FITSI Federal Body of Knowledge Guide

An Overview of the Federal Body of Knowledge (FBK) for the Federal IT Security Professional (FITSP) Certification Program

Version 2.0

Published 8/8/2017
# TABLE OF CONTENTS

1. EXECUTIVE OVERVIEW ................................................................................................................. 4

3. FEDERAL BODY OF KNOWLEDGE OVERVIEW ........................................................................ 5

3. HOW FITSP USES THE FEDERAL BODY OF KNOWLEDGE .................................................. 6

4. FBK BREAKDOWN ......................................................................................................................... 7

   DOMAINS ........................................................................................................................................ 7
   Domain 1 – NIST Special Publications ......................................................................................... 7
   Domain 2 - NIST Federal Information Processing Standards ....................................................... 9
   Domain 3 - NIST Control Families ............................................................................................. 9
   Domain 4 - Government Laws and Regulations .......................................................................... 10
   Domain 5 - NIST Risk Management Framework (formerly C&A) ............................................ 15
   Domain 6 - NIST Interagency Reports ....................................................................................... 15

   IT SECURITY TOPIC AREAS ........................................................................................................ 17
   Topic Area 1 – Access Control. .................................................................................................... 17
   Topic Area 2 – Audit and Accountability ..................................................................................... 17
   Topic Area 3 – Awareness and Training ....................................................................................... 18
   Topic Area 4 – Configuration Management ................................................................................ 18
   Topic Area 5 – Contingency Planning ......................................................................................... 19
   Topic Area 6 – Identification and Authentication ....................................................................... 19
   Topic Area 7 – Incident Response ............................................................................................... 20
   Topic Area 8 – Maintenance ........................................................................................................ 20
   Topic Area 9 – Media Protection .................................................................................................. 21
   Topic Area 10 – Personnel Security ............................................................................................ 21
   Topic Area 11 – Physical and Environmental Protection ............................................................ 21
   Topic Area 12 – Planning ............................................................................................................. 22
   Topic Area 13 – Program Management ....................................................................................... 22
   Topic Area 14 – Risk Assessment ............................................................................................... 23
   Topic Area 15 – Security Assessments and Authorization ........................................................... 24
   Topic Area 16 – System and Communication Protection ............................................................ 24
   Topic Area 17 – System and Information Integrity ...................................................................... 25
   Topic Area 18 – System and Services Acquisition ...................................................................... 25

Copyright 2009-2017 FITSI
1. Executive Overview

The Federal Body of Knowledge (FBK)* is a library of federal statutes, regulations, standards, and guidelines that federal workforce security professionals are required to use in protecting and defending systems owned by or operated on behalf of the federal government. Provided by the Federal IT Security Institute (FITSI), the purpose of this document is to help provide interested parties with an understanding of what constitutes the FBK. This document can be used for general knowledge or by Federal IT Security Professional (FITSP) candidates to help augment their study in pursuit of one of the four FITSP certifications (Manager, Designer, Operator, Auditor).

This guide is updated periodically and is meant to provide a high-level description of the body of knowledge that forms the basis of the exams.

This document is available free of charge at the following FITSI website: http://www.fitsi.org/documents. It may be forwarded to professional colleagues but must be kept in its original form.

Important note: This document includes an overview of the FBK that establishes the boundary of knowledge that cuts across all four FITSP certifications. Candidates are not expected to have read and understood all of the publications listed.

* The FBK incorporates themes, concepts, and documents focused on unclassified federal information systems.
3. Federal Body of Knowledge Overview

The FBK* is broken down into six domains and 18 IT security topic areas.

Domains
1. Domain 1 – NIST Special Publications
2. Domain 2 – NIST Federal Information Processing Standards (FIPS)
3. Domain 3 – NIST Control Families
4. Domain 4 – Governmental Laws and Regulations
5. Domain 5 – NIST Risk Management Framework
6. Domain 6 – NIST Interagency Reports

IT Security Topic Areas**
1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Configuration Management
5. Contingency Planning
6. Identification and Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Personnel Security
11. Physical and Environmental Protection
12. Planning
13. Program Management
14. Risk Assessment
15. Security Assessment and Authorization
   a. (Formerly Certification, Accreditation, and Security Assessments)
16. System and Communications Protection
17. System and Information Integrity
18. System and Services Acquisition

* The FBK incorporates themes, concepts, and documents focused on unclassified federal information systems.

