# Mapping of IoT security publications to the Code of Practice for Enterprise Connected Device Security

**Version 2.0**

accenture

# Table of Contents



 

# Introduction

The present document was created by Accenture on behalf of the Department for Science, Innovation and Technology (in the following: DSIT).

The present document provides an updated mapping of selected publications to the principles as defined in the “Code of Practice for Enterprise Connected Device Security” (Previously NCSC Device Security Principles, in the following: the CoP principles), which was part of the “Device Security Guidance”, published by the National Cyber Security Centre in June 2021 [1].

As the CoP principles focus on so-called “enterprise-connected” devices, which are defined as “devices that interact with, process or hold an organization’s data” [2], the present document mainly covers IoT-related aspects with a focus on enterprise use cases.

# References


[1] Device Security Guidance. National Cyber Security Centre. 2021.

[2] Code of Practice for Enterprise Connected Device Security. Department for Science, Innovation and Technology. 2025.

[3] *IEC 62443-4-2 - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*. International Electrotechnical Commission (IEC). 2019.

[4] *Internet of Things (IoT) Security and Privacy Recommendations*. Broadband Internet Technical Advisory Group (BITAG). 2016.

[5] *Matter Specification Version 1.0*. Connectivity Standards Alliance (CSA). 2022.

Updated by: *Matter Specification Version 1.4*. 2024.

[6] *NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline*. National Institute of Standards and Technology (NIST). 2020.

[7] *NISTIR 8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. National Institute of Standards and Technology (NIST). 2021.

[8] *NISTIR 8425 - Profile of the IoT Core Baseline for Consumer IoT Products*. National Institute of Standards and Technology (NIST). 2022.

[9] *CLP.13 v2.2 - IoT Security Guidelines Endpoint Ecosystem Version 2.2*. GSM Association (GSMA). 2020.

[10] *Baseline Security Recommendations for IoT*. European Union Agency for Cybersecurity (ENISA). 2017.

[11] *Cyber Hygiene Best Practices*. National Electrical Manufacturers Association (NEMA). 2018.

[12] *IoTSF IoT Security Assurance Framework Release 3.0 Nov 2021*. IoT Security Foundation (IoTSF). 2021.

[13] *IoT Security & Privacy Trust Framework v2.5*. Internet Society (ISOC/OTA). 2017.

[14] *Industrial Internet of Things Volume G4: Security Framework*. Industrial IoT Consortium (IIC). 2016.

[15] *EN 303 645 - V2.1.1 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*. European Telecommunications Standards Institute (ETSI). 2020.

Updated by: *EN 303 645 - V3.1.3 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*. 2024.


 

[16] *NIST SP-800-213A - IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*. National Institute of Standards and Technology (NIST). 2021.

[17] *EN 18031 Part 1 (final draft): Internet connected radio equipment.* CEN/CENELEC. 2024.

[18] *EN 18031 Part 2 (final draft): radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment.* CEN/CENELEC. 2024.

[19] *EN 18031 Part 3 (final draft): Internet connected radio equipment processing virtual money or monetary value.* CEN/CENELEC. 2024.

[20] *GUIDANCE ON THE APPLICATION OF THE HARMONISED STANDARDS SERIES EN 18031:2024 IN SUPPORT OF COMMISSION DELEGATED REGULATION 2022/30.* European Commission. 2025.

 

# List of Abbreviations

| | |
|---|---|
| **CCSC** | **Common Component Security Constraints** |
| **CoP** | Code of Practice |
| **CR** | Component Requirement |
| **CS** | Cybersecurity State Awareness |
| **DC** | Device Configuration |
| **SIT** | Department for Science, Innovation and Technology |
| **DI** | Device Identification |
| **DP** | Data Protection |
| **DS** | Device Security |
| **EC** | European Commission |
| **EDR** | Embedded Device Requirements |
| **EN** | European Norm |
| **HDR** | Host Device Requirements |
| **IoT** | Internet of Things |
| **LA** | Logical Access to Interfaces |
| **NDR** | Network Device Requirements |
| **OTA** | Over-The-Air |
| **RED** | Radio Equipment Directive |
| **SU** | Software Update |
| **H** | High Overlap |
| **M** | Medium Overlap |

# Methodology

## Mapping and Rating

As the researched publications might just cover a subset of the CoP principles, a mapping was created between them. The content of each publication is compared to each chapter of the CoP principles and a mapping was created if their respective topics match.

