ISO/IEC 27001
Information Security Management System
Vs
ITIL – IT Security Management

Presented by Mark E.S. Bernard,
CGEIT, CISM, CISA, CISSP, ISO27k Lead Auditor, PM, ITIL/COBIT Foundation, PA, CNA, IBM iSeries Servers
Manager, Compliance Assessment and Reporting, OCIO
AGENDA

✓ Overview
  - Quality Management
  - Plan, Do, Check, Act
  - Continuous Improvement
✓ ITIL-ITSM / ISO-ISMS
  - inputs/outputs
  - integration
  - service level management
  - reporting
✓ Conclusion
✓ Q & A
Instructional Objective: Participants will walk through the ITIL – IT Security Management processes as the facilitator compares it to the ISO/IEC 27001 – Information Security Management System framework. During our walk through the facilitator will highlight the pros and cons of each approach to generate discussion. As a result participants will achieve a higher degree of familiarity with these frameworks and be more effectually positioned to lead discussions within their own respective organizations concerning information security program initiatives.
EXPERIENCE: Mark has nineteen-years of proven experience within the domain of Information Security, Privacy & Compliance within a broad range of industries including, Government, Financial Services, Credit Unions, Charter Banking, Insurance, Pharmaceutical, Telecommunications, Technology, Manufacturing and Academia.

2007 – 2008 Led Credit Union Central of British Columbia’ to become the first online banking system and 2nd Financial Institution in Canada to earn the ISO/IEC 27001 Certification

2005 – 2006 Led EDS Advanced Solutions Privacy and Security Office during the migration of Revenue Services of British Columbia and citizen information from government to Alternate Service Delivery care


1997 – 2000 Led Taro Pharmaceutical with the centralization of ERP systems from Jerusalem and Taro New York to Brampton, Ontario including ISO recertification of warehousing and laboratories in compliance with FDA & Health Canada regulations

1997 – 2000 Led IBM Global Services penetration testing against off shore financial institutions located in Trinidad, Barbados, Nassau, Jamaica and Antigua and financial systems managed in Canada

1997 – 2000 Led TD Bank application conversion from CISC to RISC for Wealth Management systems including hardware upgrades of TSX systems and BCP initialization

1995 – 1997 Led Hanes Canada to implement a bar code pick pack systems including MH10 label and EDI integration


ACKNOWLEDGEMENTS: In 2002 Mark received acknowledgement from the New Brunswick Premier for his innovative contributions to the local knowledge industry. In 2002 Mark earned New Brunswick’s Rising Star award through his contributions to the local knowledge industry. In 2004 Mark received acknowledgement from the Information Systems Audit and Control Association for his contribution to the Certified Information Security Manager Common Body of Knowledge and Training materials.
Overview
Quality Management

“Quote”

‘We have learned to live in a world of mistakes and defective products as if they were necessary to life. It is time to adopt a new philosophy…’

(W. Edwards Deming, 1900–1993)
Quality Management for Information Security services is a systematic way of ensuring that all the activities necessary to design, develop, implement and maintain services satisfy the requirements of the organization and its employees while providing assurance that strategic and tactical activities are carried out cost-effectively.
Quality Management

Excerpts from Deming’s 14 points relevant to Service Management:

- break down barriers between departments (improves communications and management)

- management must learn their responsibilities, and take on leadership (process improvement requires commitment from the top; good leaders motivate people to improve themselves and therefore the image of the organization)

- improve constantly (a central theme for service managers is continual improvement; this is also a theme for Quality Management. A process led approach is key to achieve this target)

- institute a programme of education and self-improvement (learning and improving skills have been the focus of Service Management for many years)

- training on the job (linked to continual improvement)

- transformation is everyone's job (the emphasis being on teamwork and understanding).
Deming’s 14 point Service Management guidelines focus on 4 repetitive activities, which are Plan – Do – Check – Act. Through the establishment of a common theme “continuous improvement”. These activities are easily identifiable within both the ITSM and ISMS frameworks and can also be linked in to the Capability Maturity Model.
Plan – Do – Check – Act
“PDCA Model”
The PDCA Methodology is an iterative process model.

**PLAN**
- Design & Plan Information Security Program
- Lead Corrective, Preventive, and Continuous Improvement action plans
- Monitor, Audit, Review Information Security Program

**DO**
- Maintain & Improve Information Security Program

**CHECK**
- Execute and control the information security strategy including the integration into organizational practices.

