An Introduction to the ISO Security Standards
Agenda

- Security vs Privacy
- Who or What is the ISO?
- ISO 27001:2013
- ISO 27001/27002 domains
Building Blocks of Security

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

CONFIDENTIALITY

INTEGRITY

Confidentiality

Availability

Integrity
Building Blocks of Privacy

- Confidentiality
- Availability
- Integrity
- Limited Collection
- Limited Use
- Defined Purpose
- Limited Retention
- Limited Disclosure
- Consent
- Accountability
- Confidentiality
- Integrity
- Availability

#PrivSymposium
Security and Privacy

CONFIDENTIALITY
INTEGRITY
AVAILABILITY

DEFINED PURPOSE
CONSENT
LIMITED
COLLECTION
LIMITED USE
LIMITED
DISCLOSURE
LIMITED
RETENTION
ACCOUNTABILITY

#PrivSymposium

www.privacyassociation.org/symposium
## Security and Privacy

<table>
<thead>
<tr>
<th></th>
<th><strong>SECURITY</strong></th>
<th><strong>PRIVACY</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Philosophy</td>
<td>Concept of safety</td>
<td>Concept of choice</td>
</tr>
<tr>
<td>Data Protection</td>
<td>How</td>
<td>Why</td>
</tr>
<tr>
<td>Protected by Law</td>
<td>Not in Canada</td>
<td>PIPEDA and others</td>
</tr>
<tr>
<td>Customer interaction</td>
<td>Limited</td>
<td>Privacy statement</td>
</tr>
<tr>
<td>Organizational location</td>
<td>Most often in IT</td>
<td>Most often in legal</td>
</tr>
<tr>
<td>Tools</td>
<td>Primarily technical</td>
<td>Process oriented</td>
</tr>
<tr>
<td>Response to an incident</td>
<td>Contain, eradicate and correct</td>
<td>Notification</td>
</tr>
</tbody>
</table>

Security is a process….privacy is a consequence  
(Rebecca Herold)

#PrivSymposium

www.privacyassociation.org/symposium
International Organization for Standardization (ISO)

- World’s largest developer of voluntary international standards
- Benefits
  - Safe, reliable and quality of products and services
  - Minimizes waste and increases productivity
  - Levels the playing field for developing countries
  - Facilitates free and fair global trade
- Standards cover almost all aspects of technology and business
ISO 270000 Series

- The information security family of standards
- Over 30 published and/or planned standards
- Joint technology committee of ISO and IEC

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27000</td>
<td>Overview, introduction and glossary of terms for the 27000 series</td>
</tr>
<tr>
<td>27001</td>
<td>Requirements standard for an ISMS</td>
</tr>
<tr>
<td>27002</td>
<td>Code of practice for 27001 standards</td>
</tr>
<tr>
<td>27003</td>
<td>Guidance on implementing 27001</td>
</tr>
<tr>
<td>27004</td>
<td>Guidance on measurements of the ISMS program, including suggested metrics</td>
</tr>
<tr>
<td>27005</td>
<td>Risk management</td>
</tr>
<tr>
<td>27006</td>
<td>Guide to the ISO27000 certification process</td>
</tr>
<tr>
<td>27007/008</td>
<td>Guide to auditing the ISMS program and controls</td>
</tr>
</tbody>
</table>
ISO/IEC 27001:2013

“.... specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature.”

Source: www.iso.org
ISO/IEC 27001:2013

• Requires that management
  – Systematically examine security risks
  – Design and implement controls
  – Adopt an overarching management process.

• Organizations can adapt by considering
  – Internal and external issues
  – Requirements of interested parties
  – Interfaces and dependencies between activities within the organization and with other organizations
Key Benefits

- Provides an opportunity to systematically identify and manage risks
- Allows an independent review of information security practices
- It provides a holistic, risk-based approach to secure information
- Demonstrates credibility to stakeholders
- Demonstrates security status according to internationally accepted criteria
- Creates a market differentiation
- Certified once - accepted globally
Domains of ISO27001

- System Acquisition
- Organization
- Human Resources
- Asset Management
- Access Control
- Cryptography
- Physical Security
- Operations
- Communication
- Policy
- System Acquisition
- Cybersecurity
- Compliance
- Business Continuity
- Supplier Relationships
- Incident Management
Domains of ISO27001-Trust

- Policy
- Access Control
- Communication
- Organization
- Cryptography
- System Acquisition
- Business Continuity
- Human Resources
- Physical Security
- Supplier Relationships
- Compliance
- Asset Management
- Operations
- Incident Management
Cryptography (Trust)