** Seventeen of the 18 IT Security topic areas are derived directly from the minimum control requirements defined in Federal Information Processing Standard 200 (FIPS 200), one is from NIST SP 800-53 (Appendix G, Program Management).
3. How FITSP uses the Federal Body of Knowledge

Domains are the boundaries of knowledge that apply to the federal government. The IT Security topic areas include themes and skills that IT security professionals are expected to understand. *The FITSP role based exams for Manager, Designer, Operator and Auditor include questions that cover the intersection between the six domains and the 18 IT security topic areas (see illustration below).*

The interwoven nature of the domains and topic areas are below. Only five out of the 18 topic areas are present for illustration purposes.

<table>
<thead>
<tr>
<th>Domain 1</th>
<th>Domain 2</th>
<th>Domain 3</th>
<th>Domain 4</th>
<th>Domain 5</th>
<th>Domain 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST Special Publications</td>
<td>NIST FIPS</td>
<td>NIST Control Families</td>
<td>Government Laws and Regulations</td>
<td>NIST RMF</td>
<td>NIST Interagency Reports</td>
</tr>
</tbody>
</table>

- **Topic Area #1 – Access Control**
- **Topic Area #2 – Audit and Accountability**
- **Topic Area #3 – Awareness and Training**
- **Topic Area #4 – Configuration Management**
- **Topic Area #5 – Incident Response**
4. FBK Breakdown

The purpose of this section is to provide the reader with a broad overview of the domains and topic areas. Because the exam focuses on federal statutes, regulations, standards, and guidelines, this guide provides a breakdown for each FITSP domain and topic area.

This document provides the reader a reference on what constitutes the boundary of the FBK.

Domains

Domain 1 – NIST Special Publications

NIST Special Publications are written to provide guidance and best practices to federal agencies on how to protect the agency’s missions, business functions, and environment of operation. These publications are downloadable for free at the following website: http://csrc.nist.gov.

2. 800-13 - Telecommunications Security Guidelines for Telecommunications Management Network
3. 800-14- Generally Accepted Principles and Practices for Securing Information Technology Systems
4. 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
6. 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
7. 800-24 - PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
8. 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
10. 800-28 Version 2 - Guidelines on Active Content and Mobile Code
12. 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure
13. 800-33 - Underlying Technical Models for Information Technology Security
15. 800-35 - Guide to Information Technology Security Services
16. 800-36 - Guide to Selecting Information Technology Security Products
18. 800-40 Rev. 3 - Guide to Enterprise Patch Management Technologies
19. 800-41Rev 1 - Guidelines on Firewalls and Firewall Policy
20. 800-44 Version 2 - Guidelines on Securing Public Web Servers
22. 800-46 Rev. 2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
25. 800-49 - Federal S/MIME V3 Client Profile
27. 800-52 Rev. 1 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
28. 800-53 Rev 4 - Security and Privacy Controls for Federal Information Systems and Organizations
29. 800-53A Rev. 4 - Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
31. 800-57 Part 1 Rev. 4 - Recommendation for Key Management, Part 1: General
32. 800-57 Part 2 - Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
33. 800-57 Part 3 Rev. 1 - Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
35. 800-61 Rev. 2 - Computer Security Incident Handling Guide
36. 800-63-3 - Digital Identity Guidelines
37. 800-63A - Digital Identity Guidelines: Enrollment and Identity Proofing
38. 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management
39. 800-63C - Digital Identity Guidelines: Federation and Assertions
40. 800-64 Rev 2 - Security Considerations in the System Development Life Cycle
41. 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process
43. 800-70 Rev. 3 - National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
44. 800-77 - Guide to IPSec VPNs
45. 800-78-4 - Cryptographic Algorithms and Key Sizes for Personal Identity Verification
46. 800-79-2 - Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)
47. 800-81-2 - Secure Domain Name System (DNS) Deployment Guide
49. 800-83 Rev. 1 - Guide to Malware Incident Prevention and Handling for Desktops and Laptops
50. 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
51. 800-86 - Guide to Integrating Forensic Techniques into Incident Response
52. 800-87 Rev 1 - Codes for Identification of Federal and Federally-Assisted Organizations
53. 800-88 Rev. 1 - Guidelines for Media Sanitization
55. 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
56. 800-95 - Guide to Secure Web Services
57. 800-96 - PIV Card to Reader Interoperability Guidelines
61. 800-101 Rev. 1 - Guidelines on Mobile Device Forensics
62. 800-107 - Recommendation for Applications Using Approved Hash Algorithms
63. 800-111 - Guide to Storage Encryption Technologies for End User Devices
64. 800-113 - Guide to SSL VPNs
65. 800-114 Rev. 1 - User's Guide to Telework and Bring Your Own Device (BYOD) Security
68. 800-119 - Guidelines for the Secure Deployment of IPv6
69. 800-121 Rev. 2 - Guide to Bluetooth Security
70. 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
71. 800-123 - Guide to General Server Security
72. 800-124 Rev. 1 - Guidelines for Managing the Security of Mobile Devices in the Enterprise
73. 800-125 - Guide to Security for Full Virtualization Technologies
75. 800-127 - Guide to Securing WiMAX Wireless Communications
77. 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
78. 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
79. 800-145 - The NIST Definition of Cloud Computing
80. 800-146 - Cloud Computing Synopsis and Recommendations
81. 800-147 - BIOS Protection Guidelines
82. 800-150 - Guide to Cyber Threat Information Sharing
83. 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
84. 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
86. 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations
87. 800-167 - Guide to Application Whitelisting
88. 800-171 Rev. 1 - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
89. 800-181 - NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education
90. 800-183 - Networks of 'Things'
91. 800-184 - Guide for Cybersecurity Event Recovery

