Application Security ISO

Tak Chijiiwa, CISSP, CSSLP
Principal Consultant,
Security Compass
Copyright 2012
Introduction
• Tak Chijiwa has 12+ years of IT security experience

• He has been involved in a wide spectrum of information security strategy and advisory engagements for various Fortune 500 clients

• Prior to joining Security Compass, he worked at Deloitte & Touche, LLP as a Manager of the Vulnerability Management team in Toronto, Ontario for 6 years and at Kasten Chase Applied Research as a Development Manager in Mississauga, Ontario for 4 years
Abstract
Abstract

• ISO/IEC 27034 - Part 1 was published in November 2011 and the remaining parts (Part 2-6) are expected to be published soon

• What does this mean to your organization or your clients who wish to adopt or incorporate this ISO standard for their application?

• This overview will walk through the sections of standard and highlight the process approach to specifying, designing, developing, testing, implementing and maintaining security functions and controls in application systems
Agenda
Agenda

1. ISO Series Background
2. ISO Stages
3. ISO 27034 Walkthrough
4. Q&A
ISO Series Background
ISO Series Background

ISO Series Background - continued

• Standards are essential for ensuring interoperability within an IT environment

• Goal is to incorporate the views of all interested parties from manufacturers, vendors and users to research organizations and governments

• ISO 27000 series involves various technical committees, subcommittees, and working groups
ISO Series Background - continued

1. International Organization for Standardization (ISO)

   • Non-governmental consensus-building network of the national standards institutes of 156 countries

   • Do NOT represent governments but closely works with both governments and industries
2. International Electrotechnical Commission (IEC)

- Develops international standards for government, business and society for all electrical, electronic and related technologies
- These standards are relied upon for international commercial contracts and agreements
ISO Series Background - continued

3. Joint Technical Committee 1/Sub-committee 27

- Draft International Standards from joint technical committees from around the world
- Requires approval by at least 75% of the national bodies to publish as an International Standard
- Secretariat is Deutschen Institut für Normung (DIN) in Germany
ISO Series Background - continued

- Within JCT 1/SC 27, there are 5 working groups which further focuses on the elements of IT Security

- Each working group (WG) has been assigned a national secretariat
ISO Series Background - continued

- Objectives of Working Group 4 – Security Controls and Services

**Unknown or emerging information security threats**

**Objective #1:**
- a. Prepare to respond
- b. Ensure continuous monitoring
- c. Reduce risk through identifying and understanding information security threats

**Known or common information security threats**

**Objective #2:**
- a. Manage risks to the environment
- b. Prevent occurrence (likelihood)
- c. Reduce impact from occurrence

**Information security incidents**

**Objective #3:**
- a. Investigate incident and collect facts
- b. Identify who, what, where, why and how
- c. Learn from incident
ISO Series Background - continued

- Current published standards and projects in progress (review or draft)

**Unknown or emerging information security threats**

1. ISO/IEC 27031:2011 (Business Continuity)
2. ISO/IEC FDIS 27032 (Cybersecurity)
3. ISO/IEC 27035:2011 (Incident Management)
4. ISO/IEC WD 27039 (IDS)
5. ISO/IEC 24762:2008 (Disaster Recovery)

**Known or common information security threats**

1. ISO/IEC 27033 (Network Security)
2. ISO/IEC 27034 (Application Security)
3. ISO/IEC 27036 (Supplier Relationships)
4. ISO/IEC 27038 (Digital Redaction)
5. ISO/IEC 27040 (Storage Security)

**Information security incidents**

1. ISO/IEC 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence)
ISO Stages
ISO Stages

• There are various defined stages and sub-stages during the development of International Standards

• Other definitions include:
  • NP = New Work Item Proposal
  • WD = Working draft
ISO Stages - continued

