriate for any other reason.

Investment management monitors the performance of IT services, assets and resources to determine whether additional investments are required to maintain, enhance, or retire the service, asset, or resource to sustain or increase their contribution to business value.



CONSULT
COMPLY



IT Governance for Business Survival



Modeling IT Governance

CONSULT
COMPLY

Keys to success

1. Don't work in silos
2. Allocate responsibilities
3. Make sure people understand the plan and model
4. The model must be mapped across the organization
5. It must include all aspects and requirements – Policies, procedures, process maps
6. Create relationships across multiple control frameworks



Good IT Governance Principles

CONSULT
COMPLY

Commitment
Governance Policy
Roles and Responsibilities
Identification of Business Governance issues
Obligations to stakeholders
Organizational Policies
Operating procedures
Dealing with breaches
Record keeping
Internal reporting
Maintenance
Education and training
Communication and visibility
Monitoring and assessment
Review
Report back

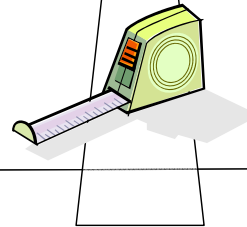


How do you measure IT Governance?

CONSULT
COMPLY

- Must have decided on the standard or framework
- Must understand your IT Governance requirements
- Must understand your business objectives
- Must understand the processes you are supporting
- Must set a baseline to work from – includes your responsibilities
- Must be able to **Monitor**
- Must have a measurement method – **Measure**
- Must be able to **Manage**

- Must be able to Self Assess



What can help you?

CONSULT
COMPLY

- Understand applicable Compliance landscape (GRC)
- ISO 20000/ITIL – Service management v.3
- ISO 27001 – Information Security Management System
- ISO/IEC 38500 It Governance Standard
- COBIT/ITGI – Val IT 2.0
- CMM – Maturity Modeling
- Six Sigma - Quality
- Balanced Scorecard - Metrics (Monitor, Measure and Manage)
- Understand your Business need and respond accordingly

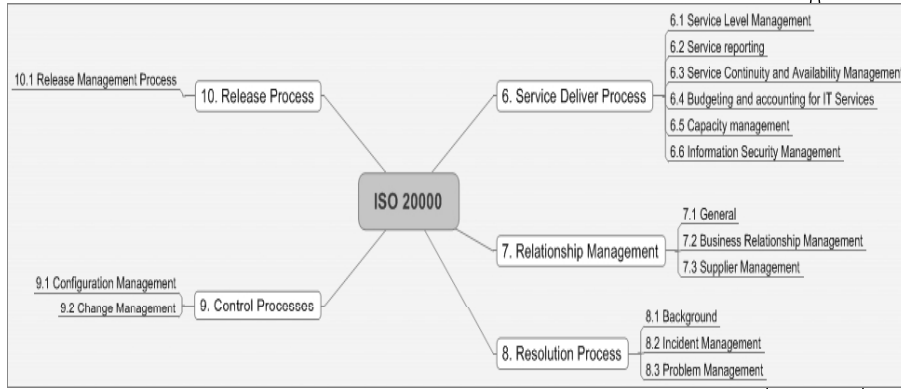


46

46

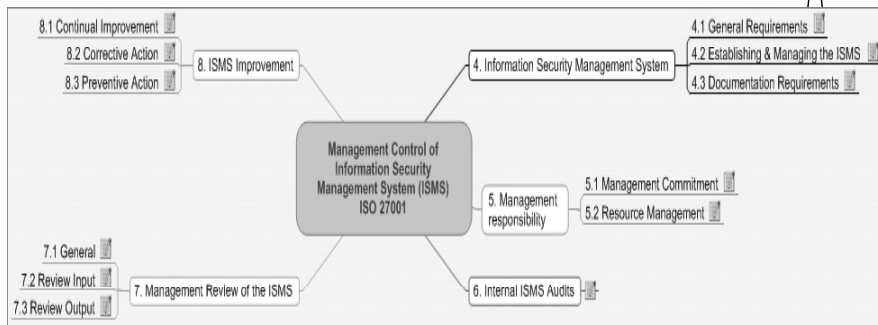
ISO 20000 IT service management structure?

