Risk Management Framework (RMF) 101 for Managers

October 17, 2017

noblis®

For the best of reasons

DoD Risk Management Framework (RMF) Process

DoDI 8510.01, Mar 2014 [based on NIST SP 800-37]

Architecture Description
Components
Firmware
Software
System Boundary

Organizational Inputs
Missions Supported
Types of Data
Goals & Objectives
Priorities

"The RMF provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information [and control] systems supporting their core missions and business functions."

(Source: NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*)

AO	Authorizing Official
ATC	Authority to Connect
ATO	Authority to Operate
CIO	Chief Information Officer
DATO	Denial of Authority to Operate
eMASS	Enterprise Mission Assurance Mgmt Sys
FAT	Factory Acceptance Testing
IATT	Interim Authority to Test
ISO	Information System Owner
ISSM	Information System Security Manager
OT	Operational Technology (controls)
PM	Program Manager
PIT	Platform Information Technology
POAM	Plan of Action & Milestones
RMF KS	DoD's RMF Knowledge System website
SAR	Security Assessment Report
SAT	Site Acceptance Testing
SCA	Security Compliance Assessor

ATO Package
- Security Plan
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POA&M)
- Inherited Controls Documentation

1 Categorize	2 Select	3 Implement	4 Assess	5 Authorize	6 Monitor
Information System CNSSI 1253 | NIST SP 800-60	*Security Controls* RMF KS | NIST SP 800-53	*Security Controls* NIST SP 800-70 | 800-82 R2	*Security Controls* NIST SP 800-53A	*Information System* NIST SP 800-37	*Security Status* NIST SP 800-37
Register in eMASS	Security Plan		Security Assessment Report	Plan of Action & Milestones	
Impact due to loss of… Confidentiality Low, Mod, High Integrity Low, Mod, High Availability Low, Mod, High	Baseline Overlays (scripted) Tailoring (custom) Inherited	Documents & Artifacts Test & Dev Environment Jump Kit/Rescue CD FAT/SAT Testing	Resolve SCA Findings	Receive IATT or… ATO ATC DATO	Continuous According to POA&M Annual Report
PM, ISO, Mission Owner	PM, ISO	PM, ISO	PM, ISO	PM, ISO, ISSM, SCA	ISO, ISSM
	SCA, CIO		SCA	AO	AO
2 manhours $400	4 manhours $800	460 manhours $92,000	135 manhours $27,000	24 manhours $4,800	312 manhours $62,400

noblis

Step 1 – Categorize the System

TASK 1-1: Categorize the system & document in security plan.

- If data **Confidentiality** is lost, what is potential mission impact? *Low*, *Moderate*, or *High*?
- If data **Integrity** is lost, what is the potential impact? *Low*, *Moderate*, or *High*?
- If data or system **Availability*** is lost, what is the potential impact? *Low*, *Moderate*, or *High*?
- System Category = {(**Confidentiality**, *impact*), (**Integrity**, *impact*), (**Availability**, *impact*)}

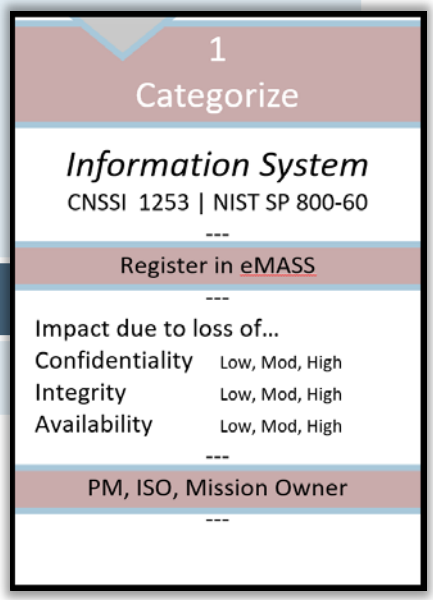
*Availability is most important for control systems, while confidentiality and integrity are most important for traditional IT

TASK 1-2: Describe the system & document in security plan.

- Purpose, capabilities, missions supported
- Information types, flows
- Hardware, firmware, software, system interfaces
- Network architecture
- Security boundary, encryption

TASK 1-3: Register system w/ appropriate.

- DoD uses the Enterprise Mission Assurance Support System (eMASS)



Primary Responsibility: Information System Owner; Information/Mission Owner
References: FIPS Publication 199; CNSS Instruction 1253; NIST SP 800-60.

2 manhours
$400

Step 2 – Select Security Controls

TASK 2-1: Identify <u>common security controls</u> provided by the organization & document in security plan.

