

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

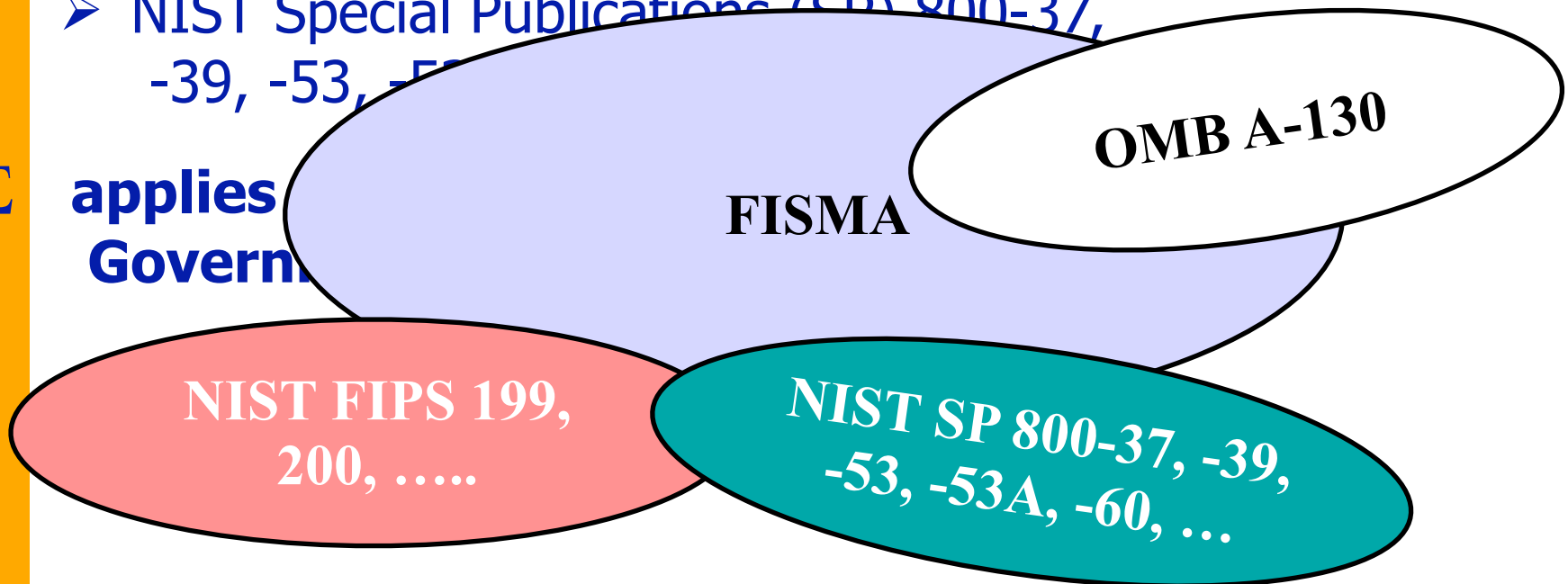
- Σ the Federal Public Key Infrastructure (FPKI) Policy Authority (PA) needs to have assurances as to the security measures in place with other PAs with which it wishes to cross-certify**
- Σ these other PAs could be from:**
 - industry
 - government
 - in and beyond the USA
- Σ assurance as to their 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)**

Σ FISMA compliance

Σ 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, ...