<table>
<thead>
<tr>
<th>STAGE</th>
<th>SUBSTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Preliminary stage</td>
</tr>
<tr>
<td>00.00</td>
<td>Proposal for new project received</td>
</tr>
<tr>
<td>00.20</td>
<td>Proposal for new project under review</td>
</tr>
<tr>
<td>00.60</td>
<td>Close of review</td>
</tr>
<tr>
<td>90</td>
<td>Decision Substages</td>
</tr>
<tr>
<td>90.00</td>
<td>Proposal for new project abandoned</td>
</tr>
<tr>
<td>90.98</td>
<td>Approval to ballot proposal for new project</td>
</tr>
<tr>
<td>90.99</td>
<td>New project approved</td>
</tr>
<tr>
<td>10</td>
<td>Repeal stage</td>
</tr>
<tr>
<td>10.00</td>
<td>Proposal for new project registered</td>
</tr>
<tr>
<td>10.20</td>
<td>Proposal for new project ballot initiated</td>
</tr>
<tr>
<td>10.60</td>
<td>Close of voting</td>
</tr>
<tr>
<td>10.92</td>
<td>Proposal returned to submittor for further definition</td>
</tr>
<tr>
<td>10.98</td>
<td>New project rejected</td>
</tr>
<tr>
<td>10.99</td>
<td>New project approved</td>
</tr>
<tr>
<td>20</td>
<td>Preparatory stage</td>
</tr>
<tr>
<td>20.00</td>
<td>New project registered in TC/SC work programme</td>
</tr>
<tr>
<td>20.20</td>
<td>Working draft (WD) study initiated</td>
</tr>
<tr>
<td>20.60</td>
<td>Close of comment period</td>
</tr>
<tr>
<td>20.98</td>
<td>Project deleted</td>
</tr>
<tr>
<td>20.99</td>
<td>WD approved for publication as CD</td>
</tr>
<tr>
<td>30</td>
<td>Committee stage</td>
</tr>
<tr>
<td>30.00</td>
<td>Committee draft (CD) registered</td>
</tr>
<tr>
<td>30.20</td>
<td>CD study/ballot initiated</td>
</tr>
<tr>
<td>30.60</td>
<td>Close of voting/comment period</td>
</tr>
<tr>
<td>30.92</td>
<td>CD referred back to Working Group</td>
</tr>
<tr>
<td>30.98</td>
<td>Project deleted</td>
</tr>
<tr>
<td>30.99</td>
<td>CD approved for publication as DIS</td>
</tr>
<tr>
<td>40</td>
<td>Enquiry stage</td>
</tr>
<tr>
<td>40.00</td>
<td>DIS registered</td>
</tr>
<tr>
<td>40.20</td>
<td>DIS ballot initiated: 5 months</td>
</tr>
<tr>
<td>40.60</td>
<td>Close of voting</td>
</tr>
<tr>
<td>40.92</td>
<td>Full report circulated: DIS referred back to TC or SC</td>
</tr>
<tr>
<td>40.93</td>
<td>Full report circulated: decision for new DIS ballot</td>
</tr>
<tr>
<td>40.98</td>
<td>Project deleted</td>
</tr>
<tr>
<td>40.99</td>
<td>Full report circulated: DIS approved for publication as FDIS</td>
</tr>
<tr>
<td>50</td>
<td>Approval stage</td>
</tr>
<tr>
<td>50.00</td>
<td>FDIS registered for formal approval</td>
</tr>
<tr>
<td>50.20</td>
<td>FDIS ballot initiated: 2 months. Proof sent to secretariat</td>
</tr>
<tr>
<td>50.60</td>
<td>Close of voting. Proof returned by secretariat</td>
</tr>
<tr>
<td>50.92</td>
<td>FDIS referred back to TC or SC</td>
</tr>
<tr>
<td>50.98</td>
<td>Project deleted</td>
</tr>
<tr>
<td>50.99</td>
<td>FDIS approved for publication</td>
</tr>
<tr>
<td>60</td>
<td>Publication stage</td>
</tr>
<tr>
<td>60.00</td>
<td>International Standard under publication</td>
</tr>
<tr>
<td>60.60</td>
<td>International Standard</td>
</tr>
</tbody>
</table>
ISO 27034 Walkthrough
ISO 27034 Walkthrough

- Part 1: Overview & concepts
- Part 2: Organization normative framework
- Part 3: Application security management process
- Part 4: Application security validation
- Part 5: Protocols and application security controls data structure
- Part 6: Security guidance for specific applications (if needed)
Overview

• Provides guidance for organizations in integrating security into the processes used for managing their applications

• Explicitly takes a process approach to specifying, designing, developing, testing, implementing and maintaining security functions and controls in application systems

• Defines application security not as a state of security but as “a process an organization can perform for applying controls and measurements to its applications in order the manage the risk of using them”
Overview - continued

- ISO/IEC 27034 is **not**:
  - Development standard for software applications
  - Application project management standard
  - Software Development Lifecycle (SDLC) standard

- ISO/IEC 27034 does **not**:
  - Provide guidelines for physical and network security
  - Provide controls or measurements (metrics)
  - Provide secure coding strategies for any programming language
Part 1

