Information Technology Governance

Steve Crutchley
CEO - Consult2Comply
www.consult2comply.com

What is IT Governance?

- **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.

Governance Issues

CONSULT COMPLY

Corporate Monitoring

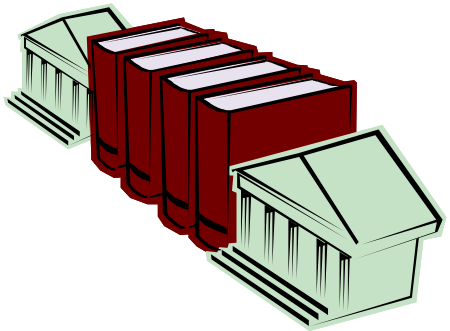
Protecting Personnel records

Weak Decision making mechanisms

Protecting IP

Ineffective enforcement and conflict resolution

Lack of Financial Resources



Good and concise Policies

Boundary Identification

Understanding Business responsibilities

Understanding Stakeholder needs

Jurisdiction Identification

Setting the Risk Appetite

Understanding Fiduciary responsibilities

Making the business owners responsible

Linking it all together

Legislative Issues

CONSULT COMPLY

PIA JSOX PCI

The European Union Directive on Data Protection

Smith Report BITS FDA

Electronic Communications Privacy Act 1986

National infrastructure Protection Act 1996

FACTA

ISO 17799 FFIEC

ISO 27001

NIST 800 Series Standards

EU Privacy Directive

UPA

UK Data Protection Act

HIPAA Basel II Bill C-6

PIPEDA

EU Regulatory Framework for Electronic Communications

SB-1386 California 21 CFR part 11

Patriot Act II Turnbull Report

Computer Security Act 1987

Anti-terrorism, Crime and Security Act 2001

Higgs Report

Freedom of Information Act

Homeland Security Act ISO 15489

Digital Millennium Copyright Act 1998

NIST OMB-123 GISRA

Computer Fraud and Abuse Act 1986

GLBA OMB-130 FISMA

Children's Online Privacy Protection Act of 1998 (COPPA)

Government Information Security Reform Act

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

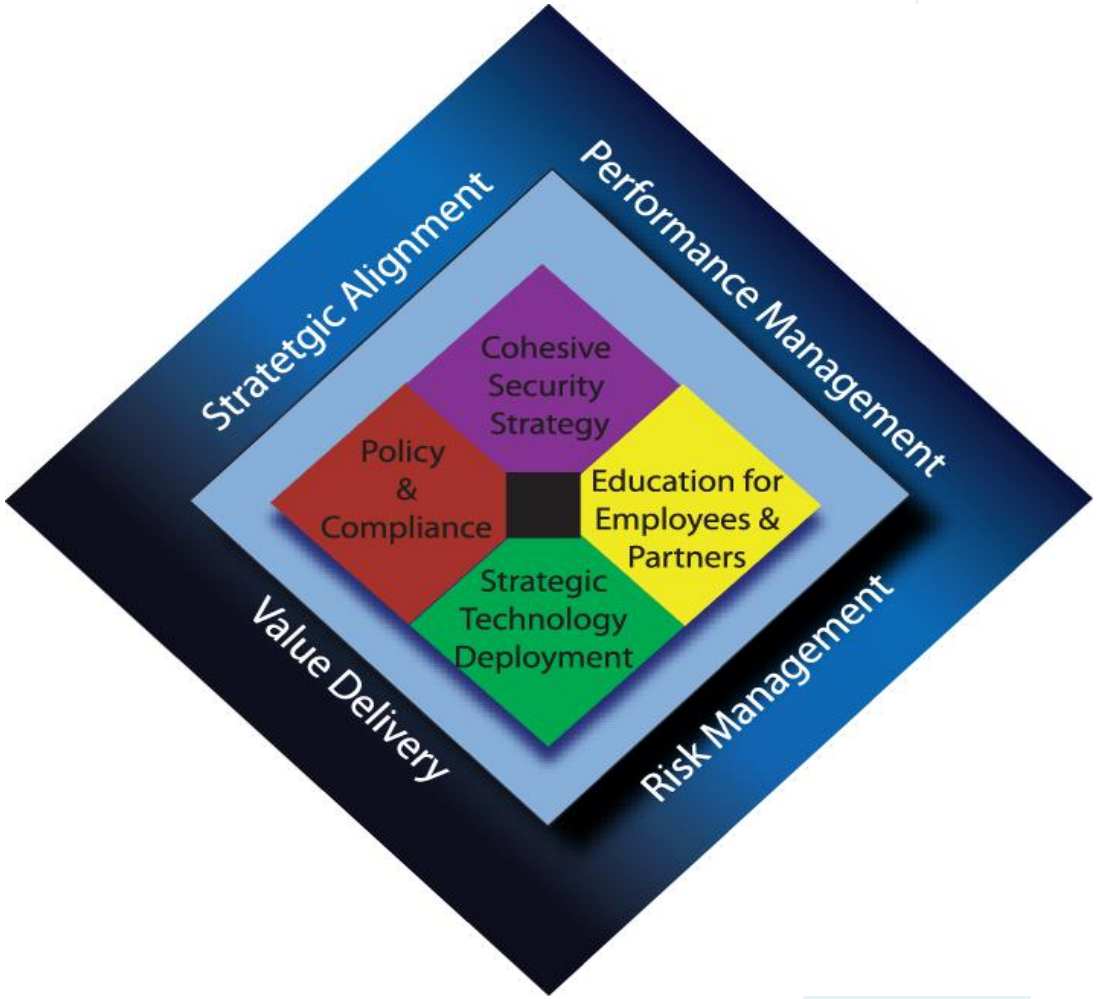
The Telecommunications (Data Protection and Privacy) Regulations 1999