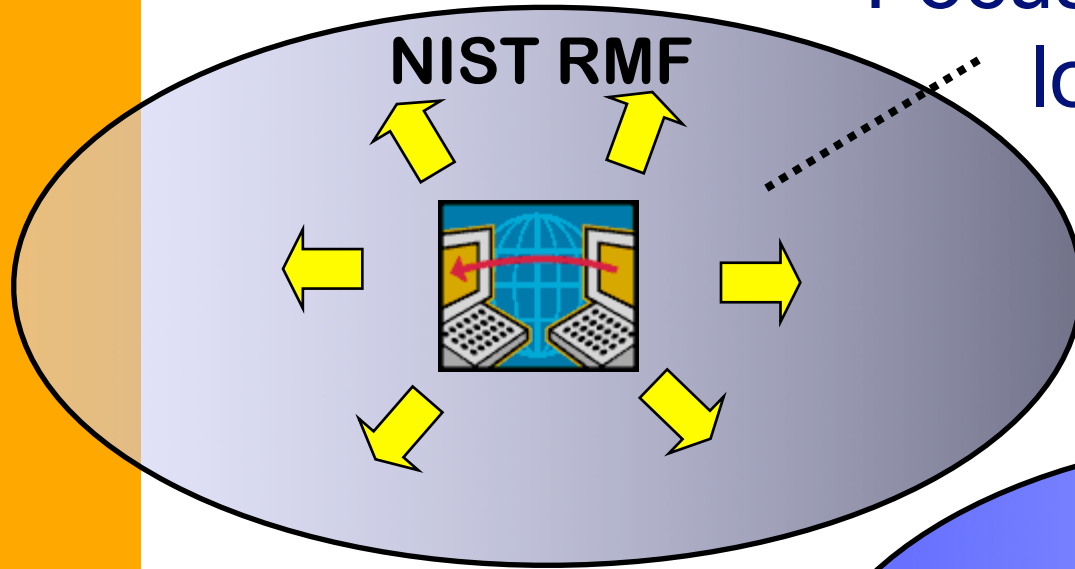
Σ applies to Federal Government



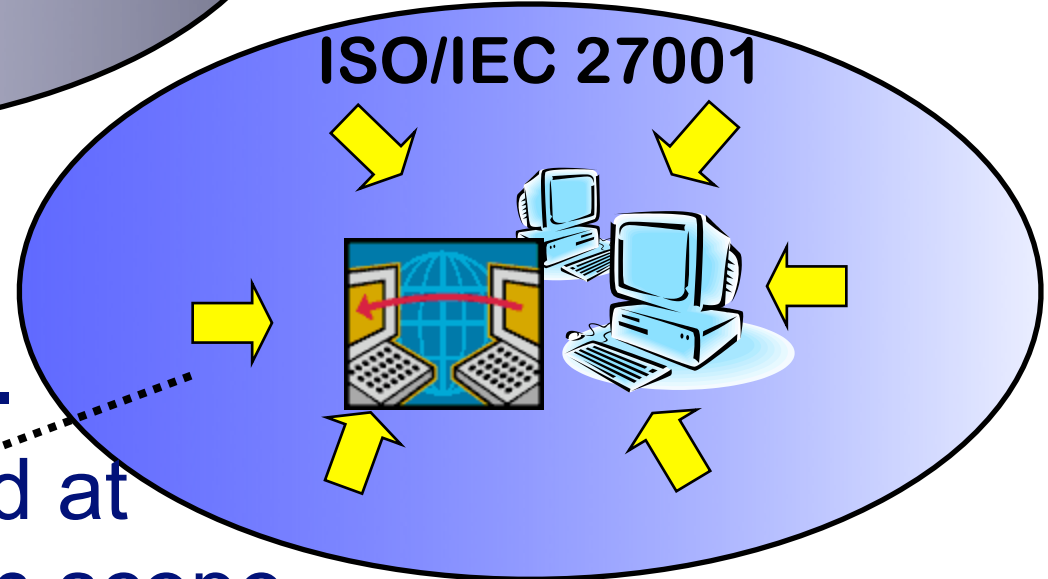
- Σ numerous Federal directives, regulation, standards, policies, to which agencies, departments and contractors have to be compliant**
- Σ FISMA has lower value/recognition in the commercial sector**
- Σ this even more so, concerning international recognition**
- Σ many agencies and contractors undergoing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

