

CONSULT
COMPLY

Information Technology Governance



Steve Crutchley
CEO - Consult2Comply
www.consult2comply.com

SMART
securityservices

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.



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.



CONSULT COMPLY

Governance Issues

Corporate Monitoring

Weak Decision making mechanisms

Ineffective enforcement and conflict resolution

Good and concise Policies

Understanding Business responsibilities

Jurisdiction Identification

Understanding Fiduciary responsibilities

Linking it all together

Protecting Personnel records

Protecting IP

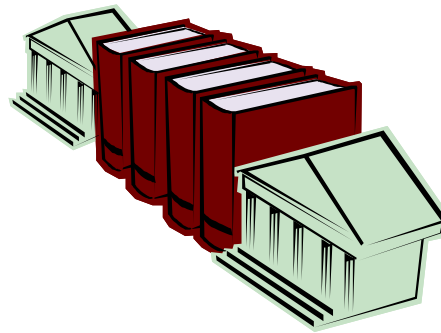
Lack of Financial Resources

Boundary Identification

Understanding Stakeholder needs

Setting the Risk Appetite

Making the business owners responsible



Legislative Issues

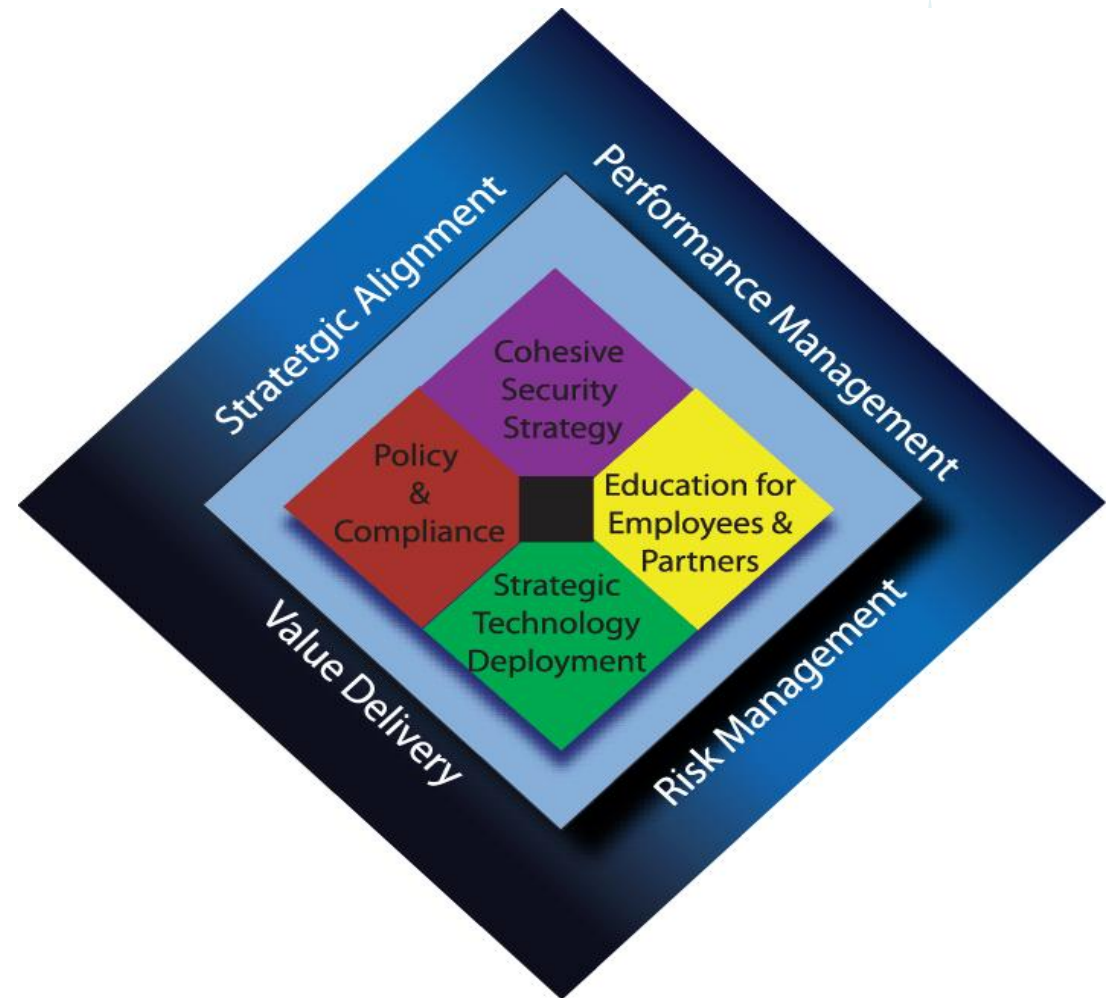
PIA **JSOX** **The European Union Directive on Data Protection** **Smith Report** **BITS** **FDA**
PCI
FACTA **Electronic Communications Privacy Act 1986** **National Infrastructure Protection Act 1996**
ISO 17799 **FFIEC** **NIST 800 Series Standards** **ISO 27001**
EU Privacy Directive
UPA **UK Data Protection Act** **HIPAA** **Basel II** **Bill C-6** **PIPEDA**
SB-1386 California **21 CFR part 11** **EU Regulatory Framework for Electronic Communications**
Computer Security Act 1987 **Patriot Act II** **Turnbull Report**
Freedom of Information Act **Anti-terrorism, Crime and Security Act 2001** **Higgs Report**
Digital Millennium Copyright Act 1998 **Homeland Security Act** **ISO 15489**
Computer Fraud and Abuse Act 1986 **NIST** **OMB-123** **GISRA**
Children's Online Privacy Protection Act of 1998 (COPPA) **Government Information Security Reform Act** **GLBA** **OMB-130** **FISMA**
Sarbanes Oxley **OECD - Corporate Guidelines Governance** **FERPA** **FERC** **BS 7799**
Foreign Corrupt Practices Act 1977 **OECD Guidelines for the Security of Information Systems & Networks**
NY Reg. 173 **The Telecommunications (Data Protection and Privacy) Regulations 1999** **NERC** **DOD 5015.2**



