SHARE
Technology · Connections · Results

ITIL and Security? (or Why You Shouldn't Trust ITIL For Security Management)

Reg Harbeck
CA

Monday, August 13, 2007
Session 1761

Agenda

- What is ITIL and how did it happen?
- What is security?
- How does security fit into ITIL?
- How do you bring security to an ITIL environment?
- So what?
- Discussion

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

ITIL Origins And Evolution

ITIL is all about which processes need to be realized within the organization for management and operation of the IT infrastructure to promote optimal service provision to the customer of the services at justifiable costs.

- Late 1980s
  - UK government project started
  - CCTA (Central Computer and Telecommunications Agency) in OGC (Office of Government Commerce) involved in development as well as practitioner and consulting organizations
  - Organizations outside of government became interested
  - First books published
- Early 1990s
  - The library completed
- Late 1990s
  - Generally accepted as the de-facto standard for IT service management worldwide
- Today
  - Still a great way for an organization to emulate the British Government!

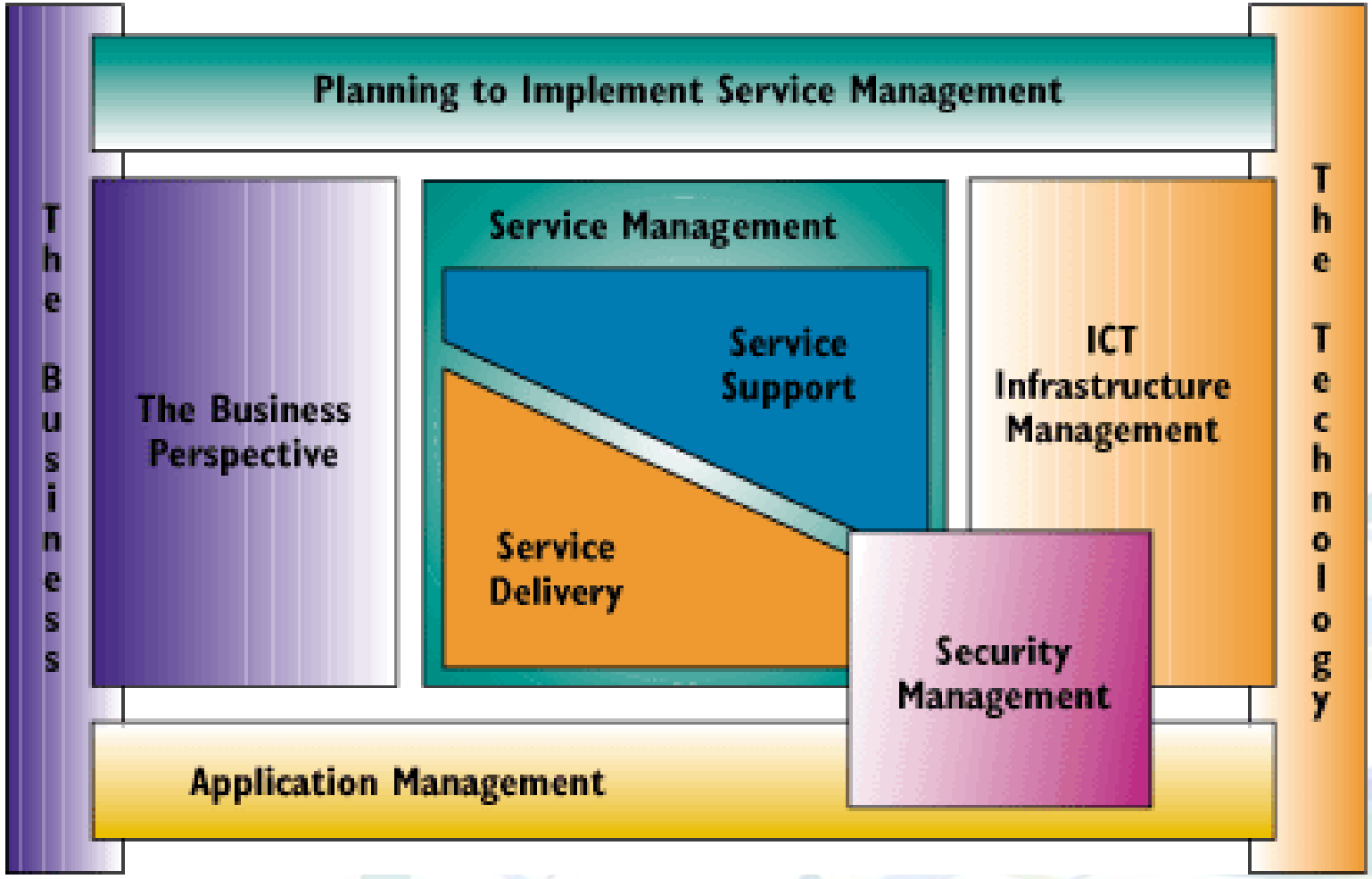
Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

The Mainframe Roots of ITIL

- ITIL basically documented how the UK Government ran their IT
- UK Government IT was essentially mainframe or descended from mainframe practices
- IBM claims that these practices were descended from its "Yellow Books" (“A Management System for the Information Business” – see http://www-5.ibm.com/services/ch/ism/download_ism/itil.pdf)

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

ITIL Books (v2)



Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

What is Security?