- A platform enclave can provide some **inheritable** (common) security controls that apply to all subsystems within the enclave boundary

TASK 2-2: Select <u>system-specific security controls</u> & document.

- Start with the recommended **baseline** for your system category [NIST SP 800-53]
- Apply any recommended **overlays** (scripted adjustments) for your mission [CNSSI 1253, NIST SP 800-82]
- Consider additional **tailoring** (ad hoc adjustments) unique to your organization
- Any baseline or overlay security controls that cannot be applied should have **compensating controls** (e.g. locked door, armed guard) documented in the security plan

TASK 2-3: Develop a strategy for <u>continuous monitoring</u> of security control effectiveness.

- Configuration management
- Assessment processes
- Reporting frequency

2
Select

Security Controls
RMF KS | NIST SP 800-53

Security Plan

Baseline
Overlays (scripted)
Tailoring (custom)
Inherited

PM, ISO

SCA, CIO

Primary Responsibility: Chief Information Officer / Senior Information Security Officer; Common Control Provider
References: CNSS Instruction 1253, NIST Special Publications 800-53 Rev 4, 800-82 Rev 2 (appendix G)

4 manhours
$800

Step 3 – Implement Security Controls

TASK 3-1: Implement security controls specified in the security plan.

- Ensure all devices receive appropriate patches and apply STIGs* required by DISA

  *A Security Technical Implementation Guide (STIG) is a methodology for standardized secure installation and maintenance of computer software and hardware. These guides, 'lockdown' permissive software to reduce vulnerabilities (Wikipedia).

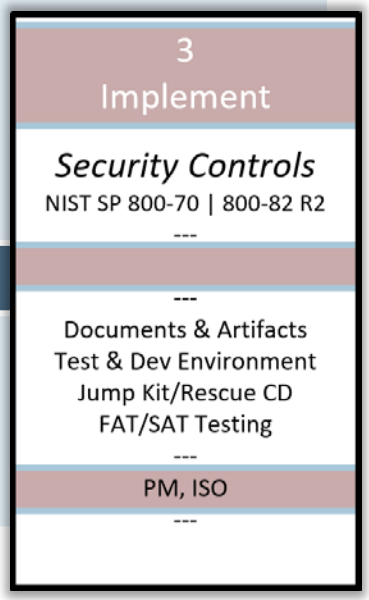
- 18 Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

TASK 3-2: Document security control implementation in the security plan.

- Use automated support tools like SCAP* to increase efficiency and cost effectiveness of security control implementation.

  *The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (Wikipedia)



Primary Responsibility: Information System Owner or Common Control Provider
References: NIST SP 800-82 Rev 2 (Chap 6); CNSS Instruction 1253; Web: SCAP.NIST.GOV

460 manhours
$92,000

Step 4 – Assess Security

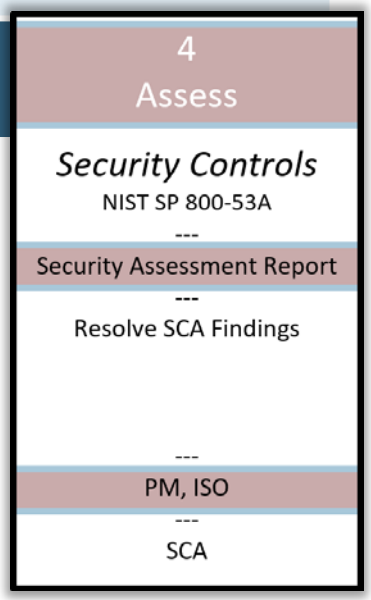
TASK 4-1: Develop, review, and approve a plan to assess security controls.

- Consider level of **independence** and **expertise** required of the assessor

TASK 4-2: Assess security controls in accordance w/ procedures defined in the security assessment plan.

TASK 4-3: Prepare security assessment report (SAR) documenting issues, findings, and recommendations from the security control assessment.

TASK 4-4: Conduct initial remediation actions based on findings and recommendations; reassess remediated control(s), as appropriate.



Primary Responsibility: Information System Owner or Common Control Provider; Security Control Assessor.
References: NIST SP 800-53A (Chap 3).

135 manhours
$27,000

Step 5 – Authorize System

TASK 5-1: Prepare plan of action & milestones (POA&M) based on findings and recommendations of the security assessment.

- Tasks required to remediate security controls
- Resources required
- Milestones
- Scheduled completion dates (before or after system goes live)

TASK 5-2: Assemble security authorization package and submit to authorizing official for adjudication.

- Security Plan
- Security Assessment Report
- Plan of Action & Milestones
- Documentation of adequacy of inherited (common) controls

TASK 5-3: Determine the risk to organizational operations.

