UNIVERSITY SYSTEM OF GEORGIA

CROSSWALK: A USG IT HANDBOOK COMPANION GUIDE

VERSION 3.0

3/1/2023

PUBLIC

Abstract: The purpose of this companion guideline is to complement the *USG IT Handbook* by providing a NIST Cybersecurity Framework (CSF) centered perspective with the corresponding standards and regulations cross-walked to the CSF.

REVISION & SIGN-OFF

Change Record

Date	Author	Version	Change Reference
20200722	Alfred Barker	1.0	Reviewed – Added NIST 800-171 – and –
			Updated PCI V3 to V3.2.1.
20200805	Alfred Barker	1.0	Reviewed for Harmful Language.
20201003	Alfred Barker	2.0	Reordered and minor editing to improve usage.
20230301	Alfred Barker	3.0	Updated CIS CSC v7 to v8

Document Properties

Item	Details
Document Title	Crosswalk: A USG IT Handbook Companion Guide
Document Type	Guideline (Internal Use Only)
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	20200224
Last Updated	20230301
Document Classification	Public

TABLE OF CONTENTS

INTRODUCTION

This guideline is classified as Public and was developed for internal use. The purpose of the guideline is to complement the *USG IT Handbook* by providing a NIST Cybersecurity Framework (CSF) centered perspective with the corresponding federal and state standards and regulations crosswalked to the CSF, the NIST Privacy Framework and the USG Business Procedures Manual where appropriate. The University System of Georgia (USG) has chosen to align with National Institute of Standards and Technology (NIST) standards and guidelines in the development of their cybersecurity program. This is intentional as many federal regulations map to NIST. More specifically, the U.S. Department of Education (ED) has mandated that all institutions of higher education entities (IHE) are to demonstrate Gramm-Leach-Bliley Act (GLBA) compliance through the implementation of NIST SP 800-171 Rev1. Failure to demonstrate compliance can result in IHEs losing the ability to administer federal student financial aid. Moreover, the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) has decided that GLBA compliance is to be a determining factor in accreditation. Failure to demonstrate compliance here can result in the loss of accreditation. The regulations mapped are defined in Appendix A. Abbreviations are used and are defined in Appendix B, which provides a short-hand clean way to capture the information. Every effort has been taken to provide versioning information as well.

The guide was designed to allow the user to first locate the USG *IT Handbook* section and determine if it maps to either the NIST Cybersecurity Framework (or the NIST Privacy Framework). If a section does map to the framework, make note of the framework section ID – PR.IP-2 for example – and locate the framework crosswalk's section ID to review all the references associated. An extra effort was taken to locate and map the Georgia State policies and standards governing state-agencies in support of the Georgia Cybersecurity Board initiatives.

As with all our documents, they are dynamic and considered works in progress. If you discover an error or have an additional standard or regulation that the community would benefit from mapping, please submit your comment to cybersecurity@usg.edu for correction or consideration.

USG IT HANDBOOK CROSSWALK TO NIST CYBERSECURITY FRAMEWORK (CSF)/PRIVACY FRAMEWORK (PF)

Section 1. Information Technology (IT) Governance

CIO role and responsibilities, IT governance structure, IT roles and responsibilities, strategic planning and resource management.

1.4.3: Development and Acquisition Standards

System Development Life Cycle to manage systems is implemented.

References:

- CSF v1.1, PR.IP-2
- PF v1.0, CT.PO-P4

1.5: Resource Management

Capacity and data availability managed.

References:

- CSF v1.1, PR.DS-4
- PF v1.0, PR.DS-P4

Section 2. Project and Service Administration

Service administration, project administration and project documentation.

2.1.3 Service Support

Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

References:

- CSF v1.1, PR.MA-1
- PF v1.0, PR.MA-P1

Section 3. Information Technology Management

Information system user account management, log management, continuity of operations planning and network services standards.