Domain 2 - NIST Federal Information Processing Standards

The FBK includes the list of all NIST Federal Information Processing Standards (FIPS). These standards are downloadable at the following website: http://csrc.nist.gov.

1. FIPS 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
2. FIPS 201-2 - Personal Identity Verification (PIV) of Federal Employees and Contractors
3. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
4. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
5. FIPS 198-1 - The Keyed-Hash Message Authentication Code
6. FIPS 197 - Advanced Encryption Standard
7. FIPS 186-4 - Digital Signature Standard (DSS)
8. FIPS 180-4 - Secure Hash Standard (SHS)
9. FIPS 140-2 - Security Requirements for Cryptographic Modules

Domain 3 - NIST Control Families

NIST SP 800-53 identifies 18 IT security control families used in the design of federal information systems. These control families are separated into three categories of controls (management, technical and operational).

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Security Assessment and Authorization
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response  
9. Maintenance  
10. Media Protection  
11. Physical and Environmental Protection  
12. Planning  
13. Personnel Security  
14. Risk Assessment  
15. System and Services Acquisition  
16. System and Communication Protection  
17. System and Information Integrity  
18. Program Management (organization level)

Domain 4 - Government Laws and Regulations

Listed below are the Acts of Congress, OMB memos, executive orders and presidential directives that impact federal IT systems. Acts of Congress, executive orders, and presidential directive are available on the Internet. OMB memos and bulletins are downloadable from http://www.whitehouse.gov/omb.

1. Acts of Congress

   a) Privacy Act of 1974  
   b) Paperwork Reduction Act of 1980  
      a. 44 USC § 3501, et. seq.  
   c) Computer Security Act of 1987  
      a. Replaced by FISMA and is no longer in effect  
   d) Chief Financial Officers Act of 1990  
   e) Government Performance and Results Act of 1993  
   f) Paperwork and Elimination Act of 1998  
   g) Government Information Security Reform Act  
      a. Replace by FISMA and is no longer in effect  
   h) Federal Information Security Management Act of 2002  
   i) Health Insurance Portability and Accountability Act  
   j) Clinger-Cohen Act of 1996  
   l) National Cybersecurity Protection Act of 2014  
   m) Cybersecurity Workforce Assessment Act of 2014  
   n) Cybersecurity Enhancement Act of 2014  
   o) Federal Information Technology Acquisition Reform Act of 2015