TASK 5-4: Determine if the risk to organizational operations is acceptable.

5
Authorize

Information System
NIST SP 800-37

Plan of Action & Milestones

Receive IATT or…
ATO
ATC
DATO

PM, ISO, ISSM, SCA

AO

Primary Responsibility: Information System Owner or Common Control Provider and Authorizing Official.
References: NIST SP 800-37 (Appendix F).

24 manhours
$4,800

Step 6 – Monitor Security

TASK 6-1: Determine security impact of changes to the system.

- Requires structured, disciplined process of documenting changes in hardware, software, firmware, and supporting infrastructure

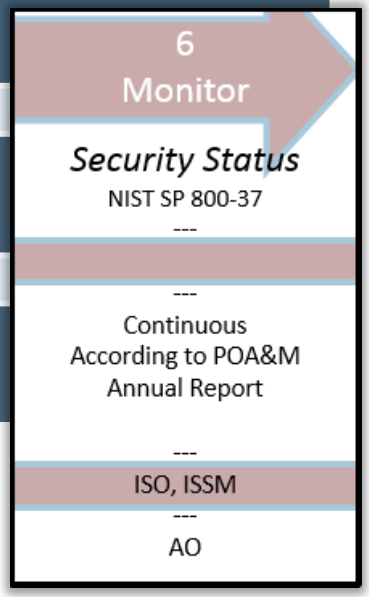
TASK 6-2: Assess security controls employed within and inherited by the information system.

TASK 6-3: Conduct remediation actions based on results of ongoing monitoring activities, assessment of risk, and outstanding items in POA&M.

TASK 6-4: Update security plan, security assessment report, and POA&M based on results of the continuous monitoring process.

TASK 6-5: Report security status of the system to the authorizing official on an ongoing basis in accordance with the monitoring strategy.

TASK 6-6: Review reported security status of the system to determine whether the risk to organizational operations remains acceptable.



Primary Responsibility: Information System Owner or Common Control Provider and Security Control Assessor.
References: NIST SP 800-37 (Appendix G), and 800-137, CNSS Instruction 1253.

312 manhours
$62,400

Estimated Cost and Time

Step	Task(s)	Responsibility(ies)	Estimated Manhours	Estimated Cost
1. Categorize	Risk Level	System Owner, Authorizing Official	**2**	**$400**
2. Select	Baseline & Tailoring	System Owner	**4**	**$800**
3. Implement	Authorization Package	System Integrator	120	$24,000
	Documents and Artifacts	System Integrator, Vendor Subs	120	$24,000
	Create Test & Dev Environment	System Integrator	40	$8,000
	Create Jump-Kit Rescue CD	System Integrator	80	$16,000
	Conduct FAT and SAT Testing	System Integrator	100	$20,000
			460	**$92,000**
4. Assess	Security Assessment Report	System Integrator	40	$8,000
	Upload to eMASS	System Integrator	15	$3,000
	Preliminary Mitigating Actions	System Integrator, Vendor Subs	80	$16,000
			135	**$27,000**
5. Authorize	Authorization Decision Document	System Owner, Authorizing Official	4	$800
	Plan of Action & Milestones	System Integrator, System Owner	20	4,000
			24	**$4,800**
			625	**$125,000**
6. Monitor	Patch Management, Reporting	System Owner	**312**	**$62,400**

- Estimates from “RMF Work Breakdown Structure”, by Chipley, Apr 2017
- Estimated time does not account for government review
- ESTCP project may not be responsible for continuous monitoring

Definitions

Reference: CNSSI 4009

Air Gap	An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). [Source: IETF RFC 4949 Ver 2]
Authorizing Official	A senior (federal) official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. [Source: CNSSI 4009]
Authorization To Operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [Source: NIST SP 800-53 Rev 4]
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. [Source: NSPD-54/HSPD-23]
Impact Levels	Used in conjunction with Security Objectives to determine the Security [Risk] Category of an information system **Low**: Loss would have **limited** adverse impact **Moderate**: Loss would have **serious** adverse impact **High**: Loss would have **catastrophic** adverse impact [Source: FIPS 199]
Facility-Related Control System	A control system which controls equipment and infrastructure that is part of a DoD building, structure, or linear structure.
Platform Enclave	A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. Enclaves can limit damage from network perimeter breaches. Segmenting networks into logical enclaves and restricting host-to-host communications paths can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves. Containment provided by enclaving also makes incident cleanup significantly less costly. [Source: ICS-CERT 2009]
Security [Risk] Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. [Source: FIPS 199]
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Objectives	**Confidentiality**: preventing unauthorized disclosure **Integrity**: preventing unauthorized modification or destruction **Availability**: preventing disruption of access to/use of information [Source: FIPS 199 and 44 U.S.C., Sec. 3542 a.k.a. Federal Information Security Management Act or FISMA]
Security Technical Implementation Guide (STIG)	Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline. [Source: DoDI 8500.01]