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

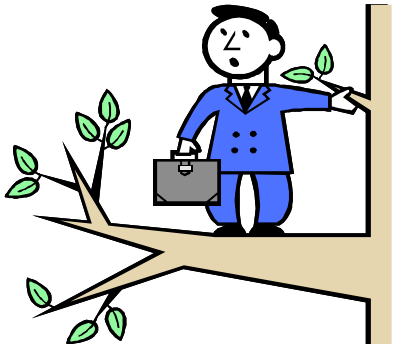
Understanding Risk Appetite

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

Risk Assessment –v- Risk Management

Accepting Residual Risk

Risk Reporting

Understanding Control Selection process

Cost of Remediation

Risk Differences:
Fraud
Business
Financial
Technology
Process
People
Tax
Governance

Risk Mitigation

Risk Integration – Linking it all together

smart securityservices

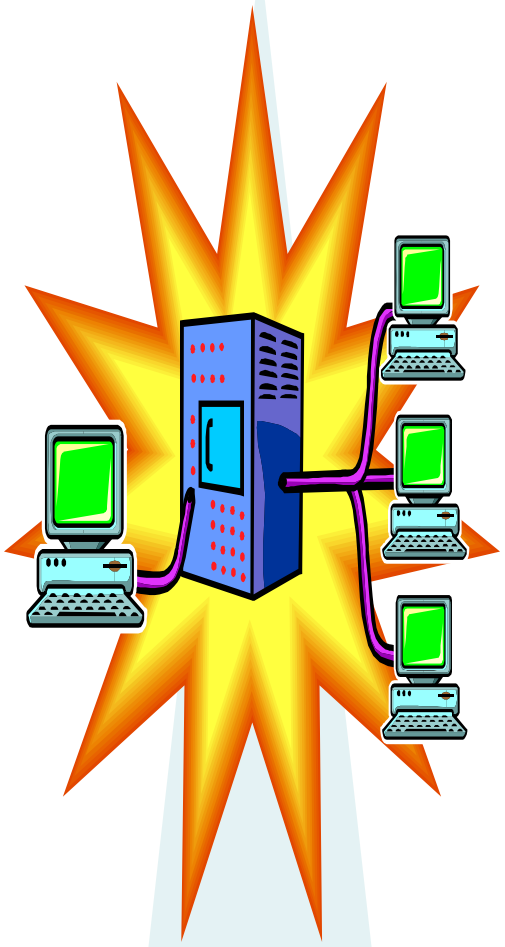
What are the IT Governance Characteristics?