2. Council of the Inspectors General for Integrity and Efficiency (CIGIE)

   a) IG FISMA ISCM Maturity Model Assessment Framework

3. DHS Binding Operational Directives

   a) BOD 15-01, Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems
b) BOD 16-01, Securing High Value Assets  
c) BOD 16-02, Threat to Network Infrastructure Devices  
d) BOD 16-03, 2016 Agency Cybersecurity Reporting Requirements

4. DHS Federal Information Security Memorandum

a) FISM 14-01 - Fiscal Year 2014 Metrics for the Federal Information Security Management Act of 2002 and Agency Privacy Management Act and Operational Reporting Instructions  
b) FISM 12-02 - FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management  
c) FISM 12-01 - Protected BIOS for New Procurements of Desktop and Laptop Computers  
d) FISM 11-02 - FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

5. DHS FISMA Documents

a) FY17 CIO Annual FISMA Metrics  
b) FY17 IG FISMA Metrics  
c) FY16 CIO Annual FISMA Metrics  
d) FY16 IG FISMA Metrics  
e) FY16 SAOP FISMA Metrics  
f) FY15 CIO Annual FISMA Metrics  
g) FY15 IG FISMA Metrics  
h) FY15 SAOP FISMA Metrics  
i) FY15 CIO Q3 FISMA Metrics  
j) FY15 CIO Q2 FISMA Metrics  
k) FY15 CIO Q1 FISMA Metrics

6. Executive Orders

a) EO - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure  
b) EO 13636 - Improving Critical Infrastructure Cybersecurity  
c) EO 12958 – Classified National Security Information  
d) 36 Code of Federal Regulation Part 1236, Management of Vital Records, revised as of July 1, 2000  
e) 41 Code of Federal Regulations 101.20.103-4, Occupant Emergency Program, revised as of July 1, 2000  
f) EO 12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions  
g) EO 12656 – Assignment of Emergency Preparedness Responsibilities  
h) EO 13231 – Critical Infrastructure Protection in the Information Age

7. Federal Audit Standards

a) Government Audit Standards (Yellow Book)  
b) GAO / PCIE Financial Audit Manual (FAM)  
c) GAO Federal Information Systems Control Audit Manual (FISCAM)
8. Federal CIO Council Guidance
   e) Federated Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0

9. FedRAMP Program Management Documents
   a) FedRAMP Security Assessment Framework Version 2.1

    a) HSPD-3 – Homeland Security Advisory System
    b) HSPD-5 – Management of Domestic Incidents
    c) HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection
    d) HSPD-8 – National Preparedness
    e) HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors
    f) HSPD-20/NSPD-51 – National Continuity Policy
    g) HSPD-24 – Biometrics for Identification and Screening to Enhance National Security

11. National Initiative for Cybersecurity Education (NICE)
    a) NICE Framework 2.0

12. NIST Cyber Security Framework Documents
    a) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0

13. OMB Circular
    a) Office of Management and Budget Circular A-11, Preparation, Submission and Execution of the Budget, June 2008
    b) Office of Management and Budget Circular A-123, Management Responsibility for Internal Control, December 2004
    d) Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016