• The process of reading and writing secret messages

• Cryptography should exist where appropriate

• Cryptography keys should be managed
Business Continuity (Trust)

- BCP / DRP
- Focus on business needs
- Organization has documented plans in place
- Plans should be tested and reviewed on a regular basis
- Redundant facilities where appropriate
Operations (Trust)

• This is the “geeky” side of IT Security
• Virus protection
• Backups
• Audit logs
• Vulnerability management
• Segregation of dev, test and production environments
Communications – Network (Trust)

- Network security – more “geeky stuff”
  - Firewalls
  - Routers
  - Segregated networks where appropriate
  - Security of network even if supplied by third party
Asset Management (Trust)

• All assets accounted for
  – Assigned owner
  – Inventory
  – Collecting assets when employees leave
  – Standards for acceptable use of assets

• Process for media handling
  – Management of removable media
  – Process for destroying media
Domains of ISO27001- Parallel

- Organization
- Human Resources
- Asset Management
- Access Control
- Cryptography
- Physical Security
- Operations
- System Acquisition
- Supplier Relationships
- Incident Management
- Communication
- Business Continuity
- Compliance

#PrivSymposium

www.privacyassociation.org/symposium
Security Policy (Parallel)

• A documented policy must exist
  – Appropriate
  – Approved
  – Available
  – Reviewed on a regular basis or as changes occur
Security Organization (Parallel)

- Roles and responsibilities for those involved in security are defined
- Contacts with external parties are established
- Security requirements are built into projects
- Mobile device policy and procedures
- Teleworking policy and procedures
Domains of ISO27001 - Cooperate

- Policy
- Access Control
- Communication
- Organization
- Cryptography
- System Acquisition
- Business Continuity
- Human Resources
- Physical Security
- Supplier Relationships
- Operations
- Incident Management
- Compliance

#PrivSymposium

www.privacyassociation.org/symposium
Human Resources (Cooperate)

- Contractual agreements with employees
- Background screening
- Awareness
- Disciplinary process
- Termination procedures
Access Control (Cooperate)

- Simple passwords to biometrics
- Users are required to follow access controls
- Formal procedures for access management
- Management of privileged access
- Regular reviews of access
Physical Security (Cooperate)

- Secure perimeters and work areas are in place
- Protection of equipment
  - From environmental risks
  - When unattended
  - When taken off site
- Protection of cabling
- Clean desk policy
Supplier Relationships (Cooperate)

• Written agreements are in place
• Security requirements are established for third parties
• Regular reviews and audits of third parties
There are documented procedures for an incident
- Includes how to recognize an incident
- Includes roles and responsibilities
- A formal learning process is in place to learn from incidents
Domains of ISO27001 - Lead

- POLICY
  - ACCESS CONTROL
  - COMMUNICATION
- ORGANIZATION
- CRYPTOGRAPHY
- SYSTEM ACQUISITION
- BUSINESS CONTINUITY
- HUMAN RESOURCES
- PHYSICAL SECURITY
- SUPPLIER RELATIONSHIPS
- OPERATIONS
- ASSET MANAGEMENT
- INCIDENT MANAGEMENT
- COMPLIANCE

#PrivSymposium
Incident Management (Lead)

- There are documented procedures for an incident
  - Includes how to recognize an incident
  - Includes roles and responsibilities
  - A formal learning process is in place to learn from incidents
Asset Management - Classification (Lead)

- All information / data should be inventoried and classified
- Data flows
- Most common classification scheme is 3 or 4 layers
  - Privacy of data should be included in the classification scheme
- Private data mixing with non private data – makes the data private
Communications – Transfer (Lead)

• Movement of Data
  – Within the organization
  – External to the organization
  – Includes all kinds of transfer mechanisms

• Formal agreements are in place
• Formal procedures are in place
System Acquisition, Development & Maintenance (Lead)

- Security is built into applications
- New software is tested for security bugs and flaws
- Appropriate change management processes in place
- Test data is protected
Compliance (Lead)

- Contract requirements are documented
- Regulatory requirements are documented
- Privacy will be ensured per applicable regulatory and business needs
- Audits conducted on a regular basis
## Summary

<table>
<thead>
<tr>
<th>ISO 27001 Domain</th>
<th>Lead</th>
<th>Cooperate</th>
<th>Parallel</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Management</td>
<td></td>
<td></td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptography</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Acq, Dev and Mtce</td>
<td></td>
<td>Red</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier Relationships</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td></td>
<td>Red</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity</td>
<td></td>
<td>Purple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td>Red</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions?

Contact Information:
Angela J Carfrael,
AJC Consulting Services
angiecarfrael@yahoo.ca
204-806-6659