**ACT**
- Facilitate semi-annual audits to determine conformance to the statement of applicability and identify opportunities for improvement. Wherever appropriate develop and integrate performance metrics which support information security program goals and objectives.
- Upon the discovery of nonconformities and/or opportunities create and track corrective, preventive, and continuous improvement action plans. Present findings from internal/external audit and risk assessments to the Management Review Committee for decisions regarding the acceptance, rejection, or transfer of risk and the commitment of resources and capital to facilitate subsequent efforts.

Interested Parties

Information Security requirements & expectations

Managed Information Security
Customer defines business requirements

Reporting According to SLA, OLA, UC

SLA/Security Chapter Agreement between customer and provider

IT Service Provider implements SLA Security requirements

MAINTAIN:
- Learn
- Improve
- Plan
- Implement

PLAN:
- Service Level Agreements
- Underpinning Contracts
- Operational Level Agreements
- Internal Policies

CONTROL:
- Organize
- Create Management Framework
- Allocate Responsibilities

EVALUATE:
- Internal audits
- External audits
- Self Assessments
- Security incidents

IMPLEMENT:
- Improve awareness
- Classification and management resources
- Personal Security
- Physical Security
- Security management of hardware, networks, applications, etc...
- Access Control
- Resolve security incidents

ITSM PDCA
Continuous Improvement
MANDATORY FOR ISO/IEC 27001 CERTIFICATION & REGISTRATION
Information Life Cycle

Characteristics:
* Multiple collection points
* Huge variance in applied technologies
* Multiple decision points, including: need and/or authorization to collect, delete, share, secure, audit, dispose, archive, consolidate, disclose, change
ICFR¹ Documentation

¹ Internal Controls over Financial Reporting
ISO/IEC 27001 - Information Security Management System is established through **mandatory conformance** to clauses:

* 4.2.1.(a). Establish Scope
* 4.2.1.(b). Establish Policy
* 4.2.1.(c). Establish Risk Assessment Practice
* 4.2.1.(d). Identify assets/threats/vulnerabilities/impacts
* 4.2.1.(e). Facilitate Risk Assessment
* 4.2.1.(f). Establish Risk Treatment Plan
* 4.2.1.(g). Control Selection practice
* 4.2.1.(h). MRC approval for residual risk
* 4.2.1.(i). MRC approval to establish ISMS
* 4.2.1.(j). MRC approval for Statement of Applicable

5. Establish/Communicate Managements Responsibility

6. Establish Audit/Assessment Practice

7. Establish Management Review Committee (MRC)

8.1. Establish Continuous Improvement practice

8.2. Establish Corrective Action plan practice

8.3. Establish Preventative Action plan practice

**ISMS should not be confused with ISO27k annex “A” control objectives**
ITIL/ITSM vs ISO/ISMS
ISMS Goals

• Mitigate threats and risks to the Confidentiality, Integrity and Availability of Assets including information, people, property, systems/software, hardware, telecommunications to acceptable level.

• Improve the effectiveness and efficiency of Information Security Management.

• Improve effectiveness and efficiencies of existing information security mechanisms.

• Improve reassurance testing and validation outcomes by Internal Audit and External Auditors.

• Mitigate and/or eliminate the likelihood that an accidental incident could have an adverse affect on BC Government.
IT Security Management has two primary objectives that fit perfectly with the ISMS Goals:

1). To meet the security requirements of SLA’s and external requirements further to contracts, legislation and external imposed policies.

2). To provide a basic level of security, independent of external requirements.
Program “Inputs/Outputs”
**“Inputs”**

**ITSM - Inputs:** SLA, OLA, Information Security Policy, Statutes, Regulations

**ISMS - Inputs:**

a). results of ISMS audits and reviews;
b). feedback from interested parties;
c). techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;
d). status of preventive and corrective actions;
e). vulnerabilities or threats not adequately addressed in the previous risk assessment;
f). results from effectiveness measurements;
g). follow-up actions from previous management reviews;
h). any changes that could affect the ISMS; and,
i). recommendations for improvement.
“Outputs”

**ITSM - Outputs:** SLA status pertaining to Security Management Metrics, Exceptions, routine security planning, ISMS Management Review Committee

