iWeb

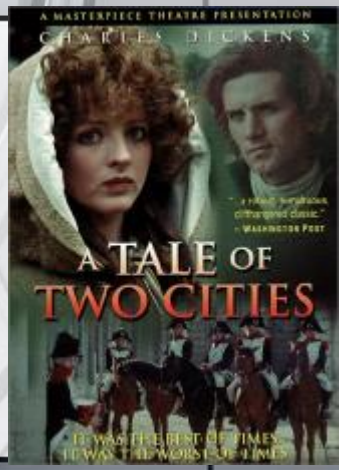
SECURITY SUMMIT 2010

IT'S **YOUR** BUSINESS!

'A Tale of 2 Cities' & Control Frameworks

'It was the best of times….it was the worst of times……..'

David Volschenk & Justin Williams
Ernst & Young



Our Story

- 'A tale of two cities'
- Parallels
- Part 1 - Introduction to the set or storyboard
- Part 2 - The story unfolds
- Part 3 - What was learnt
- Conclusion

The Two Cities

Disclaimer

- Neither of the presenters have read the book from cover to cover (or stayed awake during the DVD..... )

BUT

- ….. We have however experienced a number of framework implementation initiatives over the last few years.....

Themes from the ‘tale’

- Two major cities, alike but different
- Resurrection (Life), and Death
- Light and Darkness
- Brutalisation
- Sowing and reaping

‘Book’ to the Present

- Cities became Companies, Divisions, and BU’s
- Sovereignty became – Frameworks
- Characters became Management and Employees

Part 1 - Introduction

- The cities
- Sovereignty
- The characters

The Companies

- Anonymity
- Company A
  - large national company
- Company B
  - large multinational company
- IT control framework vs Information security framework

What is a framework

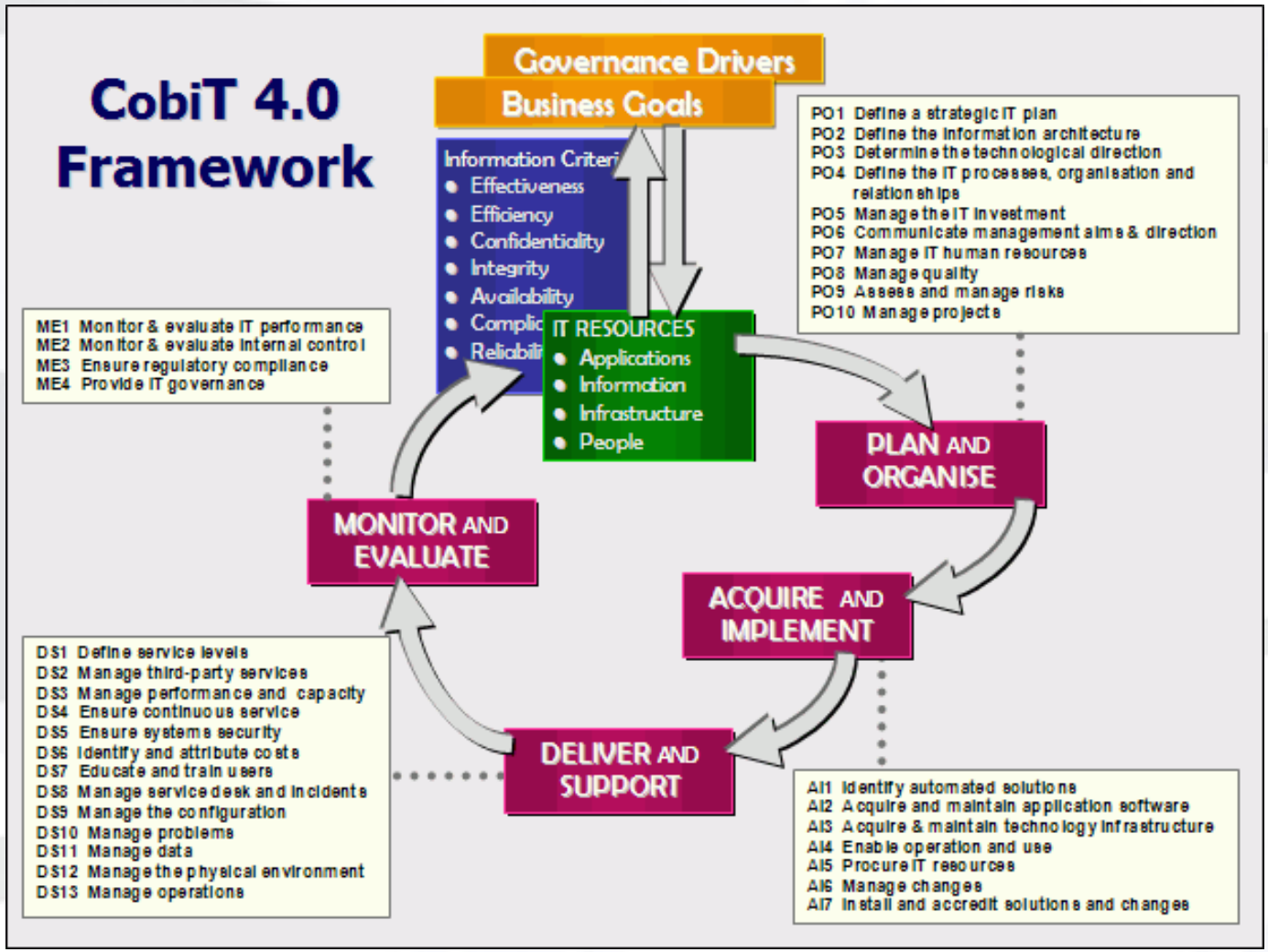
- Generally defined to:
  - Support beams that represent a building's general shape and size;
  - Combination of templates and structured processes that facilitate the establishment of an architecture;
  - Basic conceptual structure used to solve or address complex issues;
  - Guidelines on how to solve problems not explicitly defined.