CONSULT
COMPLY



ISO 27001 Information Security management – management structure?

CONSULT
COMPLY

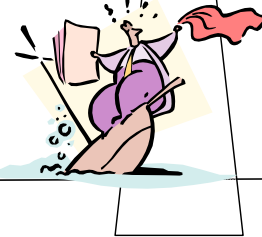


Implementation issues

CONSULT
COMPLY

Management Commitment
 IT understanding from a management perspective
 IT's understanding of business processes
 Effective and appropriate training
 People - hidden agendas
 Getting budget
 Proving Business value for IT Governance implementation

Getting it RIGHT!



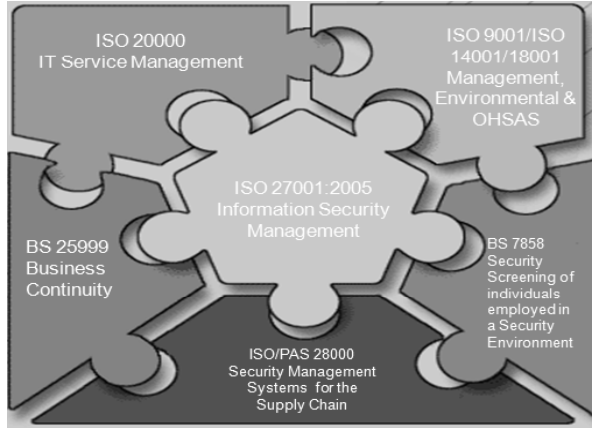
Example IT Governance Structure

CONSULT
COMPLY

The screenshot displays a complex software interface for IT Governance. It features a 'Control Panel' on the left and several main content areas, each with a 'COPY LINKS ATTACHMENTS EXPORT' button. The main areas are:

- Organizational Governance Framework:** Includes Corporate Monitoring, Protecting Intellectual Property (IP), Complete and Concise Policies, Understanding Fiduciary responsibilities, Records Protection, Boundary Identification, Financial resourcing, Stakeholder needs, Accountability and Responsibility, Risk Appetite, and Decision Making Process.
- IT Governance Framework:** Includes Organizational Governance Interface, Legal & Regulatory, Management Practices, IT Risk Assessment and Risk Management, Governance of IT used in ongoing Business Operations, Governance of Project involving IT investment, Documented Policies, Metrics/Measurements, Documented Procedures, Financial Management, DR/BCM Activites - Typically BS 25999, NFPA 1600, and Security Management - Typically ISO/IEC 27001.
- Standards and Best Practices:** Includes ISO/IEC 38500 Corporate Governance for IT, DR/BOY, Security Management, Service Management, and Val IT 2.0.
- IT Projects Management:** Includes IT Projects Management.
- Technical Infrastructure:** Includes Technical Infrastructure Management.
- Legal & Regulatory:** Includes Sarbanes Oxley (SOX), SB 1386 California Privacy Law, HIPAA, Gramm Leach Bliley (GLBA), PCI, Safe Harbor, and Clinger Cohen.
- Polices:** Includes Security Management, Personal Security, Asset Protection, Physical Security, Operations, Access Control, Systems Development, Incident Management, DR/Business Continuity, Compliance, and Records Management.
- Procedure:** Includes Security Management, Personal Security, Asset Protection, Physical Security, Operations, Access Control, Systems Development, Incident Management, DR/Business Continuity, Compliance, and Records Management.

Harmonization with existing
BS/ISO standards & guidelines



ISO 27799 Health Informatics - Security Management in Health using ISO 17799

ISO 19077 Software Asset Management

ISO 27005 Information Security Risk Management

ISO 15489 Effective Records Management

ISO 21188 Public Key Infrastructure for Financial Services

ISO 18044 Incident Management

BS 8470 Secure Disposal of confidential material

BS 8549 Security Consultancy Code of Practice

ISO 15288 System & Software Engineering - System lifecycle processes

Questions?



CONSULT
COMPLY

Thanks

Presenter Steve Crutchley
Email: scrutchley@consult2comply.com
Telephone: 571 332 8204/703 871 3950

53