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

- Σ **reduction of audit management and technical complexity, economies in time and money**
- Σ **combining will reduce the total workload where both FISMA and ISMS are required**
- Σ **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
- Σ **NIST is onboard and fully aware of these efforts**

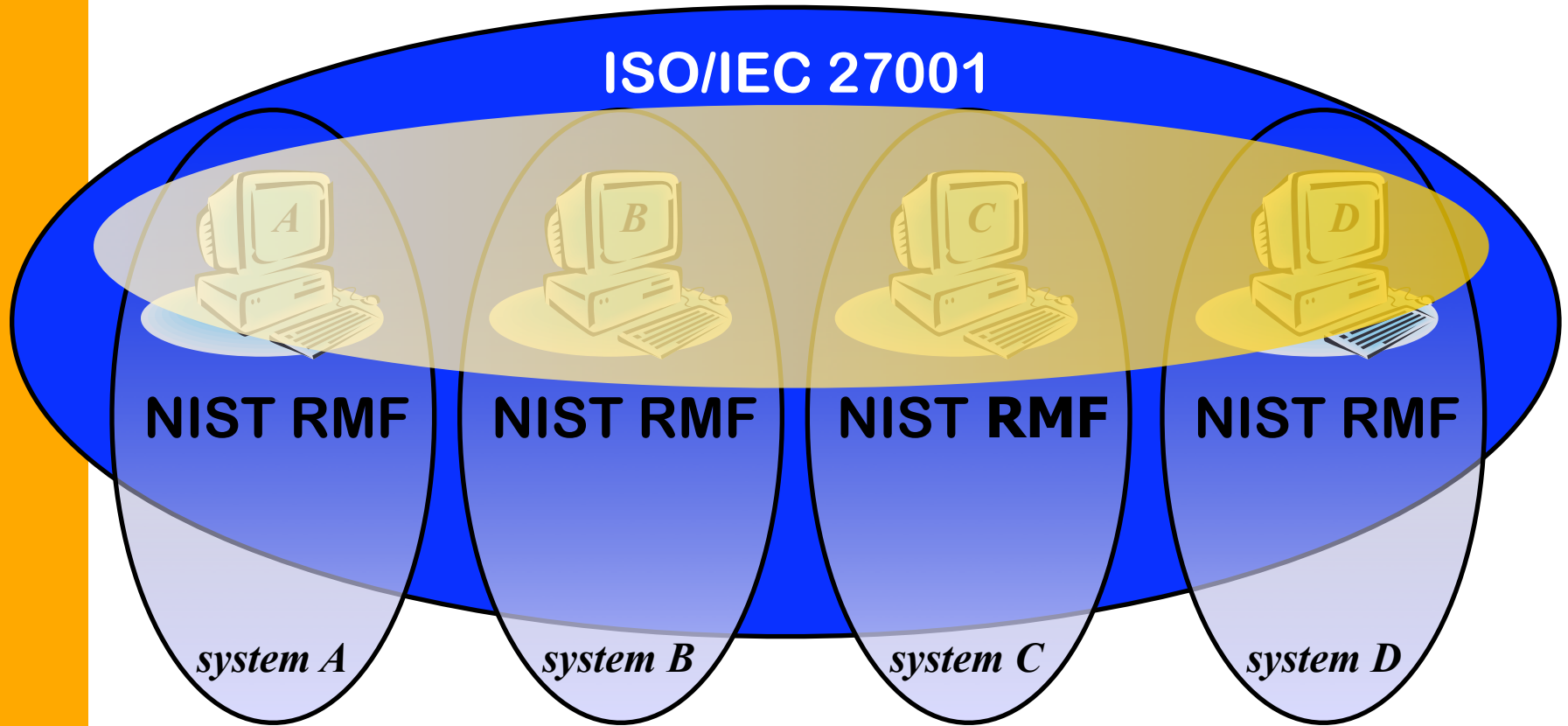


Focuses on a **system**, looks outward at its **management environment**



Focuses on the **security management**, looks inward at the **systems within scope**

differences – scope & coverage



Σ take each IS 27001 normative clause:

- §4 - §8 inclusive (processes)
- Annex A (security controls)

Σ 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

- Σ very discursive**
- Σ good content but embedded requirements**
- Σ general absence of discrete clauses**
- Σ very difficult to assess (and map) against**

- Σ content unaltered**
- Σ discrete clause references inserted**
- Σ commensurate re-structuring/layout**
- Σ insertion of cross-references to IS 27001 clauses**
- Σ 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 MINIMUM SECURITY REQUIREMENTS

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

Policies and procedures play an important role in the effective implementation of information security programs within the federal government and the success of the measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the 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 transactions and functions that authorized users are permitted to execute.

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.

| ISO/IEC 27001 clause | Commentary |
|---|--|
| §4.2.1(c), §4.3.1(a, c, g), §4.3.2 (f, <i>inter alia</i>), §5.1(a), §5.2.1(b), A.5.1.1 | '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. |

3.1 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) and to the

the solution (5) – an example

3 MINIMUM SECURITY REQUIREMENTS

The minimum security requirements cover seventeen security-related areas with regard to 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) 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) system and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. The seventeen areas represent a broad-based, balanced information 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 information security programs within the federal government and the success of the result measures employed to protect federal information and information systems. Thus, organizations develop and promulgate formal, documented policies and procedures governing the minimum requirements set forth in this standard and must ensure their effective implementation.

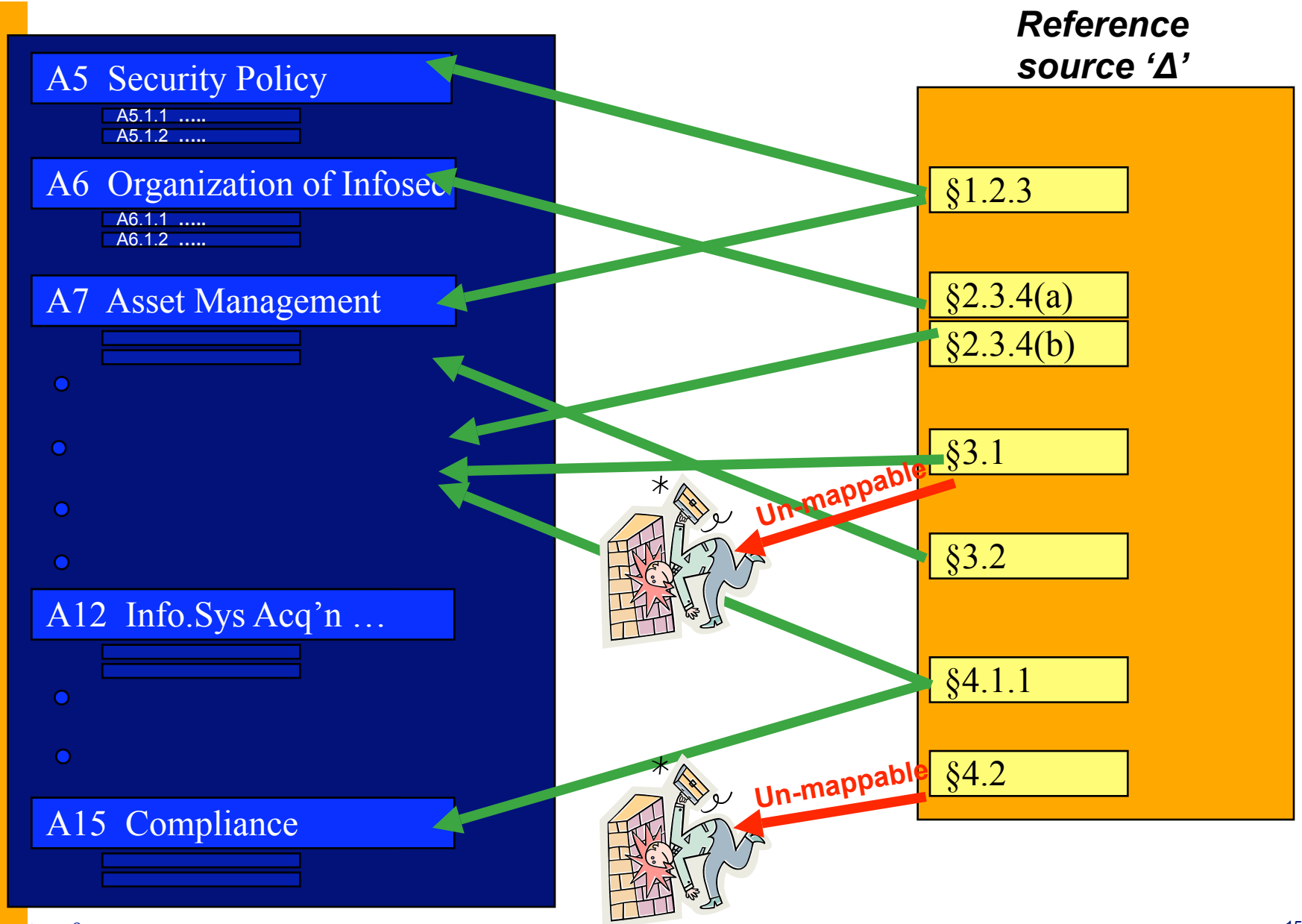
Specifications for Minimum Security Requirements