**ISMS - Outputs:**

a). Improve the effectiveness of ISMS;

b). Update the risk assessment and risk treatment plan;

c). Modification of practices and controls that effect information security, as necessary, to respond to internal or external events that may impact the ISMS, including changes to:

1). business requirements;  
2). security requirements;  
3). business processes effecting the existing business requirements;  
4). regulatory or legal requirements;  
5). contractual obligations; and,  
6). levels of risk and/or criteria for accepting risks.

d). Resource needs;

e). Improvement on how the effectiveness of controls is being measured.
“Integration”
ITSM Integration Points

- Configuration Management
- Incident Management
- Problem Management
- Change Management
- Release Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Service Level Management
ITSM - Integration: The creation and maintenance of a Change Management DataBase (CMDB) comprised of individual records of assets also known as Configuration Items (CI). This classification links the CI with specified security practices and standards. This classification takes into consideration requirements for confidentiality, integrity and availability based on business requirements for compliance with statutory, regulatory and contractual obligations. These requirements are determined as the result of risk assessments like the TRA, PIA and BIA.

ISMS - Integration: A.7.1.1 All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. A.7.2.1 Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. A.7.2.2 An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
# Configuration Management

## Continuous Improvement Framework

<table>
<thead>
<tr>
<th>PLAN</th>
<th>GOVERNANCE</th>
<th>ASSET INVENTORY</th>
<th>ASSET VALUATION</th>
<th>RISK MANAGEMENT</th>
<th>INFORMATION CLASSIFICATION</th>
<th>DATA SENSITIVITY</th>
<th>FACTUAL THREATS &amp; RELATIVE VULNERABILITIES</th>
<th>BUSINESS IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Configuration Management Table

| Asset ID | Portfolio | Department | Risk | Cost of Price | Contingency | Likelihood | Impact | Affects | Analysis | Final Consequence | Impact if Compromised |
|----------|-----------|------------|------|--------------|-------------|------------|--------|---------|----------|----------|---------------------|-----------------------|
| G1       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G2       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G3       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G4       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G5       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G6       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G7       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |
| G8       | Executive | Company    | High | No            | Low         | High       | High   | High    | High     | Uncompromised    | Not Applicable         |

## Key

- **P** - Private
- **C** - Confidential
- **O** - Operational
- **PUB** - Public

## Abbreviation Definition Description

- **LS** - Loss of Service: The compromise results in the application, information, function or service is not being available for use.
- **FL** - Financial Loss: A breach of information security results in direct financial loss, i.e. ID Theft, marketplace competitive advantage loss.
- **LE** - Loss of Employment: A breach of information security results in loss of employment directly, i.e. Orginalization loses customers and has to cut employe.
- **LI** - Legal Implications: A breach in information security results in either civil or criminal litigation, i.e. an employee stole personal information and/or Organizational was found guilty of not providing adequate data protection or due diligence and a standard of care expected by a reasonable person.
- **LT** - Loss of Trust: A breach of information security results in loss of trust in Organizational which results in customers and clients withdrawing the money and services.
- **LL** - Loss of Life: A breach of information security results in loss of human life. I.e. inadequate safeguards put in place to protect mail handlers result in a death from mail bomb or poisoned substance.
- **II** - Injury to Individuals: A breach of information security results in a safety issue which results in injury to individuals or staff. I.e. An employee working alone at night or on the weekend in the Organizational building is assaulted.
- **LP** - Loss of Privacy: A breach of information security results in the loss of privacy of an individual or staff, i.e. ID Theft, Money laundering, etc.
- **LR** - Loss of Reputation: A breach of information security results in the loss of public reputation. I.e. Loss of reputation could lead to loss of clients, customers, financial losses, market place competitive advantage losses.
Corrective/Preventative Actions

Within the following example 57% of the 110 reported information security incidents affected the information security principle “Availability”, while only 8% affected “Confidentiality” and 45% affected “Integrity”. The real surprise was the high rate of incidents impacting “integrity”.
ITSM - Integration: Incident Management is an important process for reporting security incidents. Information security incidents are not clearly understood by most business people, so it is very likely that information security incidents may be handled through a different practice other than incident management. It is therefore essential that Incident Management recognize security incidents as such. Any incident that may interfere with achieving the SLA security requirements is classified as a security incident by ITSM. It is useful to include a description in the SLA of the type of incidents to be considered as security incidents. In addition, any incident that interferes with achieving the basic internal security level is also classified as a security incident.
ISMS - Integration: A.13.1.1 Information security events shall be reported through appropriate management channels as quickly as possible.
Problem Management