Caution

Facility-related control systems cannot be treated like traditional IT systems

See:

NIST SP 800-82 Rev 2

UFC 4-010-06

Facility-Related Controls versus IT

NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*

Table 2-1 Summary of IT System and ICS System Differences

Category	Information Technology System	Industrial Control System […or Operational Technology (OT) System] […or Facility-Related Control System]
Performance Requirements	• Non-real-time • Response must be consistent • High throughput is demanded • Less critical emergency interaction • Tightly restricted access control can be implemented to as necessary for security	• Real-time • Response is time-critical • Modest throughput is acceptable • Response to human and other emergency interaction is critical • Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (Reliability) Requirements	• Rebooting is acceptable • Availability deficiencies can often be tolerated, depending on the system's operational requirements	• Rebooting not acceptable due to availability requirements • Availability requirements may necessitate redundant systems • Outages must be planned and scheduled days/weeks in advance • High availability requires exhaustive pre-deployment testing
Resource Constraints	• Systems are specified with enough resources to support the addition of third-party applications such as security solutions	• Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Risk Management Requirements	• Manage data • Data confidentiality & integrity are paramount • Fault tolerance less important – momentary downtime is ok • Major risk impact is delay of business	• Control physical world • Human safety is paramount, followed by protection of process • Fault tolerance is essential, momentary downtime not acceptable • Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Change Management	• Software changes are applied in a timely fashion with good security policy and procedures. Procedures usually automated	• Software changes must be thoroughly tested and deployed incrementally to ensure the integrity of the control system. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported

Facility-Related Controls versus IT (cont'd)

Category	Information Technology System	Industrial Control System […or Operational Technology (OT) System] […or Facility-Related Control System]
System Operation	• Systems are designed for use with typical operating systems • Upgrades are straightforward and automated deployment tools are available	• Differing and possibly proprietary operating systems, often without security capabilities built in • Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Communications	• Standard communications protocols • Primarily wired networks with some localized wireless capabilities • Typical IT networking practices	• Many proprietary, non-standard communication protocols • Several types of communications media, including dedicated wire and wireless (radio and satellite) • Networks are complex and sometimes require the expertise of control engineers
Managed Support	• Allow for diversified support styles	• Service support is usually via a single vendor
Component Lifetime	• Lifetime on the order of 3 to 5 years	• Lifetime on the order of 10 to 15 years
Component Locations	• Components are usually local and easy to access	• Components can be isolated, remote, and require extensive physical effort to access