Further, a similarity rating was performed for each created mapping. The rating should provide a better understanding of which of the publications might be of higher interest – it is based on the similarity between the researched document and the subsections of the CoP principles. A related publications has a "high overlap" (H) if the wording is similar, and at most two subsections of the CoP principles cannot be mapped to that publication. Results that are categorized to have a "medium overlap" (M) have at least a matching rate of half of the subsections.

*Note: The wording of the researched publications might not necessarily be equal to the wording of the CoP principles.*

## Publication Selection

Selection of related publications in the IoT security topic was performed in two steps: In a first step, standardisation organizations and their respective committees and work groups were researched for relevant contributions to the overall IoT topic. Secondly, the publications of those have been searched for concrete publications that cover any IoT device security standards, guidelines, recommendations, or frameworks.

*Note: Except for the EN 18031 standards, non-accessible publications, i.e. paywalls or member-restricted documents, are not included in the research.*

# Mapping Results

The following table shows the mapping results in form of a mapping between the CoP principles and the referenced sections of the researched publications, including the matching rating in the rightmost column.

Table 1: Mapping of related publications to the Code of Practice for Enterprise Connected Device Security

| Reference | | | CoP principle | Overlap |
|---|---|---|---|---|
| IEC 62443-4-2 [3] | Section 13.5<br>Section 14.5 | EDR 3.10 - Support for updates<br>HDR 3.10 - Support for updates | 1. Provide updates, securely | M |
| | Section 5.3 | CR[1] 1.1 - Human user identification and authentication | 2. Support appropriate authentication | M |
| | Section 7.3<br>Section 8.3<br>Section 8.5 | CR 3.1 - Communication integrity<br>CR 4.1 - Information confidentiality<br>CR 4.3 - Use of cryptography | 3. Protect data at rest and data in transit | H |
| | Section 7.16<br><br>Section 13.6<br><br>Section 15.8 | CR 3.15 - Integrity of the boot process<br>EDR 3.11 - Physical tamper resistance and detection<br>NDR 3.11 - Physical tamper resistance and detection | 4. Maintain device integrity | H |
| | Section 4.2 | CCSC 1 - Support of essential functions | 5. Ensure transparency of device health | M |
| | Section 10.4 | CR 6.2 - Continuous monitoring | 10. Provide security logging, alerting and monitoring capabilities | M |
| | Section 11.5 | CR 7.3 - Control system backup | 11. Enable recovery to a known good state | H |
| BITAG Report [4] | Section 4<br><br>Section 7.1 | Many Devices Do Not Follow Security and Privacy Best Practices<br>IoT Devices Should Use Best Current Software Practices | 1. Provide updates, securely | H |
| | Section 5.1<br>Section 7.1 | Insecure Network Communications<br>IoT Devices Should Use Best Current Software Practices | 2. Support appropriate authentication | H |
| | Section 7.2 | IoT Devices Should Follow Security & Cryptography Best Practices | 3. Protect data at rest and data in transit | H |
| | Section 7 | Recommendations | 4. Maintain device integrity | M |
| | Section 5.3<br><br>Section 7.3 | Susceptibility to Malware Infection and Other Abuse<br>IoT Devices Should Be Restrictive Rather Than Permissive in Communicating | 6. Permit only trusted software | M |

[1] Please note, that CR means Component Requirement.