**ITSM - Integration:** Problem Management is responsible for identifying and solving structural security failings. The resolution of a problem could introduce a new security risk which is why, Problem Management must involve Security Management during the resolution of the problem. This certification should be based on compliance with the SLA and organizational security requirements.
Corrective/Preventative Management

ITSM - Integration:

Corrective action - 8.2 The documented procedure for corrective action shall define requirements for:
a) identifying nonconformities;
b) determining the causes of nonconformities;
c) evaluating the need for actions to ensure that nonconformities do not recur;
d) determining and implementing the corrective action needed;
e) recording results of action taken (see 4.3.3); and
f) reviewing of corrective action taken.

Preventive action - 8.3 The documented procedure for preventive action shall define requirements for:
a) identifying potential nonconformities and their causes;
b) evaluating the need for action to prevent occurrence of nonconformities;
c) determining and implementing preventive action needed;
d) recording results of action taken (see 4.3.3); and e) reviewing of preventive action taken.
Corrective/Preventative Management

**ISMS - Integration:**
- 8.2 Corrective action and
- 8.3 Preventive action

*MANADATORY FOR ISO/IEC 27001 CERTIFICATION & REGISTRATION*
Continuous Improvement

Risk is measured in terms of High, Med, Low

Impact is accessed against the principles of information security, Confidentiality, Integrity and/or Availability

MANADATORY FOR ISO/IEC 27001 CERTIFICATION & REGISTRATION
Continuous Improvement

Risk is measured in terms of High, Med, Low

Impact is accessed against the principles of information security, Confidentiality, Integrity and/or Availability

Project Managers facilitate a control self assessment and the security and privacy office follows up.

If the balance between the number of active projects and impact/risk is relative then generally projects continue without direct involvement of the security and privacy office.
Change Management

**ITSM - Integration:** Change Management activities are often closely associated with security because Change Management and Security Management are interdependent. There are a number of standard operations to ensure that this security is maintained including the Request For Change (RFC) associated with governance for acceptance. The RFC should also include a proposal for dealing with security issues and based on the SLA requirements Preferably, the Security Manager (and possibly the customer’s Security Officer) should be a member of the Change Advisory Board (CAB).
Release Management

**ITSM - Integration:** All new versions of software, hardware, data communications equipment, etc… should be controlled and rolled out by Release Management. This process will ensure that:

* The correct hardware and software are used
* The hardware and software are tested before use
* The introduction is correctly authorized using change control
* The software is legal
* The software is free from viruses and that viruses are not introduced during distribution
* The version numbers are known and recorded in the CMDB by Configuration Management
* The rollout is managed effectively
ISMS - Integration: A.10.1.2 Changes to information processing facilities and systems shall be controlled. A.10.1.4 Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.
**ITSM - Integration:** Availability Management addresses the technical availability of IT components in relationship to the availability of the service. The quality of availability is assured by continuity, maintainability and resilience. Availability Management is the most important process related to the information security principle, availability and the availability of information assets. As many security measures benefit both availability and the security principles confidentiality and integrity, effective coordination of measures between Availability Management, IT Service Continuity Management, and Security Management is essential.
**ITSM - Integration:** Capacity Management is responsible for the best use of IT resources, as agreed with the customer. The performance requirements are based on the qualitative and quantitative standards defined by Service Level Management. Almost all the activities of Capacity Management affect availability and therefore also Security Management.
Capacity Management

**ISMS - Integration:** A.10.10.5 Faults shall be logged, analyzed, and appropriate action taken. A.14.1.1 A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
ITSM - Integration: IT Service Continuity Management ensures that the impact of any contingencies is limited to the level agreed with the customer. Contingencies need not necessarily turn into disasters. The major activities and defined, maintained, implemented, and testing the contingency plan, and taking preventative action. Because of security aspects, there are ties with Security Management. On the other hand, failure to fulfill basic security requirements may be considered itself contingency.