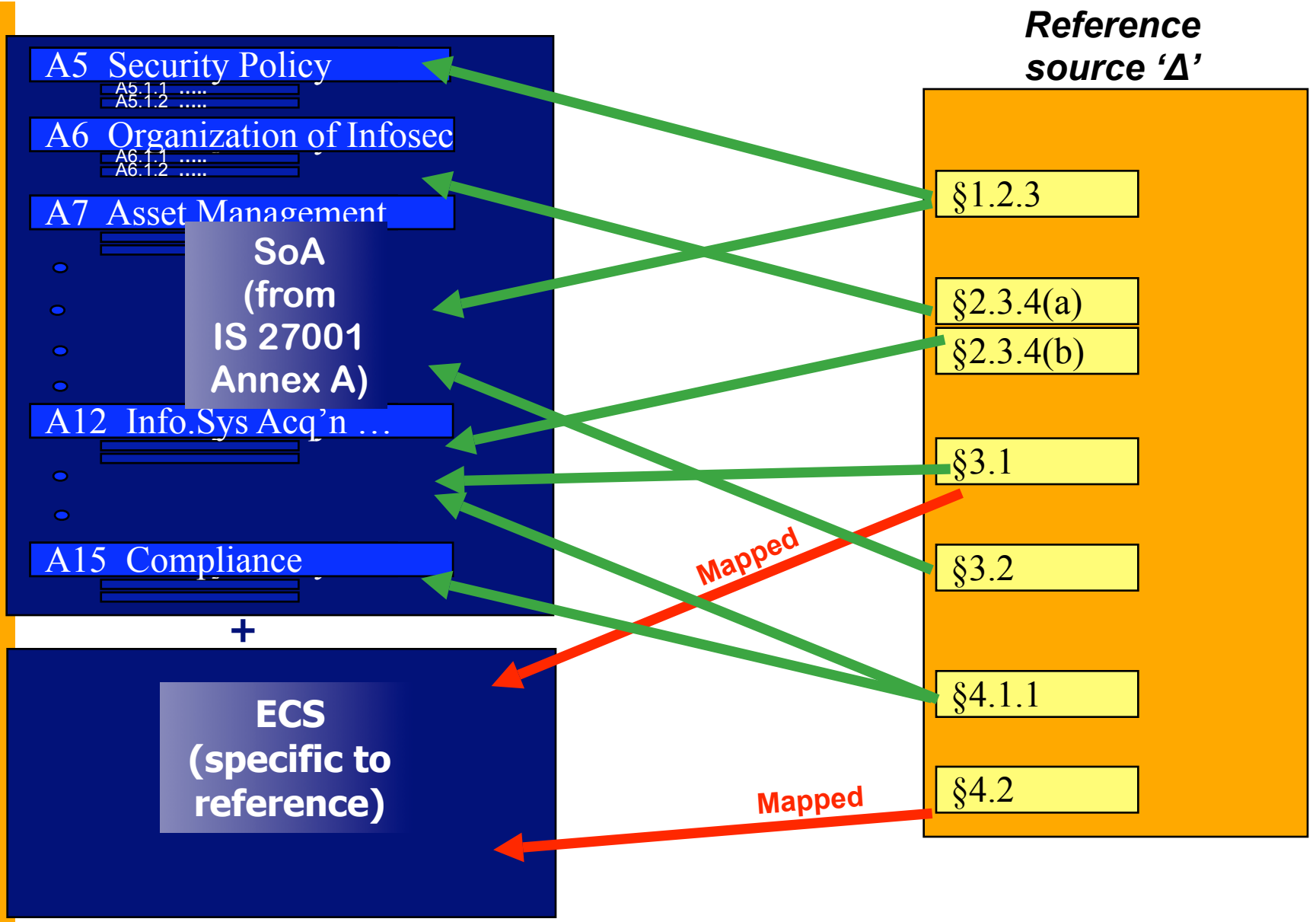
Access Control (AC): Organizations must limit information system access to authorized users, acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