- Characteristics of frameworks

Framework types

- Many to choose from
- Types
  - Governance
  - Risk Management
  - Security
  - Audit / Assurance

COBIT


CobiT 4.0 Framework
Governance Drivers
Business Goals
Information Criteri
Effectiveness
Efficiency
Confidentiality
Integrity
Availability
Complic
Reliabili
IT RESOURCES
Applications
Information
Infrastructure
People
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
PLAN AND ORGANISE
ACQUIRE AND IMPLEMENT
DELIVER AND SUPPORT
MONITOR AND EVALUATE
ME1 Monitor & evaluate IT performance
ME2 Monitor & evaluate internal control
ME3 Ensure regulatory compliance
ME4 Provide IT governance
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
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

BS 7799

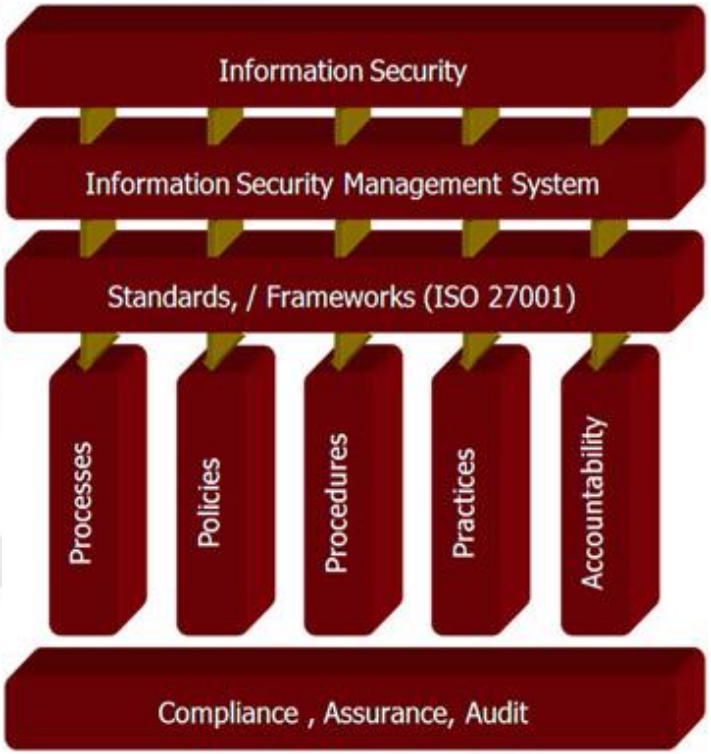
- BS 7799 Part 1 (Code of Practice)
  - Changed to ISO 17799 and then to ISO 27002
    - Has 133 controls and 500+ detailed controls
- BS 7799 Part 2
  - Changed to ISO 27001
  - Primarily deals with Information Security Management System (ISMS)