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

CONSULT COMPLY

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

External Threats

CONSULT COMPLY

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
DoS/DDoS
Crackers
Spoofing
Identity theft
Rogue Applications
Industrial Espionage
Trojan Horses
Worms
New Regulations
Script Kiddies
Labor Action
Virus's
WarGames
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

CONSULT COMPLY

Port Security "USB"

Patch Management

Policy adherence

Spam

Education and Awareness

Information leakage

UDP Services

News

Sniffing

Disgruntled Employees

Unauthorized Insider access

Webmail

Gopher

Social Engineering

TFTP

FTP

Identity theft

Rogue Applications

Access Control

External DNS Zone Transfers

Sabotage

Instant Messaging

Finger Buffers

HTTP

Too many Services

Human Factor

TCP Hijacking

Admin Errors

Sendmail

email

Wireless

NFS

IP Theft

Privilege Escalation

DNS Cache-based Trust

Modem Hijacking

Security Sensor Misconfiguration

Bad Application Code

Poorly Maintained System

Physical Security

CONSULT COMPLY

Cable Security
Building Management
Disposal Services
Anti-theft measures
Guarding
Perimeter Security
Business Continuity
Physical Protection
Trash collection
Express Kidnapping
Surveillance
Wireless
Chauffeurs/Drivers
Maintenance
Snooping
Elevators
Special Projects
Protection (People)
Access Control
Parking Lots
Utilities – Power and Water
CCTV
Communications
Booms
Telephony
Patrols
Alarms
Smoking/Smoke Areas
Contracts
Reception
Keying
Bugs & Probes
Keycards
Building Security
Evacuation
Emergency Services
Transportation
Escorting
Health & Safety
Cleaning Staff
Counter Surveillance
Entry/Exit Points
Landlords
Firearms
Turnstiles
Plants
Raised Flooring
Proximity Security
Clear Desk
Disaster Recovery
Office Erection
Fireproof Safes
First Aid
Biometrics
Emergency Exits
Entry/Exit Controls
Physical Layouts
Eavesdropping
Fire-resistant and tamper-resistant storage facilities
Anti-vandal measures