14. OMB Memoranda
    1) M-17-26, Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda
    2) M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
    3) M-17-15, Rescission of Memoranda Relating to Identity Management
    4) M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
    5) M-17-09, Management of Federal High Value Assets
6) M-17-06, Policies for Federal Agency Public Websites and Digital Services
8) M-16-24, Role and Designation of Senior Agency Officials for Privacy
9) M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
10) M-16-15, Federal Cybersecurity Workforce Strategy
11) M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government
13) M-16-02, Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops
14) M-15-14, Management and Oversight of Federal Information Technology
16) M-14-16, Guidance on Managing Email
18) M-14-03, Enhancing the Security of Federal Information and Information Systems
19) M-13-13, Open Data Policy - Managing Information as an Asset
20) M-12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
22) M-11-29, Chief Information Officer Authorities
26) M-11-06, WikiLeaks - Mishandling of Classified Information
27) M-11-02, Sharing Data While Protecting Privacy
28) M-10-31, Immediate Review of Information Technology Projects
29) M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)
30) M-10-27, Information Technology Investment Baseline Management Policy
31) M-10-26, Immediate Review of Financial Systems IT Projects
32) M-10-25, Reforming the Federal Government's Efforts to Manage Information Technology Projects
33) M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
35) M-10-10, Federal Agency Coordination on Health Information Technology (HIT)
36) M-09-32 – Update on the Trusted Internet Connections Initiative
38) M-09-02 - Information Technology Management Structure and Governance Framework
39) M-08-27 - Guidance for Trusted Internet Connection (TIC) Compliance
40) M-08-23 - Securing the Federal Government’s Domain Name System Infrastructure
41) M-08-22 - Guidance on the Federal Desktop Core Configuration (FDCC)
43) M-08-16 – Guidance for Trusted Internet Connection Statement of Capability Form (SOC)
44) M-08-09 – New FISMA Privacy Reporting Requirements for FY 2008
45) M-08-05 - Implementation of Trusted Internet Connections (TIC)
M-08-01 - HSPD-12 Implementation Status
M-07-18 - Ensuring New Acquisitions Include Common Security Configurations
M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
M-07-11 - Implementation of Commonly Accepted Security Configurations for Windows Operating Systems
M-07-06 - Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials
Recommendations for Identity Theft Related Data Breach Notification
M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
M-06-18 - Acquisition of Products and Services for Implementation of HSPD-12
M-06-16 - Protection of Sensitive Agency Information
M-06-15 - Safeguarding Personally Identifiable Information
M05-16 - Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings
M-05-08 - Designation of Senior Agency Officials for Privacy
M-05-05 - Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
M-05-04 - Policies for Federal Agency Public Websites
M-04-26 - Personal Use Policies and “File Sharing” Technology
M-04-16 - Software Acquisition
M-04-04 - E-Authentication Guidance for Federal Agencies
M-02-09 - Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones
M-02-01 - Guidance for Preparing and Submitting Security Plans of Action and Milestones
M-01-24 - Reporting Instructions for the Government Information Security Reform Act
M-01-08 - Guidance on Implementing the Government Information Security Reform Act
M-01-05 - Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
M-00-13 - Privacy Policies and Data Collection on Federal Web Sites
M-00-10 - OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act
M-00-07 - Incorporating and Funding Security in Information Systems Investments
M-00-01 - Day One Planning and Request for Updated Business Continuity and Contingency Plans
M-99-20 - Security of Federal Automated Information Resources
M-99-18 - Privacy Policies on Federal Web Sites
M-99-16 - Business Continuity and Contingency Planning for the Year 2000
Domain 5 - NIST Risk Management Framework (formerly C&A)

The Risk Management Framework deals with system authorization and is in NIST Special Publication 800-37 Rev1 and supporting documents. These special publications and standards are downloadable at the following website: http://csrc.nist.gov.

2. SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems
4. 800-53 Rev4 - Recommended Security Controls for Federal Information Systems
7. 800-59 - Guideline for Identifying an Information System as a National Security System
8. 800-60 Rev1 - Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)
11. 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
12. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
13. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems

Domain 6 - NIST Interagency Reports

NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. These NISTIRs are downloadable at the following website: http://csrc.nist.gov.

1. NISTIR 8170 - The Cybersecurity Framework - Implementation Guidance for Federal Agencies
2. NISTIR 8062 - An Introduction to Privacy Engineering and Risk Management in Federal Systems
3. NISTIR 8060 - Guidelines for the Creation of Interoperable Software Identification (SWID) Tags
4. NISTIR 8053 - De-Identification of Personal Information
7. NISTIR 7946 - CVSS Implementation Guidance
8. NISTIR 7864 - The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities
9. NISTIR 7800 - Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains
10. NISTIR 7799 - Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications
13. NISTIR 7694 - Specification for Asset Reporting Format 1.1
14. NISTIR 7693 - Specification for Asset Identification 1.1
15. NISTIR 7692 - Specification for the Open Checklist Interactive Language (OCIL) Version 2.0
17. NISTIR 7511 - Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements
19. NISTIR 7435 - The Common Vulnerability Scoring System (CVSS) and its Applicability to Federal Agency Systems
21. IR 7358 - Program Review for Information Security Management Assistance (PRISMA)
22. IR 7298 - Glossary of Key Information Security Terms
**IT Security Topic Areas**

The purpose of this listing is to provide a basic understanding of key terms and concepts rather than offer an exhaustive list. Knowledge of these terms and concepts is the foundation for effective performance of job functions associated with each of the management, operational and technical topic areas.