What should Information Technology Governance Deliver?

CONSULT
COMPLY

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



Risk Issues

CONSULT
COMPLY

Understanding Risk Appetite

Understanding Risk Acceptance (Who)

Understanding Threats and Vulnerabilities

Control Linking

Understanding Residual Risk

Understanding the Risk Process

Understanding Control Infrastructures

Ensuring the correct people are involved

Accepting Residual Risk

Risk Assessment –v- Risk Management



Risk Reporting

Cost of Remediation

Understanding Control Selection process

Risk Mitigation

Risk Differences:

- Fraud
- Business
- Financial
- Technology
- Process
- People
- Tax
- Governance

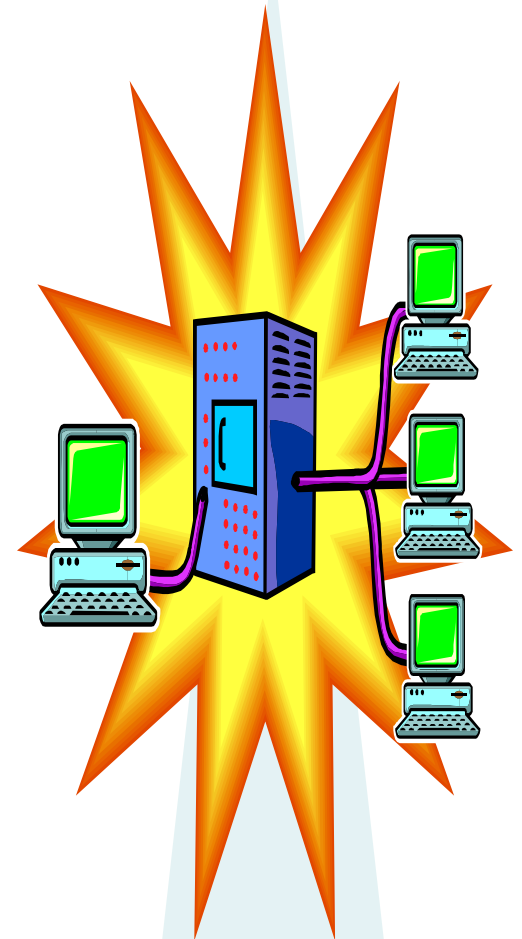
Risk Integration – Linking it all together

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**



What are the IT Governance Characteristics (2)?

