constructing an
ISO/IEC 27001 ISMS
for the
Federal PKI Management Authority
so as to achieve
NIST RMF compliance

Richard G. Wilsher
Zygma LLC

ACSAC 2008-12-11
Σ the Federal Public Key Infrastructure (FPKI) Policy Authority (PA) needs to have assurances as to the security measures in place with other PAs with which it wishes to cross-certify

Σ these other PAs could be from:
- industry
- government
- in and beyond the USA

Σ assurance as to their respective infosec operations needs to be based upon a common reference

Σ the FPKI PA has determined that this shall be accomplished by the FPKI Management Authority (FPKI MA) implementing and operating an ISO/IEC 27001-conformant information security management system (ISMS)
FISMA compliance

accomplished through adherence to NIST’s Risk Management Framework

- NIST Federal Information Processing Standards (FIPS) 199 & 200
- NIST Special Publications (SP) 800-37, -39, -53, -53A, -60, ...

applies also to contractors to the Federal Government

NIST FIPS 199, 200, …

NIST SP 800-37, -39, -53, -53A, -60, …
broader challenges

- numerous Federal directives, regulation, standards, policies, to which agencies, departments and contractors have to be compliant
- FISMA has lower value/recognition in the commercial sector
- this even more so, concerning international recognition
- many agencies and contractors undergoing multiple assessments (FISMA, WebTrust, SysTrust, tScheme, ...)
- Federal PKI needs to enjoy mutual recognition of its infrastructure with other national and with international bodies
how can FPKI MA resolve this?

- if FISMA requirements can be met, IS 27001 Certification carries wider recognition
- ISMS has a more workable approach to showing compliance with other regulations, standards, etc. (more open, flexible)
- IS 27001 is therefore an attractive solution for other parties, leading to a common basis for mutual recognition
what are the benefits?

- reduction of audit management and technical complexity, economies in time and money
- combining will reduce the total workload where both FISMA and ISMS are required
- if adopted by NIST then:
  - dual qualification of assessors needn’t be required
  - minimises set-up costs for new scheme
  - minimal/no additional training costs
  - lower cost per assessment
- NIST is onboard and fully aware of these efforts
Focuses on a **system**, looks outward at its management environment.

Focuses on the **security management**, looks inward at the **systems within scope**.
differences – scope & coverage

- NIST RMF
- ISO/IEC 27001
- system A
- system B
- system C
- system D
take each IS 27001 normative clause:
- §4 - §8 inclusive (processes)
- Annex A (security controls)

map to each clause of each Federal reference:
- FISMA
- OMB A-130
- FIPS 199, 200
- SP 800-37, 39, 53*, 53A, 60, 70

*soon to be published by NIST as the amended SP 800-53-1
the problem – NIST document style!

- very discursive
- good content but embedded requirements
- general absence of discrete clauses
- very difficult to assess (and map) against
the solution (continued) –

- content unaltered
- discrete clause references inserted
- commensurate re-structuring/layout
- insertion of cross-references to IS 27001 clauses
- where IS 27001 doesn’t obviously accommodate a FISMA need, build it in
  - Extended Control Set (ECS) principle
3 MINIMUM SECURITY REQUIREMENTS

The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. The seventeen areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems.

Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the federal government and the success of the resulting security measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.

Specifications for Minimum Security Requirements

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
the solution (4) – an example

3.0.2 Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.

### Specifications for Minimum Security Requirements

**ISO/IEC 27001 - clause** | **Commentary**
--- | ---
§4.2.1(c), §4.3.1(a, c, g), §4.3.2 (f, inter alia), §5.1(a), §5.2.1(b) | ‘minimum security requirements’ can be taken to mean the controls set out in the SoA, consistent with the risk assessment.

These are the principle related ISMS processes and control objectives. Others will become apparent in the §3.1.x mappings.

### Specifications for Minimum Security Requirements

**ISO/IEC 27001 - clause** | **Commentary**
--- | ---
See below | The mappings in this group refer to the most obvious applicable ISO/IEC 27001 references. Extensive mappings per control are found in EZP 853.

**3.1.1 Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) that authorized users are permitted to control.
**3.1.1 Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

<table>
<thead>
<tr>
<th>ISO/IEC 27001 clau</th>
<th>Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>§4.2.1(c)</td>
<td>Refer to EZP 853 for a comprehensive mapping for this control group.</td>
</tr>
<tr>
<td>§5.1</td>
<td></td>
</tr>
<tr>
<td>A.5.1.1</td>
<td></td>
</tr>
<tr>
<td>A.5.1.2</td>
<td></td>
</tr>
<tr>
<td>A.6.1.3</td>
<td></td>
</tr>
<tr>
<td>A.8.1.1</td>
<td></td>
</tr>
<tr>
<td>A.9.1.1</td>
<td></td>
</tr>
<tr>
<td>A.9.1.2</td>
<td></td>
</tr>
<tr>
<td>A.9.1.3</td>
<td></td>
</tr>
<tr>
<td>A.11.1.1</td>
<td></td>
</tr>
<tr>
<td>A.11.2.1</td>
<td></td>
</tr>
<tr>
<td>A.11.2.2</td>
<td></td>
</tr>
<tr>
<td>A.11.2.3</td>
<td></td>
</tr>
<tr>
<td>A.11.2.4</td>
<td></td>
</tr>
<tr>
<td>A.11.4.1</td>
<td></td>
</tr>
<tr>
<td>A.11.6.1</td>
<td></td>
</tr>
<tr>
<td>A.11.7.1</td>
<td></td>
</tr>
<tr>
<td>A.11.7.2</td>
<td></td>
</tr>
</tbody>
</table>
the solution (6) –
the Extended Control Set paradigm