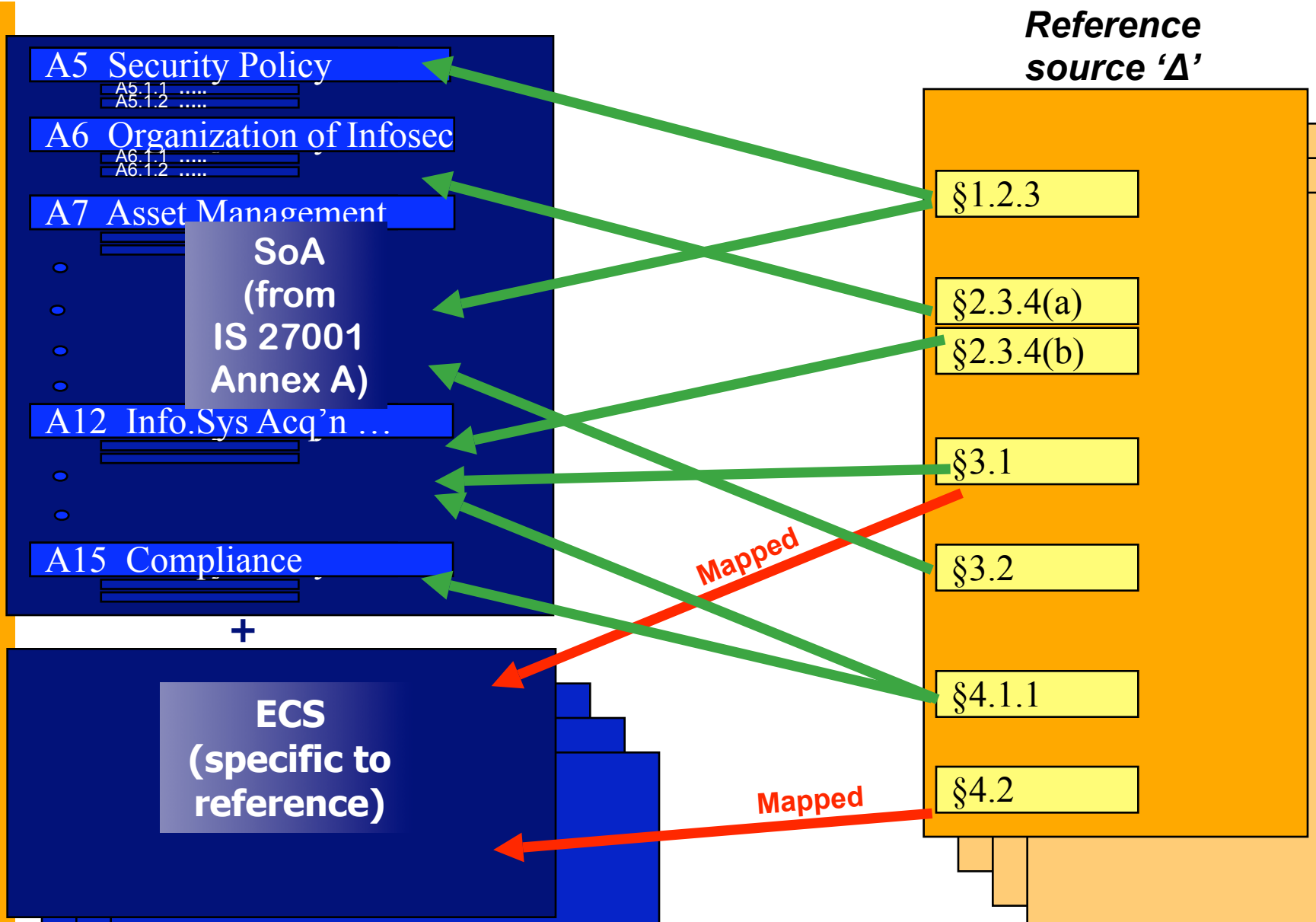
3.1.1 Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