***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...*



Security Issues

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



External Threats

- Remote Control Tools
- Hackers
- Process Hijacking
- Website Attacks
- Social Engineering
- Backdoor ownership of Host machines
- Terrorism
- Dumpster Diving
- Hostile Code
- Sniffing
- Buffer Overflows
- Theft of Trade Secrets
- Breach of Physical Security
- Crackers
- DoS/DDoS
- Spoofing
- Identity theft
- Rogue Applications
- Industrial Espionage
- Worms
- New Regulations
- Trojan Horses
- Script Kiddies
- WarGames
- Labor Action
- Virus's
- Intrusion to commit a Felony
- Human Factor
- Foreign Government Espionage
- Abuse of Civil Authority
- Denial of Service Attacks
- Data Lineage
- Legacy Systems
- Hostile Java Applets
- Hostile VB Scripts
- ECHELON/CARNIVORE – Government Surveillance
- IP Theft
- Compromise of centralized 3rd Party Data Repositories



Internal Threats

Port Security "USB" Patch Management Policy adherence
Information leakage Spam Education and Awareness UDP Services News
Sniffing Disgruntled Employees Unauthorized Insider access
Webmail Gopher TFTP FTP Identity theft
Social Engineering Rogue Applications Access Control External DNS Zone Transfers
Sabotage Instant Messaging Finger Buffers
HTTP Too many Services Human Factor TCP Hijacking
Admin Errors Sendmail Wireless NFS email
IP Theft Privilege Escalation Modem Hijacking DNS Cache-based Trust
Security Sensor Misconfiguration Bad Application Code Poorly Maintained System



Physical Security

- 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
- Biometrics
- Office Erection
- Emergency Exits
- Disposal Services
- Business Continuity
- Physical Protection
- Chauffeurs/Drivers
- Special Projects
- Utilities – Power and Water
- Patrols
- Keying
- Emergency Services
- Cleaning Staff
- Firearms
- Clear Desk
- Entry/Exit Controls
- Anti-theft measures
- Trash collection
- Maintenance
- Protection (People)
- Smoking/Smoke Areas
- Bugs & Probes
- Transportation
- Counter Surveillance
- Tumstiles
- Plants
- Disaster Recovery
- Anti-vandal measures
- Guarding
- Keycards



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 of information, business processes, applications, infrastructure, etc.



Disciplines to support IT Governance



What can help you?



- Understand applicable Compliance landscape
- ISO 20000/ITIL – Service management
- ISO 27001 – security management
- COBIT/ITGI
- CMM - Maturity
- Six Sigma - Quality
- Balanced Scorecard - Metrics (Monitor, Measure and Manage)
- Understand Business need and respond accordingly