Reference
source ‘Δ’

$1.2.3$

$2.3.4(a)$

$2.3.4(b)$

$3.1$

$3.2$

$4.1.1$

$4.2$

Un-mappable

© Zygma LLC 2008
the solution (8) –

Reference source ‘Δ’

§1.2.3

§2.3.4(a)

§2.3.4(b)

§3.1

§3.2

§4.1.1

§4.2

A5 Security Policy

A6 Organization of Infosec

A7 Asset Management

A12 Info.Sys Acq’n …

A15 Compliance

SoA
(from
IS 27001
Annex A)

ECS
(specific to
reference)
### SP53.CM

**Objective:** To ensure that configuration management policy and procedures are in place to fully meet the FISMA requirements.

| SP53.CM.1a | Baseline Configurations | Control:†
The organization shall develop, document, and maintain a baseline configuration for each information system falling within the scope of the ISMS.‡

**Guidance:**
This control should be considered to be a specific extension to A 7.1.1 and A 7.1.2, and is allied closely to SP53.AA.1. The scope of an ISMS may embrace one or more information systems and it is important that the organization maintains a record of the configuration for each of those systems within the ISMS which is accurate, reliable and up-to-date. Refer to SP 800-53 Security Control CM-2.¶

| SP53.CM.2a | Configuration Settings | Control:†
The organization shall establish, document, enforce and regularly review configuration settings for all information technology products employed within each information system falling within the scope of the ISMS. Configuration shall be the most restrictive consistent with operational requirements.¶

**Guidance:**
Refer to SP 800-53 Security Control CM-6.¶

| SP53.CM.3a | Least Functionality | Control:†
The organization shall configure each information system falling within the scope of the ISMS such that it provides only essential capabilities. The use of functions, ports, protocols, and/or services not consistent with operational requirements shall be disabled.¶

**Guidance:**
Refer to SP 800-53 Security Control CM-7.¶

### SP53.CP

**Objective:** To ensure that contingency planning policy and procedures are in place to fully meet the FISMA requirements.

| SP53.CP.1a | Telecommunications Services | Control:†
The organization shall establish service agreements for primary telecommunications and alternate services to enable critical mission/business function continuity when the primary telecommunications capabilities are reduced or unavailable. Agreements shall address how services are switched between primary and alternate providers.¶

**Guidance:**
This control should be seen as a specific instance of A 8.10.2.3.c.†
INTRODUCTION

Objective

This document is the US Federal PKI Operational Authority's ("the OA") “Information Security Management System (ISMS)”. The objective of the ISMS is to empower the OA to manage its information security risks in the operation of the Federal Bridge Certification Authority, including its compliance with the requirements of the US Federal Information Security Management Act 2002.

Contents

This document defines the scope of the ISMS and all applicable QA policies. It defines the context for the Risk Assessment and Risk Treatment Plan and presents the Statement of Applicability (SoA) in accordance with ISO/IEC 27001:2005. The SoA refers out to other relevant processes and procedures.

This document also details the processes and procedures for training and awareness, general "check and act" activities, Internal ISMS Audit, Management Review and ISMS improvements in accordance with the FDCA model.

It includes all the ISMS records.

Approval and Distribution Policy

This ISMS was approved by the OA on yyyy-mm-dd. Specifically, management accepts the residual risks identified in the Risk Treatment Plans.
<table>
<thead>
<tr>
<th>ISO/IEC 27001 mappings for FISMA compliance</th>
<th>Regulations</th>
<th>Standards</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>§10.3.1 - Controls for the Information Security Management System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>A1</td>
<td>B1</td>
<td>C1</td>
<td>D1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>§10.3.1 General</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td>B1</td>
<td>C1</td>
<td>D1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>§10.3.1 Information Security Policy and Objectives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td>B1</td>
<td>C1</td>
<td>D1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>§10.3.1 Scope</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td>B1</td>
<td>C1</td>
<td>D1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
the solution (12) – key steps

- re-structured Federal reference documents
- mapped IS 27001 «→» Federal reference docs
- building an ISMS based on a proven HTML ISMS skeleton
- review FPKI MA documentation system
- construct required ISMS documentation, minimising replication with existing docs
- ‘connecting the dots’ to show how the ISMS fulfills compliance with Federal imperatives – PSoA+(C)SoA+ECS
- build-in specific actions to satisfy FISMA and RMF requirements and processes (e.g. SP 800-37/53A)
broader applicability

Σ \[ \text{generic approach} \]

Σ \[ \text{mapping process and ECS principles have been adopted into Draft ISO/IEC 27003} \]

Σ \[ \text{other specific mappings are available} \]

➢ CobiT
➢ HIPAA
➢ SOX
➢ PCI DSS
➢ ...

© Zygma LLC 2008
although the work is under weigh the essential basis is proven:

- ‘flow-through’ for compliance is understood
- ISMS base is proven and guaranteed conformant

the approach taken is essentially re-usable

revision to 27001 (currently starting) will be readily accomodated by changes to the skeleton ISMS
For further contact:

Richard G. Wilsher

+1 714 965 94 42 (office)
+1 714 797 99 42 (mobile)

RGW@Zygma.biz

www.Zygma.biz