Seventeen of the 18 IT Security topic areas come from the requirements defined in the Federal Information Processing Standard 200 (FIPS 200). One of the topic areas, Program Management, is new and comes from NIST SP 800-53 (Appendix G).

**Topic Area 1 – Access Control**

This topic area refers to the knowledge and understanding that 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.

- Access
- Access Authority
- Access Control
- Access Control List
- Account Management
- Access Enforcement
- Authorization
- Brute Force
- Concurrent Session Control
- Discretionary Access Control (DAC)
- Information Flow Enforcement
- Least Privilege
- Mandatory Access Control (MAC)
- Permitted Actions
- Previous Login Notification
- Role Based Access Control (RBAC)
- Security Attributes
- Separation of Duties
- Session Lock
- Session Termination
- System Use Notification
- Unsuccessful Login Attempt

**Topic Area 2 – Audit and Accountability**

This topic area refers to the knowledge and understanding that organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

- Accountability
- Auditable Event
- Audit
- Audit Analysis
- Audit Data
- Audit Review
- Audit Trail
- Audit Storage Capacity
- Audit Failure Response
- Contents of Audit Record
### Topic Area 3 – Awareness and Training

This topic area refers to the knowledge and understanding that organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

- Awareness (Information Security)
- Behavioral Outcome
- Certification
- Computer Based Training (CBT)
- Curriculum
- Education (Information Security)
- End User Security Training
- Information Sharing
- Instructional Systems Design (ISD)
- Instructor Led Training (ILT)
- IT Security Awareness
- IT Security Awareness and Training Program
- IT Security Education
- IT Security Training Program
- Learning Management System (LMS)
- Learning Objectives
- Needs Assessment (IT Security)
- Role-Based Training
- Testing
- Training (Information Security)
- Training Assessment
- Training Effectiveness
- Training Effectiveness Evaluation
- Web Based Training (WBT)

### Topic Area 4 – Configuration Management

This topic area refers to the knowledge and understanding that organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

- Access Restriction for Change
- Baseline Configuration
- Configuration Change
- Configuration Management Plan
- Configuration Management Policy
- Configuration Setting
- Federal Desktop Core Configuration
- Least Functionality
- Security Checklists
- Security Impact Analysis
### Topic Area 5 – Contingency Planning

This topic area refers to the knowledge and understanding that organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

- Alternate Processing / Storage Site
- Backup Strategy
- Business Continuity Plan
- Business Impact Analysis
- Business Recovery Plan
- Call Tree
- Cold Site
- Contingency Plan
- Contingency Plan Policy
- Contingency Plan Training
- Contingency Plan Testing
- Continuity of Operations Plan
- Continuity of Support Plan
- Crisis Communication
- Cyber Incident Response
- Delegation of Authority
- Disaster Recovery Plan
- Disruption
- Essential Functions
- Hot Site
- Information Technology
- Interoperable Communications
- Mission Assurance
- Occupant Emergency Plan
- Order of Succession
- Preparedness/Readiness
- Reconstitution
- Recovery
- Risk Mitigation
- Standard Operating Procedures
- Telecommunications Services
- Threat Environment
- Vital Records and Databases
- Warm Site

### Topic Area 6 – Identification and Authentication

This topic area refers to the knowledge and understanding that organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

- Authenticate
- Authentication
- Authentication Mechanism
- Authentication Mode
- Authentication Protocol
- Authentication Token
- Authenticator Feedback
- Authenticator Management
- Authenticity
- Biometric
- Biometric System
- Biometric Information
- Device Authentication
- Device Identification
- Digital Certificate
- Certificate Policy
- Certificate Revocation List (CRL)
- Certification Authority
- Claimant
- Credential
- Cryptographic Module Authentication
- Electronic Authentication
- Identification
- Identifier Management
- Mutual Authentication
Topic Area 7 – Incident Response

