



# Bridging the gap between ISO17799 and Security Operations

Jean-François Legault, M.Sc.  
CISSP, CISM  
514-870-0605



## The light side of Security Operations

- Technically competent staff
- Excellent knowledge of networking and systems
- Excellent technical knowledge of security

## The dark side of Security Operations

- Often lack structure: who does what and how?
- Documentation: it's all in their heads
- Often left to their own devices (are they IT or not?)
- No segregation of duties: no dedicated resources to security operations
- Clean desks: the sign of an insane admin
- Ever absent operator logs



## Key security operations processes

- Fault management
- Change management
- Capacity management
- Incident management
- Business continuity
- Technical compliance





## Bridging the gap

- ISO17799 provides a framework for security operations
- Identify delivery mechanisms to achieve the "how" and "what" of security operations controls
  - ITIL
  - COBIT
  - NIST
  - Others



## ITIL: Information Technology Infrastructure Library

- Created by the British Office of Government Commerce
- Series of documents that are used to aid the implementation of a framework for IT Service Management
- Customisable framework defines how Service Management is applied within an organisation
- Focus on the client
- ITIL self-assessment: <http://www.itsmf.com>





## **COBIT: Control Objectives for Information and related Technology**

- Created by ISACA
- Provides information technology control objectives
- <http://www.isaca.org>





## **NIST: National Institute of Standards and Technology**

- Non-regulatory federal agency within the U.S. Commerce Department's Technology Administration
- NIST's Computer Security Division develops standards, metrics, tests and validation programs in the field of information security
- <http://csrc.nist.gov>



## Fault management: ISO 17799:2000

- 8.4.2: Operator log
  - Operational staff should maintain an activity log
- 8.4.3: Fault logging
  - Faults should be reported and actions taken
  - Review of faults
  - Review of corrective measures



## Fault management: Bridging the gap

- COBIT DS10: Manage problem and incidents
  - Define and implement a problem management system
  - Escalation procedures
  - Problem tracking and audit trail
- ITIL: Incident management
  - Incident recording and alerting
  - Incident support and classification
  - Resolution and recovery
  - Incident tracking
- ITIL: Problem management
  - Identification of root cause
  - Proactive problem prevention



## Change management: ISO 17799:2000

- 10.5.1: Change control procedures
  - Strict control over the implementation of changes
  - Enforcement of formal change control procedures
  - Authorization changes
  - Audit logs



## Change management: Bridging the gap

- COBIT A16: Manage changes
  - Standardization request for changes
  - Prioritization of changes
  - Impact assessments
  - Documentation of changes
- ITIL: Change management
  - Changes to configuration are carried out in a planned and authorised manner
  - Business reason behind each change
  - Planning and testing
  - Backout plan



## Capacity management: ISO 17799:2000

- 8.2.1: Capacity planning
  - Monitoring capacity demands
  - Projection of future capacity requirements
  - Identify and avoid potential bottlenecks



## Capacity management: Bridging the gap

- COBIT DS3: Manage performance and capacity
  - Business needs for capacity and performance should be identified
  - Process for reporting on the performance of IT resources
  - Forecasting capability
- ITIL: Capacity management
  - Identify services and IT infrastructure required
  - Identification of inputs into the capacity management process



## Incident handling

- Incident handling procedures
  - Identifying and managing incidents
- Vulnerability management
  - Managing technical threats
- Evidence collection
  - Digital evidence handling



## Incident management procedures: ISO 17799:2000

- 6.3.1: Reporting security incidents
  - Quick reporting through appropriate management channels
  - Formal reporting procedure
  - Training of employees and contractors
- 6.3.4: Learning from incidents
  - Quantify and monitor the types, volumes and costs of incidents
  - Identify high impact or recurring incidents
- 8.1.3: Incident management procedures
  - Procedures to ensure quick and orderly response to incidents
  - Collection of audit trails and evidence
  - Post incident recovery



## Incident management procedures: Bridging the gap

- COBIT DS5.11: Incident handling
  - Establish computer security incident handling capability
  - Sufficient expertise
  - Incident management procedures to address incidents efficiently
- NIST SP800-61: Computer security incident handling guide
  - Organizing a computer security incident response capability
  - Incident response lifecycle