| Reference | | | CoP principle | Overlap |
|---|---|---|---|---|
| | Section 7.10 | The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues | 11. Enable recovery to a known good state | H |
| **CSA Matter Standard 1.4** [5] | Section 13.5<br>Section 11.19<br>Section 13.6 | Firmware<br>Over-the-Air (OTA) Software Update<br>Security Best Practices | 1. Provide updates, securely | M |
| | Section 13.6 | Security Best Practices | 2. Support appropriate authentication | M |
| | Section 13.6 | Security Best Practices | 3. Protect data at rest and data in transit | M |
| | Section 13.3<br>Section 13.5<br>Section 13.6<br>Section 13.7 | Commissioning<br>Firmware<br>Security Best Practices<br>Threats and Countermeasures | 4. Maintain device integrity | H |
| | Section 13.6.2 | Commissioning and Administration | 7. Minimise the privilege and reach of applications | M |
| | Section 13.6.4 | Manufacturing | 8. Constrain the use of all device interfaces | M |
| | Section 13.4. | Factory Reset | 11. Enable recovery to a known good state | M |
| **NISTIR 8259A** [6] | Page 9: Software Update | | 1. Provide updates, securely | M |
| | Page 7: Data Protection | | 3. Protect data at rest and data in transit | H |
| | Page 6: Device Configuration | | 4. Maintain device integrity | M |
| | Page 8: Logical Access to Interfaces | | 8. Constrain the use of all device interfaces | M |
| | Page 6: Device Configuration | | 9. Allow robust device management | H |
| **NIST IR 8228** [7] | Expectation 5:<br>Expectation 6: | Vulnerability Management<br>Vulnerability Management | 1. Provide updates, securely | M |
| | Expectation 8:<br>Expectation 9:<br>Expectation 10:<br>Expectation 11:<br>Expectation 12:<br>Expectation 13:<br>Expectation 24:<br><br>Expectation 25: | Access Management<br>Access Management<br>Access Management<br>Access Management<br>Access Management<br>Access Management<br>PII Processing<br>Permissions Management<br>Information Flow Management | 2. Support appropriate authentication | M |
| | Expectation 19:<br>Expectation 20:<br>Expectation 21: | Data Protection<br>Data Protection<br>Data Protection | 3. Protect data at rest and data in transit | M |

| Reference | | CoP principle | Overlap |
|---|---|---|---|
| | Expectation 14: Access Management | 4. Maintain device integrity | M |
| | Expectation 12: Access Management | 7. Minimize the privilege and reach of applications | M |
| | Expectation 15: Incident Detection<br>Expectation 16: Incident Detection | 10. Provide security logging, alerting and monitoring capabilities | M |
| **NIST IR 8425** [8] | Page 9: Software Updates | 1. Provide updates, securely | M |
| | Page 7: Data Protection | 3. Protect data at rest and data in transit | M |
| | Page 8: Interface Access Control | 7. Minimize the privilege and reach of applications | M |
| | Page 8: Interface Access Control | 8. Constrain the use of all device interfaces | M |
| | Page 6: Product Configuration | 9. Allow robust device management | H |
| | Page 6: Product Configuration | 11. Enable recovery to a known good state | M |
| **GSMA CLP.13** [9] | Section 7.5 Over the Air Application Updates | 1. Provide updates, securely | M |
| | Section 7.6 Improperly Engineered or Unimplemented Mutual Authentication | 2. Support appropriate authentication | M |
| | Section 6.19 Endpoint Communications Security<br>Section 6.20 Authenticating an Endpoint Identity | 3. Protect data at rest and data in transit | H |
| | Section 5.2 How should I Secure the Endpoint Identity?<br>Section 5.6 How do I Disallow Tampering of Firmware and Software? | 4. Maintain device integrity | M |
| | Section 7.9 Enforce a Separation of Duties in the Application Architecture | 7. Minimise the privilege and reach of applications | M |
| | Section 6.13 Logging and Diagnostics | 10. Provide security logging, alerting and monitoring capabilities | H |
| **NISA Security Recommendations** [10] | Section 4.3 Technical Measures (GP-TM-05, GP-TM-06, GP-TM-18, GP-TM-19) | 1. Provide updates, securely | M |
| | Section 4.2 Organisational, People and Process measures (GP-OP-04)<br>Section 4.3 Technical Measures (GP-TM-02, GP-TM-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM-39, GP-TM-40) | 3. Protect data at rest and data in transit | H |
| | Section 4.3 Technical Measures (GP-TM-55, GP-TM-56) | 5. Ensure transparency of device health | M |