- "A computer is secure if you can depend on it and its software to behave as you expect."
  - "Practical UNIX and Internet Security", by Simson Garfinkel and Gene Spafford
- SHARE Requirements for External Security (1970's)
- External Security vs Native Security
- Rainbow Series Books on Computer Security Standards (1980's and 1990's)
- Security Specialists

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

How does Security fit into ITIL?

- Security division at CCTA (Central Computer and Telecommunications Agency) was writing their own guidebook
- ITIL authors contented themselves with CIA (Confidentiality, Integrity and Availability) - ensuring that services are used in an appropriate way by the appropriate people:
  - Confidentiality - protection of data from unauthorized access
  - Integrity - completeness and soundness of the data
  - Availability - the data is available as and when required
- Security portion secret for government only, not shared outside - not publicizing security issues
  - Concept: “How did they do it?” → “How could I do it?”
- Conscious decision to just make ITIL “aware” of security
  - Isolated process
  - Other tenets of the library talk about integration and sharing information, but security must be stand-alone
  - Must be a domain expert (current ITIL folks aren't security domain experts)

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

How does Security fit into ITIL? (cont'd)

- Eventually put a book out which was a passable resume of what's already in the market, "10 seconds' worth"
- Just a 1-hour portion on security in ITIL manager course
- Guidance in ITIL written for people in ITIL, not for security experts:
  - "I'm not a security person, but here's my perspective"
  - A security person would NEVER use ITIL
- ITIL is about best practices for managing operations

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

How do you bring security to an ITIL environment?

- COSO (Committee of Sponsoring Organizations of the Treadway Commission)?
  - Intended to identify and reduce factors that cause fraudulent financial reporting.
  - Established common definition of internal controls, standards, and criteria.
  - Contains requirements for a range of areas of governance.
  - There is little in the COSO framework regarding specific IT controls.

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

How do you bring security to an ITIL environment?

- COBIT (Control Objectives for Information and related Technology)?
  - Published by the IT Governance Institute, which is affiliated with the Information Systems Audit and Control Association (ISACA).
  - Contains a broad set of IT control objectives that provide statements of "the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."
  - Widely adopted framework for IT controls.
  - See session 1742, "Aligning ITIL Processes with COBIT Stages" on Wednesday at 11am.
  - Goes well beyond security…

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

How do you bring security to an ITIL environment?

- ISO 27000!
  - A Standard of the the Joint Technical Committee (JTC1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
  - Part of the ISO 27000 Series "family" of ISO ISMS (Information Security Management Systems) standards.
  - ISO 27000 is ***the*** source of security information for ITIL.
  - Frameworks have nothing to do with guidance.
    - COBIT just says do you have a process that you can audit?
    - ITIL says you might need a security manager.
  - ISO 27000 identifies what to audit and shows its ITIL relevance.
  - "Smart people in the ITIL world use ISO 27000 as their bible." – Brian Johnson, ITIL Author

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

More about ISO 27000 Series

- ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary (not yet published)
- ISO/IEC 27001 - the certification standard against which organizations' ISMS may be certified
- ISO/IEC 27002 - the proposed re-naming of existing standard ISO 17799
- ISO/IEC 27003 - a new ISMS implementation guide (not yet published)
- ISO/IEC 27004 - a new standard for information security management measurements (not yet published)
- ISO/IEC 27005 - a proposed standard for risk management (not yet published)
- ISO/IEC 27006 - a guide to the certification/registration process

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

ISO/IEC 27001

- Originally BS 7799 parts 2, 3 from the British Standards Institute (BSI)
- “ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements”
- Often used in conjunction with ISO 17799, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls.
- Certification of an organization's ISMS against ISO/IEC 27001 is one means of providing assurance that the certified organization has implemented a system for the management of information security in line with the standard.

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

ISO/IEC 27002

- BS 7799 part 1 from the British Standards Institute (BSI)
- Adopted by ISO (International Organization for Standardization) as ISO/IEC 17799:2005, "Information Technology - Code of practice for information security management."
- Becoming ISO/IEC 27002
- 12 main sections…

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

ISO/IEC 27002 cont'd

1. **Risk assessment and treatment** - analysis of the organization's information security risks
2. **Security policy** - management direction
3. **Organization of information security** - governance of information security
4. **Asset management** - inventory and classification of information assets
5. **Human resources security** - security aspects for employees joining, moving and leaving an organization
6. **Physical and environmental security** - protection of the computer facilities
7. **Communications and operations management** - management of technical security controls in systems and networks
8. **Access control** - restriction of access rights to networks, systems, applications, functions and data
9. **Information systems acquisition, development and maintenance** - building security into applications
10. **Information security incident management** - anticipating and responding appropriately to information security breaches
11. **Business continuity planning** - protecting, maintaining and recovering business-critical processes and systems
12. **Compliance** - ensuring conformance with information security policies, standards, laws and regulations

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

So What?

- You can't "do ITIL" anyway – it's a framework
- What are you trying to achieve? Security or certification of/and compliance?
- Security is a journey, not a destination
- Certification of/and Regulatory Compliance are achievable using standards and other guidance (e.g. see Mainframe Compliance paper)
- I can suggest some great software to help ☺

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Acknowledgements

- Brian Johnson, ITIL Author, CA ITIL Practice Manager
- Nancy Hinich, CA ITIL Solution Manager
- Wikipedia.org

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.

Discussion

Copyright © 2007 CA. All trademarks, trade names, services marks and logos referenced herein belong to their respective companies.