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

Business Technology Optimization

Strategic Planning

Organizational Structure

Service Level Management

Security Management

Availability Management

Project Governance

Release Management

Training

Enterprise Architecture

Service Continuity

Change Management

Problem Management

Financial Management

Business Relationship Management

Incident Management

Asset Management

Supplier Management

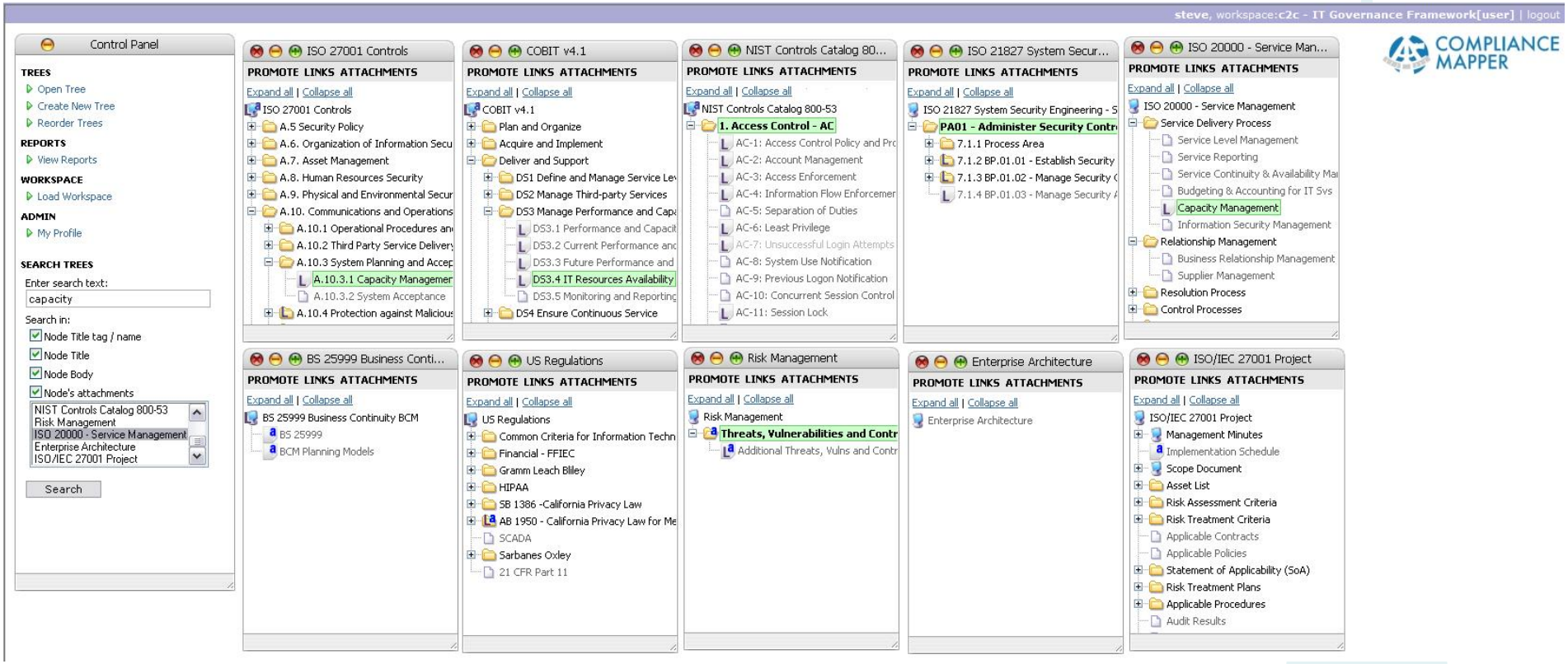
Capacity Management

What can help you?

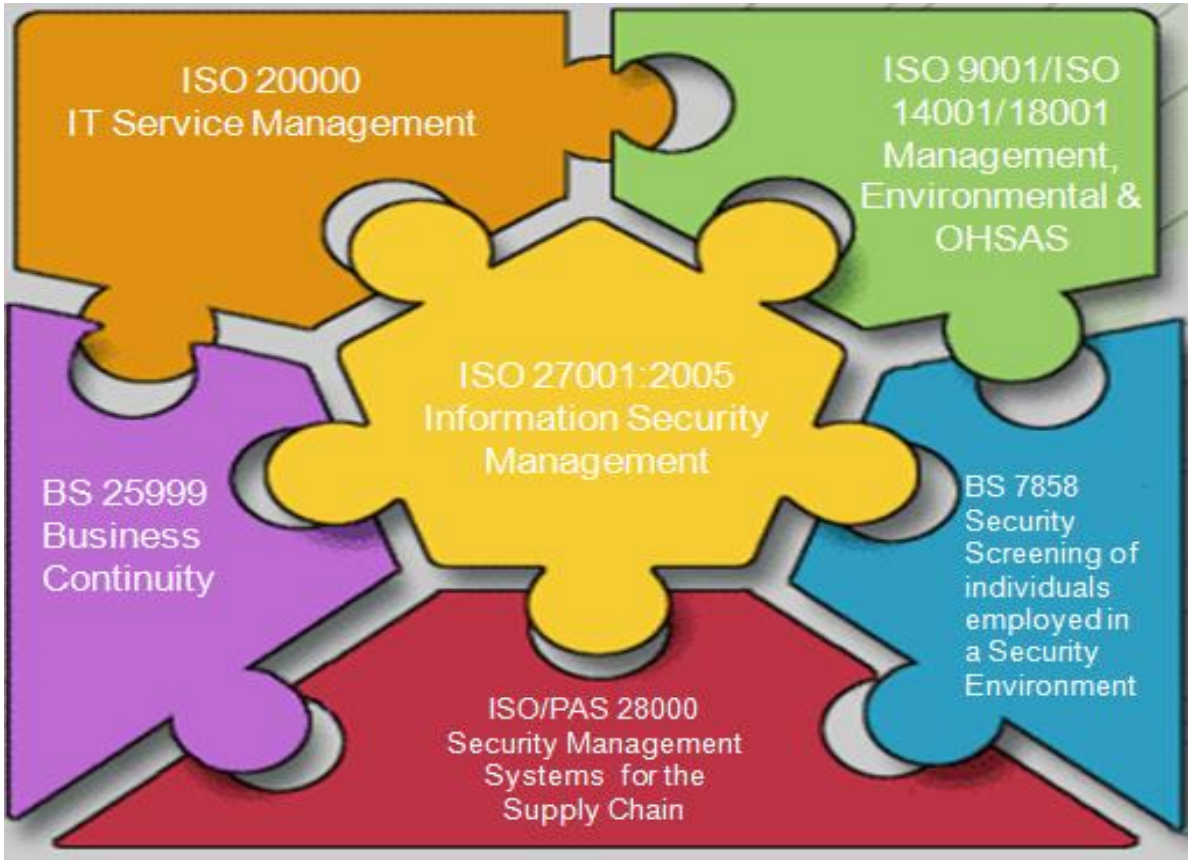
CONSULT COMPLY

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



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