ISO 27000 Family

ISO 27000 (Family)

- ISMS fundamentals and vocabulary, umbrella standards

- 27001 ISMS
- 27002 Code of Practice
- 27003 ISMS implementation guide
- 27004 ISM metrics
- 27005 Infosec risk management
- 27006 Certification agencies
- 27007 Audit guidelines
- 27009 IS governance
- 27010 critical infrastructure



Information Security Forum (ISF)

- 'Standard of Good Practice' for Information Security
- Has 5 "aspects" to it
  - Security Management
  - Critical Business Applications
  - Computer Installations
  - Networks
  - Systems Development
- Segregated into 30 "areas" and 135 "sections"

ITIL

- Information Technology Infrastructure Library
  - Provides management guidelines on:
    - Incident response
    - Problem management
    - Change management
    - Release management
    - Configuration management
    - Service desk management
    - Service level management
    - Availability
    - Capacity management
    - Service continuity
    - IT financials
    - IT workforce/HR management

Resistance to frameworks

- Common "Complaints" or excuses
  - 'Nothing has happened for the past X years. What is going to happen now and why do you want all this security all of a sudden ??'
  - 'We want work to be done. Do not hamper our routine to integrate your security practices.'
  - 'Security!!! Not our problem, go and ask IT
  - 'If I change this now, nothing is going to work. Don't fix what isn't broken'
- Why do people change?
  - The fire and the light
  - Unfreeze change freeze (Kurt Luwin)

Why A Framework

- Drivers for Frameworks
  - Consistency
  - Legislation
  - Demanded by “King 3”
  - Reputation
- Benefits of implementing frameworks
  - roadmap
  - defines roles
  - provides structure
  - tool for senior corporate executives and managers
  - identifies cornerstone practices

Views on Frameworks

- CIO's views on ISO standards
- Microsoft hosted products (ISO 27001)
- Google cloud computing services (FISMA)
- CIO's views on Cobit 4

The 5 COSO Questions

- Do we have the right foundations to control our business? (control environment)
- Do we understand all those risks that stop us from being in control of the business? (risk assessment)
- Have we implemented suitable control activities to address the risks to our business? (control activities)
- Are we able to monitor the way the business is being controlled? (monitoring)
- Is the control message driven down through the organization and associated problems and ideas communicated upwards and across the business? (communication and information)

Quality responses to the questions demonstrates controls

King 3 – security & control

- Board responsible for IT governance (5.1)
  - Board should ensure that an **IT internal control framework** is adopted and implemented (5.1.4)
- Board to ensure information assets are managed effectively (5.6)
  - Systems in place for information management, security and privacy
  - All personal information identified and treated as important business asset
  - **Information Security Management System** is developed and implemented (5.6.3)
  - Information security strategy approved at Board level
  - implementation delegated to empowered management

King 3 – security & control

- Risk & audit committees assist board carrying out IT responsibility (5.7)
  - Risk committee to:
    - ensure that **IT risks are adequately** addressed (5.7.1)
    - obtain appropriate assurance that **controls are in place and is effective** in addressing IT risks (5.7.2)

The characters & roles

- CEO's ,CFO's
- CIO's, CISO's
- ISO's, Risk Managers, Audit Managers
- Forum or 'IS Organisation' members
- Business unit management
- Technical staff
- Consultants

Part 2 – The Story Unfolds

- The process followed
- Implementing the framework

The Story Unfolds-'A'

- The process followed for company A
  - IT control framework selected
  - Process driven by C suite
  - Small project team evaluated frameworks
  - Key stakeholders identified

- Many interventions were held, with key stakeholder participation and support

- Final framework was adopted for rollout throughout the enterprise

The Story Unfolds – 'B'