This topic area refers to the knowledge and understanding that organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

- Attack Signature
- Computer Forensics
- Computer Security Incident
- Computer Security Incident Response Team
- Computer Security
- Escalation Procedures
- Honey Pot
- Incident Handling
- Incident Monitoring
- Incident Records
- Incident Reporting
- Incident Response Assistance
- Incident Response Plan
- Incident Response Policy
- Incident Response Testing
- Incident Response Training
- Intrusion
- Intrusion Prevention System
- Intrusion Detection System
- Measures
- Personally Identifiable Information (PII)
- Reconstitution of System
- Security Alerts
- Security Incident
- System Compromise
- Threat Motivation
- Unauthorized Access
- Vulnerability

Topic Area 8 – Maintenance

This topic area refers to the knowledge and understanding that organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

- Antivirus Software
- Backup
- Baseline
- Configuration Management
- Controlled Maintenance
- Insider Threat
- Maintenance Tools
- Maintenance Personnel
- Non-Local Maintenance
- Patch Management
- Penetration Testing
- Security Data Analysis
- Security Measures
- Security Reporting
- System Hardening
- System Logs
- System Maintenance Policy
- System Monitoring
- Threat Analysis
- Threat Monitoring
- Timely Maintenance
- Vulnerability Analysis
Topic Area 9 – Media Protection

This topic area refers to the knowledge and understanding that organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

• Degaussing  • Media Protection Policy
• Media Access  • Media Storage
• Media Destruction  • Media Transport
• Media Marking  • Sanitization

Topic Area 10 – Personnel Security

This topic area refers to the knowledge and understanding that organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

• Access Agreement  • Personnel Security Policy
• Background Checks  • Personnel Screening
• Background Investigation  • Personnel Termination
• Confidentiality  • Personnel Transfer
• Digital Identity  • Security Breach
• Human Resources  • Security Clearance
• Insider Threat  • Separation of Duties
• Job Rotation  • Social Engineering
• Nondisclosure Agreement  • Special Background Investigation (SBI)
• Position Categorization  • Suitability Determination
• Position Sensitivity  • Third-Party Personnel Security
• Personnel Sanctions

Topic Area 11 – Physical and Environmental Protection

This topic area refers to the knowledge and understanding that organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

• Access Cards  • Inventory
• Access Control

Copyright 2009-2017 FITSI  FITSI Federal Body of Knowledge Guide v2.0
Topic Area 12 – Planning

This topic area refers to the knowledge and understanding that organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

- Privacy Impact Assessment
- Rules of Behavior
- Security Planning Policy
- Security Planning Procedures
- Security Related Activity Planning
- System Security Plan

Topic Area 13 – Program Management

This topic area refers to the knowledge and understanding that organizations are required to implement security program management controls to provide a foundation for the organization’s information security program.

- Critical Infrastructure Plan
- Enterprise Architecture
- Information Security Measures of Performance
- Information Security Program Plan
- Information Security Resources
- Information System Inventory
- Mission/Business Process Definition
- Security Authorization Process
- Senior Information Security Officer
- Plan of Action and Milestones Process
- Risk Management Strategy
**Topic Area 14 – Risk Assessment**

This topic area refers to the knowledge and understanding that organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

| • Acceptable Risk                  | • Risk Limitation                |
| • Assessment                      | • Risk Management                |
| • Asset Valuation                 | • Risk Matrix                   |
| • Business Impact Analysis        | • Risk Mitigation               |
| • Controls                        | • Risk Research                 |
| • Impact                          | • Risk Scale                    |
| • Inside Threat                   | • Risk Transference             |
| • Likelihood Determination        | • Security Categorization       |
| • National Vulnerability Database | • Security Controls             |
| • Qualitative                     | • Security Measures             |
| • Quantitative                    | • Threat                       |
| • Risk                            | • Threat and Vulnerability      |
| • Risk Assessment                 | • Threat Modeling               |
| • Risk Assessment Policy          | • Types of Risk                 |
| • Risk Avoidance                  | • Vulnerability                 |
| • Risk Level                      | • Vulnerability Scanning        |
Topic Area 15 – Security Assessments and Authorization