| ISO/IEC 27001 clause | Commentary |
|---------------------------|--|
| §4.2.1(c) | Refer to EZP 853 for a comprehensive mapping for this control group. |
| §5.1 | |
| A.5.1.1 | |
| A.5.1.2 | |
| A.6.1.3 | |
| A.8.1.1 | |
| A.9.1.1 | |
| A.9.1.2 | |
| A.9.1.3 | |
| A.11.1.1 | |
| A.11.2.1 | |
| A.11.2.2 | |
| A.11.2.3 | |
| A.11.2.4 | |
| A.11.4.1 | |
| A.11.6.1 | |
| A.11.7.1 | |
| A.11.7.2 | |

the solution (6) – the Extended Control Set paradigm







the solution (9) – example Extended Controls

| | | |
|--|------------------------------|---|
| SP53.CM ¶ <i>Objective:</i> To ensure that configuration management policy and procedures are in place to fully meet the FISMA requirements. | | |
| SP53.CM.1a | Baseline Configurationa | <i>Control</i> ➤ The organization shall develop, document, and maintain a baseline configuration for each information system falling within the scope of the ISMS.¶ <i>Guidance</i> ➤ 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 Settingsa | <i>Control</i> ➤ 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.¶ <i>Guidance</i> ➤ Refer to SP 800-53 Security Control CM-6 . |
| SP53.CM.3a | Least Functionalitya | <i>Control</i> ➤ 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.¶ <i>Guidance</i> ➤ Refer to SP 800-53 Security Control CM-7 . |
| SP53.CP ¶ <i>Objective:</i> To ensure that contingency planning policy and procedures are in place to fully meet the FISMA requirements. | | |
| SP53.CP.1a | Telecommunications Servicesa | <i>Control</i> ➤ 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.¶ <i>Guidance</i> ➤ This control should be seen as a specific instance of A.10.2.1 and/or |



Index

PLAN

Introduction

Scope

Policy

Context

- [Assets](#)
- [Threats](#)
- [Impacts](#)

Risk Assessment

- [RTP Index](#)

SOA

DO

Metrics/Incidents

Training/Awareness

Other Manuals

CHECK/ACT

- [Internal Audit](#)
- [Mngmnt Review](#)
- [Improvement](#)