- The process followed for company B
  - A security framework selected
  - Process driven by CIO, IT Management and ISO
  - Total framework implementation in project scope
  - Key stakeholders identified

- Roundtable security forum created (monthly)
  - Driven centrally
  - Erratic and scattered representation
  - Long time decision making and approval processes

- Continuous loss of traction in framework component selection efforts

Implementation ‘A’

- Process supported through organisational structure
  - Division reporting to CIOs;
  - CIOs to CFO & internal control risk committees (ICRC);
  - Process driven from the top;
  - Integrated into staff KPAs;
  - Bonuses affected

- Training rolled out for staff
- Weekly meetings held
- Hard line taken

Implementation ‘A’

- Controls written into standard operating procedures
  - Supported by checklists
  - Regular self assessments (monthly)
  - internal audit assessments (six monthly)

- All findings recorded and followed up

Implementation ‘B’

- Forum sessions
  - Standard agenda’s and formal minutes
  - Poor participation
  - Strong central influence impaired participation
  - Long decision making process
  - Slow implementation
  - Poor accountability
  - Empty threats
  - Repetitive activities

- Incorrect organisational support
- Disconnect – divisions expected to execute but acted autonomously
- No periodic compliance assessments

Part 3 – What was learnt

- What did we learn from our story and 'characters'
- Challenges
- Outcomes
- Benefits (or not)
- Continuous improvements

What was learnt

- What did we learn from our story and ‘characters’
  - Frameworks
  - Roleplayers
  - Sponsorship

- To Succeed
  - Right sponsors
  - Keep it simple
  - Choose what is right for organisation
  - Constant monitoring

Challenges to implementation 'A'

- Resistance to Change
- Culture and Mindset Change
- Business Acceptance of IT Controls
- System Limitations
- Differences between business and audit requirements
- Staff retention and rotation
- Manual Processes

Challenges to Implementation 'B'

- Organisational structure
- Executive management support and sponsorships
- Non committal stakeholders and continuous changes
- Poor discipline
- Disconnect between BU's and Central
- Autonomous Business Units
- Inadequate disciplinary actions for non performance
- Performance expectations not incorporated in personal KPI's

Outcomes of implementation ‘A’

- Framework compliance reviews continually improved
- Reviews seamless
- Management response to findings positive
- General awareness of controls improved
- Internal audit and governance become trusted partners

Outcomes of Implementation ‘B’

- No proper traction
- Isolated initiatives
- Assessments not performed
- Re-assessment of framework with view to replace
- Continued discussion forums
- Implementations not considered a success
- Implementation of standards problematic

Benefits from the framework ‘A’

- Enforcing key controls
- Structured approach in IT Environments
- Clarification of roles
- Increased accountability
- Increased reliance on data
- External audit place reliance
- Improved compliance
- Increased knowledge and understanding
- Improved skill set of staff
- System security threats were addressed
- Reviews highlighted risks and anomalous activity
- Harmonious relationships

Story Changes for 'B'

- City or Company
  - Organisational structure and reporting structure is important to create buy in and commitment across enterprise
- Laws or frameworks
  - Concentrate on business requirements
  - Framework as starting point and adapt to business
  - Frameworks provide structure for program
  - Enterprise security is a commitment, not a project
  - Incremental approach
  - Construct own framework from components
- Characters
  - ISMS implementations need group business executive support
  - Key stakeholders identified carefully
  - Stakeholders must be fully committed
  - Autonomous and individual efforts must not be allowed

Continuous Improvements

- Automation of controls
- Handover when staff changes occur
- Institutionalisation of further controls
- Continuous training
- Updating SOPs
- Integration into all future projects

The Sequel (Next steps)

- Will our successful character continue to prosper, or will he succumb
- Does our failed city have a hope of turning around and mirroring the success of the other

Questions?

Thank You

Where to get more info

- ISO
- Cobit (WWW.ISACA.ORG)
- ITIL
- ISF Standards of Good Practice (WWW.ISF.ORG)
- SANS (WWW.SANS.ORG)

Contact us

- David Volschenk
  - David.Volschenk@za.ey.com
  - +27 82 322 2994
- Justin Williams
  - Justin.Williams@za.ey.com
  - +27 83 601 2736