Example IT Governance Structure

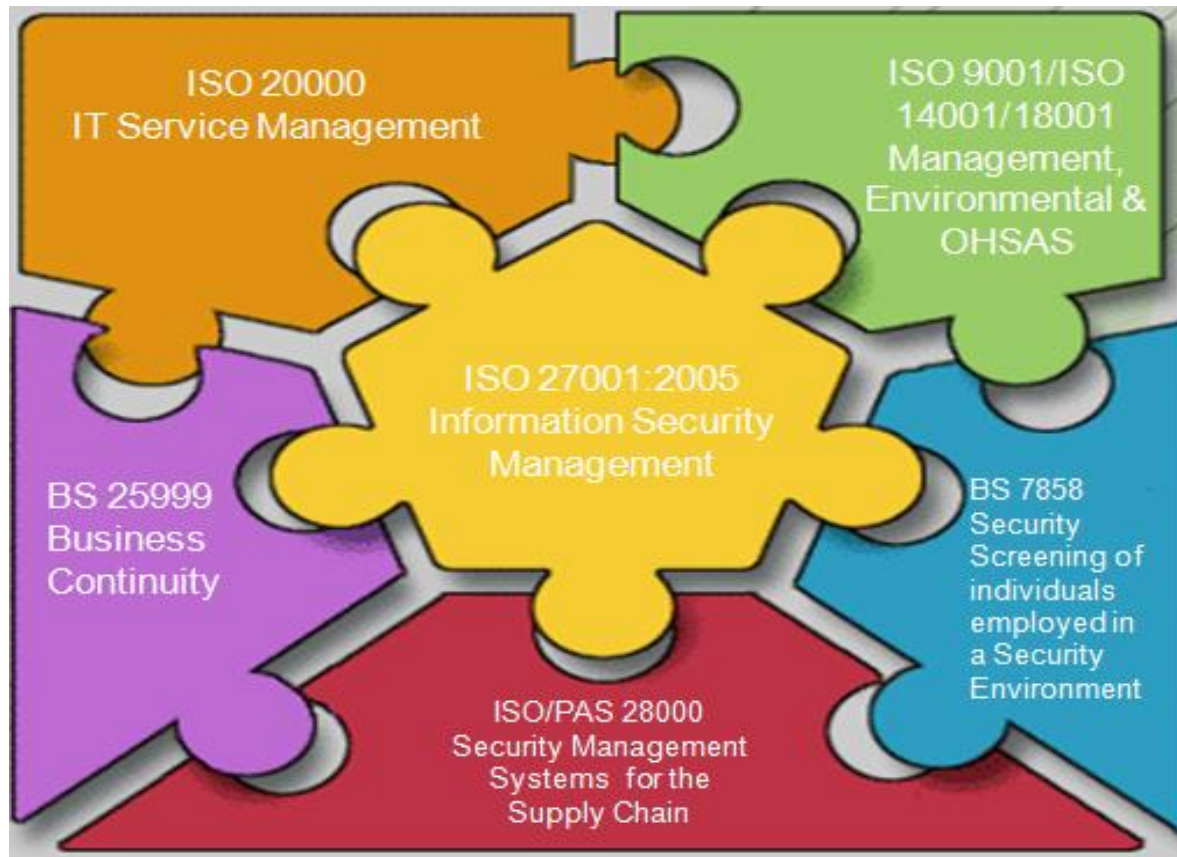


steve, workspace:c2c - IT Governance Framework[user] | logout

The screenshot displays a web-based interface for IT Governance Framework management. On the left is a 'Control Panel' sidebar with sections for TREES, REPORTS, WORKSPACE, ADMIN, and SEARCH TREES. The main area contains a grid of control panels, each representing a different standard or framework. Each panel has a 'PROMOTE LINKS ATTACHMENTS' header and a tree view of its components. The visible panels include:

- ISO 27001 Controls:** A.5 Security Policy, A.6 Organization of Information Security, A.7 Asset Management, A.8 Human Resources Security, A.9 Physical and Environmental Security, A.10 Communications and Operations, A.10.1 Operational Procedures and Plans, A.10.2 Third Party Service Delivery, A.10.3 System Planning and Acceptance, A.10.3.1 Capacity Management, A.10.3.2 System Acceptance, A.10.4 Protection against Malicious Insiders.
- COBIT v4.1:** Plan and Organize, Acquire and Implement, Deliver and Support, DS1 Define and Manage Service Level Agreements, DS2 Manage Third-party Services, DS3 Manage Performance and Capacity, DS3.1 Performance and Capacity, DS3.2 Current Performance and Capacity, DS3.3 Future Performance and Capacity, DS3.4 IT Resources Availability, DS3.5 Monitoring and Reporting, DS4 Ensure Continuous Service.
- NIST Controls Catalog 800-53:** 1. Access Control - AC, AC-1: Access Control Policy and Procedures, AC-2: Account Management, AC-3: Access Enforcement, AC-4: Information Flow Enforcement, AC-5: Separation of Duties, AC-6: Least Privilege, AC-7: Unsuccessful Login Attempts, AC-8: System Use Notification, AC-9: Previous Logon Notification, AC-10: Concurrent Session Control, AC-11: Session Lock.
- ISO 21827 System Security Engineering - S:** PA01 - Administer Security Controls, 7.1.1 Process Area, 7.1.2 BP.01.01 - Establish Security, 7.1.3 BP.01.02 - Manage Security, 7.1.4 BP.01.03 - Manage Security.
- ISO 20000 - Service Management:** Service Delivery Process, Service Level Management, Service Reporting, Service Continuity & Availability Management, Budgeting & Accounting for IT Svs, Capacity Management, Information Security Management, Relationship Management, Business Relationship Management, Supplier Management, Resolution Process, Control Processes.
- BS 25999 Business Continuity BCM:** BCM Planning Models.
- US Regulations:** US Regulations, Common Criteria for Information Technology Security Evaluation, Financial - FFIEC, Gramm Leach Bliley, HIPAA, SB 1386 - California Privacy Law, AB 1950 - California Privacy Law for Medical Information, SCADA, Sarbanes Oxley, 21 CFR Part 11.
- Risk Management:** Risk Management, Threats, Vulnerabilities and Controls, Additional Threats, Vulns and Controls.
- Enterprise Architecture:** Enterprise Architecture.
- ISO/IEC 27001 Project:** ISO/IEC 27001 Project, Management Minutes, Implementation Schedule, Scope Document, Asset List, Risk Assessment Criteria, Risk Treatment Criteria, Applicable Contracts, Applicable Policies, Statement of Applicability (SoA), Risk Treatment Plans, Applicable Procedures, Audit Results.

Harmonization with existing BS/ISO standards & guidelines



Additions:

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

ISO 19077 Software Asset 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

Questions?

CONSULT
COMPLY



Thank You!



Presenter Steve Crutchley

Email: scrutchley@consult2comply.com

Telephone: 571 332 8204/703 871 3950