Records

- [To-Do-List](#)
- [Impact Log](#)
- [Amendment Record](#)

Clear Footnotes

Skeleton Rev 6.0.1gZ

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 OA 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 PDCA 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.

the solution (11) - mapping matrix

| | A | B | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | | | | | | | | | | | | | | | | | | | | | | |
|-----|--|--|---|--------------|--------------------|---------------------------|-----------------|-----------------|------------------|------------------|------------------|-------------------|------------------|--------------------------|-------------------|------------------|------------------|-----------|------|------|---|--|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| 1 | ISO/IEC 27001 mappings for FISMA compliance | | <i>Note: per col. C for ECS details</i> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | © 2008 Zyigma LLC | | Regulation | | | Standards | | Guidelines | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 27001 Clause/ Control | 27001 Requirement/ Control Objective | SoA | FISMA | OMB A-130 | OMB A-130 App. III | FIPS 199 | FIPS 200 | SP 800-18 | SP 800-26 | SP 800-30 | SP 800-37 | SP 800-39 | SP 800-53 | SP 800-53A | SP 800-60 | SP 800-70 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 193 | §4.2.3(h) | Record actions and events that could impair performance or effectiveness of the ISMS | | | | | | | | | | | | Considered ISMS-specific | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 194 | §4.2.4 | Maintaining and improving the ISMS | | | §8.b.1(c)(ii, iii) | §A.3.a.(3) | §A.3.b.(3) | | | | §5 | | | | §3.5.1 | §3.5.2(c) | §3.5.2(b) | §3.5.2(c) | CA-1 | PL-3 | | | | | | | | | | | | | | | | | | | | | | | |
| 195 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 196 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 197 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 198 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 199 | §4.2.4(c) | Implement improvements | | | | | | | | | | | | Considered ISMS-specific | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 200 | §4.2.4(b) | Take actions to continually improve the ISMS | | | | | | | | | | | | Considered ISMS-specific | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 201 | §4.2.4(c) | Communicate and agree improvement actions | | | | | | | | | | | | Considered ISMS-specific | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 202 | §4.2.4(d) | Ensure that improvements fulfill the intention | | | | | | | | | | | | Considered ISMS-specific | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 203 | §4.3 | Documentation requirements | | | §8.a.1(j) | | | §3.114 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 204 | | | | | §8.a.4(s-c) | | | | | | §3.31(a, b, h) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 205 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 206 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 207 | §4.3.1 | General | | | §8.a.1(j) | §8.a.4(s-c) | §8.b.1(c)(v) | | | | §3.5.2(b) | | | | §2 | §3.10.1 | §3.10.2 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 208 | | | | | | | | | | | | | | | | | | | | | | | Evidence of established and documented management framework | | | | | | | | | | | | | | | | | | | | |
| 209 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 210 | §4.3.(v) | Statements of policy and objectives | | | §8.a.1(j) | §8.a.4(s-c) | | | §3.0.2 | | §2 | §3.112(a, b, d-g) | §3.3.4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 211 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 212 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 213 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 214 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 215 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 216 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 217 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 218 | §4.3.(b) | Scope | | | §8.a.1(j) | §8.a.4(s-c) | | | §3.4.2 | §2 | §2 | §3.111(f, g, h) | §3.3.4 | §3.4.2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 219 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 220 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 221 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 222 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 223 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 224 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 225 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 226 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 227 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 228 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 229 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 230 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 231 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

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

- Σ **generic approach**
- Σ **mapping process and ECS principles have been adopted into Draft ISO/IEC 27003**
- Σ **other specific mappings are available**
 - CobiT
 - HIPAA
 - SOX
 - PCI DSS
 - ...

- Σ although the work is under weigh the essential basis is proven:**
 - 'flow-through' for compliance is understood
 - ISMS base is proven and guaranteed conformant
- Σ the approach taken is essentially re-usable**
- Σ 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