BS25999 – scheduled for adoption as ISO/IEC 27032
ISMS Business Continuity

SERVICE REQUIRES INFORMATION TO FUNCTION

BUSINESS DRIVERS
“CUSTOMERS DEMAND
NEW SERVICES AND
IMPROVEMENTS TO
EXISTING SERVICES”

REQUIREMENTS
To deliver these services we’ll need specific information gathered and stored, maintained, processed and exchanged

TECHNOLOGY
+ TELECOMMUNICATIONS
+ BUSINESS SYSTEMS
+ HARDWARE
+ SKILLED LABOR

To deliver these services we’ll need business systems created in a program language to ensure consistent and effective processing. We’ll also need reliable hardware and telecommunication suitable for the requirements and skilled people/resources to write code, trouble shoot administer security, patching/fixes, configure systems, configures communications, build in redundancy

MANADATORY FOR ISO/IEC 27001 CERTIFICATION & REGISTRATION
Service Level Management
ITSM - Integration: Service Level Management ensures that agreements about services to be provided to customers are defined and achieved. The Service Level Agreements should also address security measures. The objective is to optimize the level of service provided. Service Level Management includes a number of related security activities, in which Security Management plays an important role:

(a). Identification of the security needs of the customers. Naturally, determining the security needs is the responsibility of the customer as these needs are based on their business interests verifying the feasibility of the customer’s security requirements

(b). Proposing, discussing and defining the security level of IT services in the SLA Identifying, developing and defining the internal security requirements for IT services through OLA

(c). Monitoring the security standards defined within OLA

(d). Reporting on the IT services provided
Organizational Security and Privacy group will assist Managers by reviewing and recommending amendments to contracts and agreements to ensure they address information security and privacy obligations as outlined within data protection statutes (PIP Act, PIPED Act, and FOIPP Act). Some of these provisions may include the following:

- Disclosure of Personal Information
- Annual Compliance Certificate
- Ownership and Control of Personal Information
- Privacy Strategy/Plan
- Training/Awareness
- Risk Assessments (PIA, TRA, CSA)
- Testing and Development Work
- Removal of Personal Information
- Destruction of sensitive information and media Containing sensitive information

- Physical and Environmental Security
- Security standards for sensitive Databases
- Transmission and Back-ups of Personal Information
- Information handling for Database/Media
- System Logs, Audit Logs
- Breach or Demand Notification
- Security Controls for Authorized Personnel
- Agreements with contractors/service providers
- US based companies
- Sensitive information sharing
- Collection of Personal Information
- Non-Compliance Reports
### Service Catalogue

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management/Governance</td>
<td>Manage the Information Security Management System to determine its effectiveness by reviewing policy objectives, scope, security controls, taking into account risk assessments, threats, regulatory and contractual obligations, security audits, incidents, effectiveness measurements, suggestions and feedback, updating security plans and formally recording actions and events.</td>
</tr>
<tr>
<td>Security Policy</td>
<td>Manage the information security policy in accordance with business requirements and relevant laws and regulations.</td>
</tr>
<tr>
<td>Security Risk Management</td>
<td>Manage risk to information assets and system resources, identifying risks, evaluating risks, evaluating treatment, selecting controls, and obtaining management approval.</td>
</tr>
<tr>
<td>Security Risk Treatment</td>
<td>Manage a Risk Treatment Plan that lists organizational assets and identifies threats, vulnerabilities and safeguards selected by management to remediate residual risk.</td>
</tr>
<tr>
<td>Security Continuous Improvement</td>
<td>Manage a Continuous Improvement plan that identifies corrective and preventative action plans designed to improve existing information security policies, practices and standards.</td>
</tr>
<tr>
<td>Privacy Impact Assessment</td>
<td>Manage the Privacy Impact Assessment process to establish compliance with data protection statutes and identify any potential gaps for remediation.</td>
</tr>
<tr>
<td>Threat-Risk Assessment</td>
<td>Manage the Threat-Risk Assessment process to identify threats and risks to information assets and systems resources to identify residual risk and recommend safeguards designed to remediate any potential gaps.</td>
</tr>
<tr>
<td>SERVICE LEVEL AGREEMENT</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>SERVICE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>Security Management</td>
<td>Manage the Information Security Management System to determine its effectiveness by reviewing policy objectives, scope, security controls, taking into account risk assessments, threats, regulatory and contractual obligations, security audits, incidents, effectiveness measurements, suggestions and feedback, updating security plans and formally recording actions and events.</td>
</tr>
<tr>
<td></td>
<td>• Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>• Asset Management</td>
</tr>
<tr>
<td></td>
<td>• Human Resource Security</td>
</tr>
<tr>
<td></td>
<td>• Physical and Environmental Security</td>
</tr>
<tr>
<td></td>
<td>• Communications and Operations Management</td>
</tr>
<tr>
<td></td>
<td>• Access Control</td>
</tr>
<tr>
<td></td>
<td>• Information Systems Acquisition, Development and Maintenance</td>
</tr>
<tr>
<td></td>
<td>• Information Security Incident Management</td>
</tr>
<tr>
<td></td>
<td>• Business Continuity Management</td>
</tr>
<tr>
<td></td>
<td>• Statutory, Regulatory &amp; Contractual Compliance</td>
</tr>
</tbody>
</table>
Key Performance Indicators