## Incident management procedures: Bridging the gap

- RFC 2350: Expectations for Computer Security Incident Response
  - Describes constituent community expectations from a CSIRT
  - Policies, charter, procedures,
- ISO 18044: Information security incident management
  - Advice and guidance on information security incident management
- CERT/CC: CSIRT Handbook (<http://www.cert.org>)
  - CSIRT framework
  - Functions of the incident handling process
  - CSIRT Operations



## Vulnerability management: ISO 17799:2000

- 6.3.2: Reporting security weaknesses
  - Note and report observed or suspected security weaknesses
- 8.3.1: Controls against malicious software
  - Detection and prevention controls to protect against malware



## Vulnerability management: Bridging the gap

- NIST SP800-40: Procedure for handling security patches
  - Identification of vulnerabilities and patches
  - Patching procedures
- CERT/CC: CSIRT Handbook
  - Proactive incident management services
- SANS: Top 20 vulnerabilities (<http://www.sans.org/top20>)
  - Consensus list of vulnerabilities that require immediate remediation
- MITRE: Common vulnerabilities and exposures (<http://cve.mitre.org>)
  - List of standardized names for vulnerabilities and other information security exposures



## Evidence collection: ISO 17799:2000

- 12.1.7.3: Quality and completeness of evidence
  - Strong evidence trail
  - Prevent destruction of evidence



## Evidence collection: Bridging the gap

- RFC 3227: Guidelines for Evidence Collection and Archiving (<http://www.faqs.org/rfcs>)
  - Guiding principles during evidence collection
  - Collection procedure
  - Archiving procedure
- IOCE: Guidelines for Best Practice in the Forensic Examination of Digital Technology (<http://www.ioce.org>)
  - Quality assurance
  - General principles applying to the recovery of digital evidence



## **Business continuity: ISO 17799:2000**

- 11.1: Aspects of business continuity management
  - Counteract interruptions to business activities
  - Protect critical business processes from the effects of major failures
  - Business continuity management process
  - Business continuity and impact analysis
  - Testing of contingency plans



## **Business continuity: Bridging the gap**

- **COBIT DS4: Ensure continuous service**
  - Establish a continuity framework in cooperation with business process owners
  - Ensure that IT plan is in line with the business continuity plan
  - Testing and maintenance of the plan
- **ITIL: Continuity management**
  - Prioritise the functions to be recovered
  - Evaluate options for recovery
- **NIST SP800-34: IT Contingency planning guide**
- **BSI PAS 56: Guide to Business Continuity Management**

## **Business continuity: Bridging the gap**

- **NIST SP800-34: IT Contingency planning guide**
  - IT contingency planning process
  - IT contingency plan development
  - Technical contingency planning considerations
- **BSI PAS 56: Guide to Business Continuity Management**
  - British Standards Institute Publicly Available Specification 56
  - Overview of activities involved in setting up a BCM process
  - Makes recommendations for best practice





## Technical compliance: ISO 17799:2000

- 12.2.2: Technical compliance checking
  - Regular check systems for compliance with security implementation standards
  - Examination of OS
  - Penetration testing



## Technical compliance: Bridging the gap

- COBIT M2: Assess internal control adequacy
  - Monitor the effectiveness of internal controls
  - Audit to establish whether security controls are operating in accordance to requirements
- NIST SP800-42: Security testing
  - Roles and responsibilities
  - Security testing techniques
- OSSTMM: Open Source Security Testing Methodology Manual
  - Peer-reviewed methodology for performing security tests and metrics
  - Focuses on the technical details of which items need to be tested, what to do before, during, and after a security test, and how to measure the result



## Bridging the gap

- ISO 17799
  - Security requirements
- COBIT
  - Control objectives
  - Management guidelines
  - Audit guidelines
- ITIL
  - Basic concepts activities
  - Planning for implementation
- NIST and others
  - Technical implementation



## Do's and Dont's

### Do's

- Have processes supported by policies
- Define procedures from the bottom up
- Use today's methods as a base
- Assume technical expertise from Ops staff
- Survey what is being done in the industry

### Dont's

- Let processes evolve without alignment
- Impose processes from the top
- Recreate everything
- Assume process expertise from Ops staff
- Apply exactly what others are doing