| Reference | | CoP principle | Overlap |
|---|---|---|---|
| | Section 4.3 Technical Measures (GP-TM-08, GP-TM-09, GP-TM-21, GP-TM-22, GP-TM-25, GP-TM-27, GP-TM-29, GP-TM-33, GP-TM-42, GP-TM-44, GP-TM-45) | 8. Constrain the use of all device interfaces | M |
| | Section 4.3 Technical Measures (GP-TM-06) | 9. Allow robust device management | M |
| **NEMA** [11] | Principle 3: Monitoring Devices and Systems | 5. Ensure transparency of device health | M |
| | Principle 1: Segmenting Networks<br>Principle 4: User Management<br>Principle 5: Hardening Devices | 8. Constrain the use of all device interfaces | M |
| **IoTSF IoT Security Assurance Framework** [12] | Section 2.4.5 Device Software (2.4.5.1, 2.4.5.2, 2.4.5.3, 2.4.5.4, 2.4.5.8)<br>Section 2.4.6 Device Operating System (2.4.6.1) | 1. Provide updates, securely | M |
| | Section 2.4.6 Device Operating System (2.4.6.5)<br>Section 2.4.7 Device Wired and Wireless Interfaces<br>Section 2.4.8 Authentication and Authorization (2.4.8.8, 2.4.8.16)<br>Section 2.4.9 Encryption and Key Management for Hardware<br>Section 2.4.12 Data Protection and Privacy (2.4.12.2)<br>Section 2.4.16 Device Ownership Transfer (2.4.16.1, 2.4.16.2) | 3. Protect data at rest and data in transit | M |
| | Section 2.4.8 Authentication and Authorization (2.4.8.17)<br>Section 2.4.15 Configuration | 4. Maintain device integrity | M |
| | Section 2.4.7 Device Wired and Wireless Interfaces | 5. Ensure transparency of device health | M |
| | Section 2.4.5 Device Software (2.4.5.1) | 6. Permit only trusted software | M |
| | Section 2.4.4 Device Hardware & Physical Security (2.4.4.5, 2.4.4.9)<br>Section 2.4.5 Device Software (2.4.5.5)<br>Section 2.4.6 Device Operating System (2.4.6.3, 2.4.6.4)<br>Section 2.4.7 Device Wired and Wireless Interfaces<br>Section 2.4.8 Authentication and Authorization | 8. Constrain the use of all device interfaces | H |

| Reference | | CoP principle | Overlap |
|---|---|---|---|
| | Section 2.4.8 Authentication and Authorization (2.4.8.17)<br>Section 2.4.15 Configuration | 9. Allow robust device management | M |
| **ISOC/OTA** [13] | Security Principle: 1, 6 and 8 | 1. Provide updates, securely | M |
| | Security Principle: 2<br>User Access & Credentials: 17<br>Privacy, Disclosures & Transparency: 33 | 3. Protect data at rest and data in transit | M |
| | Privacy, Disclosures & Transparency: 26 | 11. Enable recovery to a known good state | M |
| **IIC Security Framework** [14] | Section 7.3 Endpoint Protection<br>Section 11.5.1 Secure Software Patching and Firmware Update | 1. Provide updates, securely | M |
| | Section 7.3 Endpoint Protection<br>Section 7.4 Communications and Connectivity Protection<br>Section 7.6 Security Configuration and Management<br>Section 7.7 Data Protection<br>Section 8.8 Endpoint Data Protection<br>Section 8.11 Cryptography Techniques for Endpoint Protection<br>Section 8.13 Resource-Constrained Device Considerations<br>Section 9.1 Cryptographic Protection of Communications & Connectivity<br>Section 10.4 Security Data Protection<br>Section 11.9 Configuration and Management Data Protection | 3. Protect data at rest and data in transit | M |
| | Section 7.3 Endpoint Protection<br>Section 7.6 Security Configuration and Management<br>Section 8.10 Endpoint Configuration and Management | 4. Maintain device integrity | H |
| | Section 7.3 Endpoint Protection<br>Section 7.5 Security Monitoring and Analysis<br>Section 7.7 Data Protection<br>Section 8.9 Endpoint Monitoring and Analysis<br>Section 10.3 Capturing and Storing Data for Analysis<br>Section 10.4 Security Data Protection | 5. Ensure transparency of device health | H |