Facility-Related Control Systems

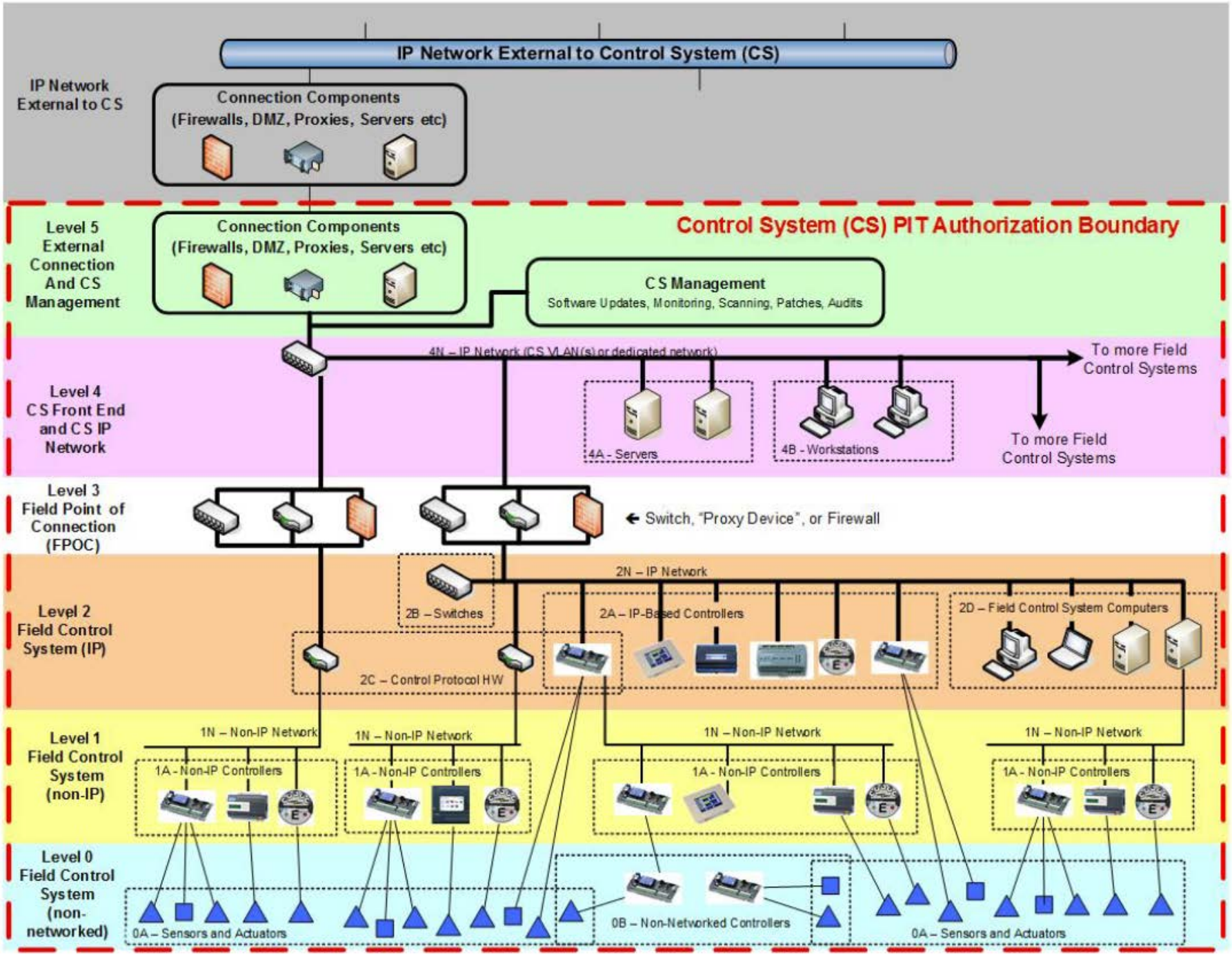
Notional 5-level Reference Architecture

from

Unified Facility Criteria (UFC) 4-010-06, 19 September 2016

Change 1, 18 January 2017

Appendix E


IP Network External to Control System (CS)
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control System (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End and CS IP Network
4N – IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
Switch, "Proxy Device", or Firewall
Level 2 Field Control System (IP)
2N – IP Network
2B – Switches
2A – IP-Based Controllers
2D – Field Control System Computers
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers

Notional 5-Level Facility-Related Controls Network

- **LEVEL 0: Sensors and Actuators**

  Devices that lack a network and therefore can only be exploited from physical proximity, not remotely via a network. If they communicate at all, they use only simple analog and binary signals; they do not use any form of digital protocol for communication. A sensor or actuator that uses a communications protocol (e.g., Zigbee, Bluetooth) is a Level 1 (non-IP) or Level 2 (IP) device.

  Examples: thermistor temperature sensor, electric actuator

- **LEVEL 1: Field Control System (non-IP)**

  That portion of the controls network which does not use the IP protocol. This includes both the controllers themselves (Level 1A) and the network (Level 1N).

  Examples: VAV box controllers, networked (non-IP) electric meter, intelligent (networked) thermostat

- **LEVEL 2: Field Control System (IP)**

  The portion of the control system which uses IP, but is not shared with any other system.

  Examples: air handler controller, control system at a central plant where nature and criticality requires a local operator interface.

Notional 5-Level Facility-Related Controls Network

- **LEVEL 3: Field Point of Connection (FPOC)**

  The device which connects the dedicated Level 2 IP network with the Level 4 IP network. For each field control system, the FPOC is the specific single demarcation point in the control system between that field control system and the front end system.

  Examples: Standard IT managed ethernet switch or IP router

- **LEVEL 4: Control System Front End and Control System IP Network**

  The site-wide IP network used for the control system, along with front end servers and workstations (desktops and laptops). The IP network may be a dedicated physical network, or a Virtual Local Area Network (VLAN) or a Virtual Private Network (VPN).

  Examples: Servers and racks, computers, laptops, operator interfaces

- **LEVEL 5: External Connection and Control System Management**

  Interfaces to "external" networks (IP networks other than the control system network). this level provides the enclave boundary defense between the control system (at Level 4 and below) and IP networks external to the control system.

  Examples: Firewalls, proxy servers, de-militarized zone (DMZ), wide area network