• If the risk rating equals “High” for Internet facing system then “Immediate” action is require.

• If the risk rating is “high” for an internal system then a resolution must be applied within “7 days”, all other systems must be have 60 days to remediate;

• If the risk rating equals “Medium” for Internet facing systems then remediation is required within “7 days”.

• If the risk rating is “Medium” for an Internal system then remediation is required within “60 days”. All other systems have a 90 day time span to remediate gaps in security;

• If the risk rating is “Low” for Internet facing system then remediation is required within “30 days”.

• If the risk rating is “Low” for an Internal system then remediation is required within “180 days”.

• All other systems have up to 18 months for remediation or until the next maintenance cycle, whichever is first.
**Contractual Obligations**

**ISMS - Integration:** A.15.1.1 All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.

---

<table>
<thead>
<tr>
<th>Priority</th>
<th>Section</th>
<th>Detail</th>
<th>ISMS Reference (ISO/IEC 27001)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.2</td>
<td>Access control</td>
<td>Implement controls to ensure the confidentiality of information</td>
<td>ISO 11799</td>
</tr>
<tr>
<td>1.1.1.4</td>
<td>Data classification</td>
<td>Information handling procedures (backup, encryption, etc.)</td>
<td>ISO 11799</td>
</tr>
<tr>
<td>1.1.1.5</td>
<td>Data classification / Policy development</td>
<td>Classification schemes (public, operational, personal, confidential)</td>
<td>ISO 11799</td>
</tr>
<tr>
<td>1.1.1.6</td>
<td>Personnel screening</td>
<td>Contractor screening</td>
<td>ISO 11799</td>
</tr>
<tr>
<td>1.1.1.7</td>
<td>Personnel screening</td>
<td>Security responsibilities in role descriptions</td>
<td>ISO 11799</td>
</tr>
<tr>
<td>1.1.1.8</td>
<td>Systems development</td>
<td>Security environment of new development projects and changes to existing systems</td>
<td>ISO 11799</td>
</tr>
<tr>
<td>1.1.1.9</td>
<td>Third party reviews / Policy development</td>
<td>Vendor assessment policy and requirements</td>
<td>ISO 11799</td>
</tr>
</tbody>
</table>

**MANADATORY FOR ISO/IEC 27001 CERTIFICATION & REGISTRATION**
Reporting
**ITSM - Integration:** Customer Service Reports must be provided at the intervals agreed in the SLA. These reports compare the agreed service levels and the service levels that were actually measured. Examples include the following:

- availability and downtime during a specific period
- average response times during peak periods
- transaction rates during peak periods
- number of functional areas
- frequency and duration of service degradation
- average number of users at peak periods
- number of successful and unsuccessful attempts to circumvent security
- proportion of service capacity used
- number of completed and open changes
- cost of service provided
ITSM Reports

**ITSM - Integration:** Management reports, in contrast to service level reports, are not for the customer, but to control or manage the internal process. They may contain metrics about actual service levels supported, and trends such as:

* total number of SLA in the pool
* number of times SLA was not fulfilled
* cost of measuring and monitoring the SLA
* customer satisfaction, based on survey/complaints
* statistics about incidents, problems, and changes
* progress of continuous improvement action plans
ISMS Reporting

ISMS - Integration: Compliance Management, Asset Management, Risk Treatment Management, Continuous Improvement, TRA, PIA, CSA, etc…