(Formerly Certification, Accreditation, and Security Assessments)

This topic area refers to knowledge and understanding that organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

- Assessment Method
- Assessment Procedure
- Authorization (to operate)
- Authorization Boundary
- Authorize Process
- Authorizing Official
- Designated Representative
- Dynamic Subsystem
- Common Control Provider
- Common Control
- Compensating Control
- Complex Information System
- Continuous Monitoring
- Cost Effective
- Critical Control
- External Subsystems
- Hybrid Security Control
- Information Owner/Steward
- Information System Boundary
- Information System Owner
- Information System Security Engineer
- Information Type
- Interconnection Agreement
- Net-centric Architecture
- Plan of Action and Milestones (POAM)
- Reciprocity
- Risk Executive
- Security Control Assessor
- Senior Information Security Officer
- Tailored Security Control Baseline
- Volatile Control

Topic Area 16 – System and Communication Protection

This topic area refers to the knowledge and understanding that organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

- Application Partitioning
- Boundary Protection
- Collaborative Computing Devices
- Communications Security
- Configuration
- Covert Channel Analysis
- Cryptographic Key Establishment
- Cryptographic Key Management
- Defense-in-Depth
- Denial of Service Protection
- Penetration Testing
- Port
- Protection of Information at Rest
- Public Access Protections
- Public Key Infrastructure Certificates
- Resource Priority
- Router
- Secure Name Resolution
- Security Function Isolation
- Security Trust
Topic Area 17 – System and Information Integrity

This topic area refers to the knowledge and understanding that organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Information Input Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Software</td>
<td>Information Output Handling and Retention</td>
</tr>
<tr>
<td>Application</td>
<td>Information System Monitoring</td>
</tr>
<tr>
<td>Application Content Filtering</td>
<td>Macro Virus</td>
</tr>
<tr>
<td>Blended Attack</td>
<td>Malicious Code Protection</td>
</tr>
<tr>
<td>Boot Sector Virus</td>
<td>Predictable Failure Prevention</td>
</tr>
<tr>
<td>Buffer Overflow</td>
<td>Security Alerts, Advisories, and Directives</td>
</tr>
<tr>
<td>Computer Virus</td>
<td>Security Functionality Verification</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Spam Protection</td>
</tr>
<tr>
<td>Flaw Remediation</td>
<td>Software and Information Integrity</td>
</tr>
<tr>
<td>Information Input Restrictions</td>
<td>System and Information Integrity Policy</td>
</tr>
</tbody>
</table>

Topic Area 18 – System and Services Acquisition

This topic area refers to the knowledge and understanding that organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
<table>
<thead>
<tr>
<th>Acquisitions</th>
<th>Risk Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation of Resources</td>
<td>Risk-Based Decision</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>Risk Mitigation</td>
</tr>
<tr>
<td>Contract</td>
<td>Security Engineering Principles</td>
</tr>
<tr>
<td>Cost-Benefit Analysis</td>
<td>Security Requirements</td>
</tr>
<tr>
<td>Critical Information System Components</td>
<td>Service Level Agreement (SLA)</td>
</tr>
<tr>
<td>Developer Configuration Management</td>
<td>System and Services Acquisition Policy</td>
</tr>
<tr>
<td>Developer Security Testing</td>
<td>Software usage Restrictions</td>
</tr>
<tr>
<td>Disposal</td>
<td>Solicitation</td>
</tr>
<tr>
<td>External Information System Services</td>
<td>Supply Chain Protection</td>
</tr>
<tr>
<td>Information System Documentation</td>
<td>Statement of Objectives (SOO)</td>
</tr>
<tr>
<td>Life Cycle Support</td>
<td>Statement of Work (SOW)</td>
</tr>
<tr>
<td>Prequalification</td>
<td>Total Cost of Ownership (TCO)</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>Trustworthiness</td>
</tr>
<tr>
<td>Request for Information</td>
<td>User Installed Software</td>
</tr>
<tr>
<td>Request for Proposal (RFP)</td>
<td></td>
</tr>
</tbody>
</table>