| Reference | | CoP principle | Overlap |
|---|---|---|---|
| | Section 7.3 Endpoint Protection<br>Section 7.6 Security Configuration and Management<br>Section 8.10 Endpoint Configuration and Management<br>Section 11.7.1 Enrolment Phase | 9. Allow robust device management | H |
| | Section 10.3 Capturing and Storing Data for Analysis | 10. Provide security logging, alerting and monitoring capabilities | H |
| **EN 303 645** [15] | Provision 5.3 Keep software updated | 1. Provide updates, securely | H |
| | Provision 5.1-1<br>Provision 5.1-2 | 2. Support appropriate authentication | H |
| | Provision 5.5 Communicate securely<br>Provision 5.11 Make it easy for users to delete user data | 3. Protect data at rest and data in transit | M |
| | Provision 5.6-8<br>Provision 5.7-1 | 4. Maintain device integrity | H |
| | Provision 5.7 Ensure Software Integrity | 5. Ensure transparency of device health | H |
| | Provision 5.6 Minimize exposed attack surfaces<br>Provision 5.7-2 | 7. Minimise the privilege and reach of applications | M |
| | Provision 5.5 Communicate securely<br>Provision 5.6 Minimize exposed attack surfaces | 8. Constrain the use of all device interfaces | M |
| | Provision 5.6 Minimize exposed attack surfaces<br>Provision 5.12 Make installation and maintenance of devices easy | 9. Allow robust device management | M |
| | Provision 5.10 Examine system telemetry data | 10. Provide security logging, alerting and monitoring capabilities | M |
| | Provision 5.7 Ensure Software Integrity<br>Provision 5.12 Make installation and maintenance of devices easy | 11. Enable recovery to a known good state | M |
| **NIST SP-800-213A** [16] | DC-CTL Device Configuration Control<br>DP-CRY Cryptographic Capabilities and Support<br>DP-STX Secure Transmission<br>SU-APP Update Application Support<br>SU-UPD Update Capabilities | 1. Provide updates, securely | H |

| Reference | | | CoP principle | Overlap |
|---|---|---|---|---|
| | DC-PRV<br>DI-DAS<br>DI-IMS<br>DP-CRY<br>DP-KEY<br>DS-COM<br>LA-ACF<br>LA-AIM<br>LA-AUN<br>LA-AUZ<br>LA-XCN | Logical Access Privilege Configuration<br>Device Authentication Support<br>Identifier Management Support<br>Cryptographic Capabilities and Support<br>Cryptographic Key Management<br>Secure Communication<br>Authentication Configuration<br>Authentication and Identity Management<br>Authentication Support<br>Authorization Support<br>External Connections | 2. Support appropriate authentication | H |
| | DP-CRY<br>DP-KEY<br>DP-STO<br>DP-STX<br>DS-COM | Cryptographic Capabilities and Support<br>Cryptographic Key Management<br>Secure Storage<br>Secure Transmission<br>Secure Communication | 3. Protect data at rest and data in transit | H |
| | CS-AUP<br>CS-AWR<br>DS-DIN<br>DS-EXE<br>DS-RSC<br>SU-UPD | Audit Support and Protection<br>State Awareness Support<br>Device Integrity<br>Secure Execution<br>Secure Resource Usage<br>Update Capabilities | 4. Maintain device integrity | H |
| | CS-AUP<br>CS-AWR<br>DS-DIN | Audit Support and Protection<br>State Awareness Support<br>Device Integrity | 5. Ensure transparency of device health | H |
| | LA-LDU<br>LA-ROL | Limitations on Device Usage<br>Role Support and Management | 6. Permit only trusted software | H |
| | DS-EXE<br>DS-RSC<br>LA-ROL | Secure Execution<br>Secure Resource Usage<br>Role Support and Management | 7. Minimize the privilege and reach of applications | H |
| | DC-INT<br>DI-AID<br>DI-IMS<br>DS-OPS<br>LA-IFC | Interface Configuration<br>Actions Based on Device Identity<br>Identifier Management Support<br>Secure Device Operation<br>Interface Control | 8. Constrain the use of all device interfaces | M |
| | DC-AUT<br>DC-CTL<br>DI-AID<br>DS-DIN<br>DS-ONB<br>LA-IFC | Authentication and Authorization Configuration<br>Device Configuration Control<br>Actions Based on Device Identity<br>Device Integrity<br>Secure Network Onboarding Support<br>Interface Control | 9. Allow robust device management | M |