ISMS Data Base Flowchart Explained

Sample Quarterly Information Security Management System Performance Metric

C-I-A Criticality

<table>
<thead>
<tr>
<th>Category</th>
<th>H</th>
<th>M</th>
<th>L</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>$37,000,000.00</td>
</tr>
<tr>
<td>Threats</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>$2,700,000.00</td>
</tr>
<tr>
<td>Statutory, Regulatory Compliance</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>$1,200,000.00</td>
</tr>
<tr>
<td>Contractual Compliance</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>$1,200,000.00</td>
</tr>
<tr>
<td>Controls enforced</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>$750,000.00</td>
</tr>
<tr>
<td>Risk Assessments</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>$300,000.00</td>
</tr>
<tr>
<td>Incidents</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>$700,000.00</td>
</tr>
<tr>
<td>Corrective Actions plans</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>$200,000.00</td>
</tr>
<tr>
<td>Preventative Actions plans</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>$13,500,000.00</td>
</tr>
<tr>
<td>Continuous Improvement</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$19,800,000.00</td>
</tr>
</tbody>
</table>

MANADATORY FOR ISO/IEC 27001 CERTIFICATION & REGISTRATION
Conclusion
Both information security programs are based on excellent Quality Management frameworks.

ITSM is an excellent operational level security management framework which effectively positions the information security office as a direct contributor to service delivery.

ISMS is also an excellent advisory level security management framework that effectively positions the information security office as an impartial, independent governing body over organizational information security.

Appropriately implemented and integrated into existing operational program both ITSM and ISMS could be combined to establish an extremely effective information security posture for almost any organization.

However, in my own personal opinion ISMS has the most potential upside due to its visibility and independence it is the ultimate marketing tool that provides a high degree of trust and confidence with partners, clients and ultimately customers.
Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

Credit Union Central of British Columbia
1441 Creekside Drive
Vancouver
British Columbia
V6J 4S7
Canada

Holds Certificate No:  IS 523384
and operates an Information Security Management System which complies with the requirements of IS
the following scope:

The provision of secure and managed internet banking services to credit unions, banks,
other financial institutions, and third-party businesses from its office in Vancouver,
British Columbia.
This is in accordance with the Statement of Applicability dated November 20, 2007.
Feedback
## Evaluation

### Presentation Evaluation

<table>
<thead>
<tr>
<th>Instructor Name</th>
<th>[Name]</th>
<th>Status</th>
<th>[Role]</th>
<th>[Phone]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Date</td>
<td>[Date]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>BRITISH COLUMBIA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instructions</td>
<td>We would appreciate your feedback on today's presentation as we continue to improve the effectiveness of our materials and delivery. Please assess today's presentation using the following assessment criteria: 1 = Disagree, 2 = Somewhat agree, 3 = Agree, 4 = Strongly agree, 5 = Completely agree. Additional comments may be added to further supplement your response. Thanks in advance for your comments and participation in today's session.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Did you find the presentation topic useful?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>1 = Disagree, 2 = Somewhat agree, 3 = Agree, 4 = Strongly agree, 5 = Completely agree.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Was the information shared through the presentation clear?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>1 = Disagree, 2 = Somewhat agree, 3 = Agree, 4 = Strongly agree, 5 = Completely agree.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Was the speaker able to provide useful information that linked the presentation topic to current roles, responsibilities and practices?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>1 = Disagree, 2 = Somewhat agree, 3 = Agree, 4 = Strongly agree, 5 = Completely agree.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>At the end of this presentation, are you leaving with an improved understanding of the topic?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>1 = Disagree, 2 = Somewhat agree, 3 = Agree, 4 = Strongly agree, 5 = Completely agree.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>At the end of this presentation will you be able to apply your new knowledge to the work you do today?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>1 = Disagree, 2 = Somewhat agree, 3 = Agree, 4 = Strongly agree, 5 = Completely agree.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Contact Information:** If you'd like a response to any of your comments above please include your name & contact information.

| Contact Name | |
| Contact Information | |
Questions

Mark E.S. Bernard,
CGEIT, CISM, CISA, CISSP, ISO27K LA, PM, COBiT/ITIL Foundation,
Manager, Compliance Assessment and Reporting, OCIO,
Phone: (250) 953-4565
E-Mail: mark.bernard@gov.bc.ca