ISO/IEC 27034-1:2011 – Overview & concepts

• Published November 21, 2011

• Provides and overview of application security

• Introduces definitions, concepts, principles and processes involved in application security

• Designed to be used in conjunction with other standards in the ISO27000 family
Part 1 - continued

• Applicable to applications:
  1. developed (in-house)
  2. acquired from third parties
  3. where development or operation is outsourced

• The intended use and benefits are highlighted below:

<table>
<thead>
<tr>
<th>Roles</th>
<th>Responsibility</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers</td>
<td>Manage the cost of implementing and maintaining application security</td>
<td>Leverage ISO/IEC 27034 processes to prove that the application has attained and maintained a targeted level of trust</td>
</tr>
<tr>
<td>Developers</td>
<td>Understand what security should be applied at each phase of the application life cycle</td>
<td>Leverage ISO/IEC 27034 processes to identify control points and safety functions to be implemented</td>
</tr>
<tr>
<td>Auditors</td>
<td>Verify controls to prove the application has reached the required level of trust</td>
<td>Leverage ISO/IEC 27034 processes to standardize the application security certification</td>
</tr>
<tr>
<td>End users</td>
<td>N/A</td>
<td>Assurance that it is deemed secure to use the application</td>
</tr>
</tbody>
</table>
Key principles defined for this standard include:

“Security is a requirement”
Requirements should be defined and analyzed for each and every stage of the application's life cycle and managed on a continuous basis.

“Application security is context-dependent”
The type and scope of application security requirements are influenced by the risks associated with the application which come in the form of (1) business; (2) regulatory; and (3) technological.

“Appropriate investment for application security”
Costs for applying Application Security Controls and performing audit measurements should align with the Targeted Level of Trust.

“Application security should be demonstrated”
Auditing process leverage the verifiable evidence provided by Application Security Controls to confirm if it has reached management’s Targeted Level of Trust.
Part 1 - continued

• “Target application level of trust” definition:

  • Confidence level required by the organization using the application

  • Defined when establishing the Organization Normative Framework (ONF)
Part 2

ISO/IEC WD 27034-2 – Organization normative framework

• Standards under development

• Describes the relationships and interdependencies between processes in the Organization Normative Framework (ONF)

• Processes include creating, maintaining and adapting it to the organization’s needs and contexts (e.g. business, regulatory, technological)
Part 2 - continued

- Describes how to implement an Application Security Management Process (ASMP) for an organization

1. Establish an Organizational Normative Framework (ONF)
   It will contain regulations, laws, best practices, roles & responsibilities accepted by the organization.

2. Application Security Risk Management (ASRM)
   Obtain the organization’s approval on a target level of trust through specific application-oriented risk analysis.

3. Application Normative Framework (ANF)
   Identify the relevant elements from the ONF which are applicable to the target business project.

4. Business Application Project
   Implement the security activities contained in the ANF.

5. Application Security Verification
   Verify and provide evidence that an application has reached and maintained the targeted level of trust.
Part 3

ISO/IEC NP 27034-3 – Application security management process

- Standards under development

- Considered to be widely applicable and useful to organizations dealing with application security

- Describes information security relevant processes within an application development project

- Attempts to highlight process relationships and interdependencies
Part 4

ISO/IEC NP 27034-4 – Application security validation

- Standards under development
- Describes application security certification and validation processes
- Methods for assessing and comparing the Level of Trust against information security requirements
Part 5

ISO/IEC NP 27034-5 – Protocols and application security controls data structure

• Standards under development (preliminary text released recently ~April 2012)

• Defines the Application Security Control (ASC) data structure

• Electronic business eXtensible Markup Language (ebXML) designated as the format to establish libraries of reusable security functions that may be shared both within and between organizations
• An Application Security Control (ASC) may satisfy various aspects of information security
Part 6

ISO/IEC NP 27034-6 – Security guidance for specific applications (if needed)

- Standards under development and may be considered for inclusion

- Identifies Application Security Controls corresponding to “specific application security requirements” (if applicable)

- For example:
  - N-Tier and web applications security
  - Client/Server applications security
Considerations

• The requirements and processes specified in ISO/IEC 27034 are **not** intended to be implemented in isolation but rather integrated into an organization's existing processes

• Annex A of ISO/IEC 27034-1 presents a case study on how to **map** an existing software development process to some of the components of ISO/IEC 27034 (to reduce overall effort to conform with this standard)
Q&A
Thank you!

tak@securitycompass.com
Security Compass

Please let me know your comments and thoughts!