| Reference | | | CoP principle | Overlap |
|---|---|---|---|---|
| | CS-AEI<br>CS-AUP<br>CS-EIM<br>CS-EVR<br>CS-LCT<br>CS-LSR<br>CS-RDL<br>CS-SRT<br>DS-COM | Access to Event Information<br>Audit Support and Protection<br>Event Identification and Monitoring<br>Event Response<br>Logging Capture and Trigger Support<br>Audit Log Storage and Retention<br>Support of Required Data<br>Support for Reliable Time<br>Secure Communication | 10. Provide security logging, alerting and monitoring capabilities | H |
| | CS-EVR<br>DP-STO | Event Response<br>Secure Storage | 11. Enable recovery to a known good state | M |
| **EN 18031 Parts 1-3** [17][18][19] | Req. SUM-2 (Parts 1, 2, 3)<br>Req. SUM-3 (Parts 1, 2, 3)<br>Req. CRY-1 (Parts 1, 2, 3) | | 1. Provide updates, securely | M |
| | Req. ACM-2 (Parts 1, 2, 3)<br>Req. AUM-1-1 (Parts 1, 2, 3)<br>Req. AUM-1-2 (Parts 1, 2, 3)<br>Req. AUM-2 (Part 1)<br>Req. AUM-2-1 (Parts 2, 3)<br>Req. AUM-3 (Parts 1, 2, 3)<br>Req. AUM-4 (Parts 1, 2, 3)<br>Req. AUM-5-1 (Parts 1, 2, 3) [RED-restricted, see footnote 2]<br>Req. AUM-5-2 (Parts 1, 2, 3) [RED-restricted, see footnote 2]<br>Req. AUM-6 (Parts 1, 2, 3)<br>Req. CCK-2 (Parts 1, 2, 3)<br>Req. CCK-3 (Parts 1, 2, 3)<br>Req. CRY-1 (Parts 1, 2, 3) | | 2. Support appropriate authentication | H |
| | Req. SSM-1 (Parts 1, 2, 3)<br>Req. SSM-3 (Parts 1, 2, 3)<br>Req. SCM-1 (Parts 1, 2, 3)<br>Req. SCM-2 (Parts 1, 2, 3)<br>Req. SCM-3 (Parts 1, 2, 3)<br>Req. SCM-4 (Parts 1, 2, 3)<br>Req. CCK-3 (Parts 1, 2, 3)<br>Req. CRY-1 (Parts 1, 2, 3)<br>Req. DLM-1 (Part 2) | | 3. Protect data at rest and data in transit | H |
| | Req. SUM-2 (Parts 1, 2)<br>Req. SUM-2 (Part 3) [RED-restricted, see footnote 3]<br>Req. SSM-1 (Parts 1, 2, 3)<br>Req. GEC-8 (Part 3) | | 4. Maintain device integrity | H |
| | Req. ACM-2 (Parts 1, 2, 3) | | 7. Minimize the privilege and reach of applications | M |

[2] As per EC Guidance on the application of the EN 18031 standards [20]: "This harmonised standard does not confer a presumption of conformity with Article 3(3), first subparagraph, point (d), (e) and (f), of Directive 2014/53/EU if, by applying its clauses 6.2.5.1 and 6.2.5.2, the user is allowed not to set and use any password."

[3] As per EC Guidance on the application of the EN 18031 standards [20]: "As regards the assessment criteria set out in clause 6.3.2.4 of this harmonised standard, this harmonised standard does not confer a presumption of conformity with the essential requirement set out in Article 3(3), first subparagraph, point (f), of Directive 2014/53/EU."

| Reference | | CoP principle | Overlap |
|---|---|---|---|
| | Req. GEC-3 (Parts 1, 2, 3)<br>Req. GEC-4 (Parts 1, 2, 3)<br>Req. GEC-5 (Parts 1, 2, 3) | 8. Constrain the use of all device interfaces | H |
| | Req. NMM-1 (Part 1)<br>Req. LGM-1 (Parts 2, 3)<br>Req. LGM-4 (Parts 2, 3)<br>Req. UNM-1 (Part 2) | 10. Provide security logging, alerting and monitoring capabilities | M |