3.1.1: Information System User Account Management

Identities/credentials issued, managed, verified, revoked, and audited for authorized devices, users and processes; identities and credentials confirmed; and, cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

References:

- CSF v1.1, PR.AC-1, PR.AC-6, PR.IP-11
- PF v1.0, PR.AC-P1, PR.AC-P6, PR.PO-P9

3.1.1.1 Information System User Account Management Procedures

Critical systems identification plan and communicated. Access permissions/authorizations are managed, using principles of least privilege and separation of duties.

References:

- CSF v1.1, ID.BE-2, PR.AC-4
- PF v1.0, PR.AC-P4

3.1.2: Managing Multifactor Authentication

Critical systems identification plan and communicated and Authentication of authorized devices (MFA).

References:

- CSF v1.1, ID.BE-2, PR.AC-7
- PF v1.0, PR.AC-P6

3.2: Log Management

Purpose, objectives and standards. Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools; and audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

References:

- CSF v1.1, PR.PT-1
- PF v1.0, CT.DM-P8, PR.MA-P1

3.3.1: USG Continuity of Operations Planning Standard

Recovery planning. Backups of information are conducted, maintained, and tested. Recovery plans executed on or after incident.

References:

- CSF v1.1, PR.IP-4, RC.RP-1
- PF v1.0, PR.PO-P3

Recovery plans includes lessons learned, and recovery strategies updated.

References:

- CSF v1.1, RC.IM-1, RC.IM-2

Communications. Public relations managed, reputation repaired after incident, and recovery activities are communicated to internal, external stakeholders and executive, management teams.

References:

- CSF v1.1, RC.CO-1, RC.CO-2, RC.CO-3

Incident Response/Business Continuity and Incident Recovery/Disaster Recovery plans are in place and managed.

References:

- CSF v1.1, PR.IP-9
- PF v1.0, PR.PO-P7

Critical systems dependencies established and communicated.

References:

- CSF v1.1, ID.BE-4

3.4.1: Network Services Standard

Communications and control networks are protected.

References:

- CSF v1.1, PR.PT-4
- PF v1.0, PR.PT-P3

SECTION 5. CYBERSECURITY

Program charter, organization and administration, incident management, asset management, risk management, systems categorization, information classification, endpoint security, awareness training, required reporting, password security, DNS security and email use and protection.

5.0: Charter

Effectiveness of protection technologies is shared.

References:

- CSF v1.1, PR.IP-8
- PF v1.0, PR.PO-P7

5.1: USG Cybersecurity Program

Priorities for mission, objectives, and activities established and communicated.

References:

- CSF v1.1, ID.BE-3
- PF v1.0, ID.BE-P2

Cybersecurity policy and organizational responsibilities are established and communicated.

References:

- CSF v1.1, ID.GV-1
- PF v1.0, GV.PO-P1

5.1.3 Policy, Standards, Processes, and Procedure Management Requirements

Configuration change control processes are in place.

References:

- CSF v1.1, PR.IP-3
- PF v1.0, PR.PO-P2

Cybersecurity roles and responsibilities for workforce and third-party stakeholders are established.

References:

- CSF v1.1, ID.AM-6

- PF v1.0, GV.PO-P3

Communication and data flows mapped (diagrams).

References:

- CSF v1.1, ID.AM-3
- PF v1.0, ID.IM-P8

Data-at-rest is protected.

References:

- CSF v1.1, PR.DS-1
- PF v1.0, PR.DS-P1

A vulnerability management plan is developed and implemented.

References:

- CSF v1.1, PR.IP-12
- PF v1.0, PR.PO-P10

Removable media is protected, and its use restricted according to policy.

References:

- CSF v1.1, PR.PT-2
- PF v1.0, PR.PT-P1

The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

References:

- CSF v1.1, PR.PT-3
- PF v1.0, PR.PT-P2

A baseline of network operations and expected data flows for users and systems is established and managed.

References:

- CSF v1.1, DE.AE-1

Vulnerability scans are performed.

- CSF v1.1, DE.CM-8

5.1.4: Appropriate Usage Policy (AUP) Guidelines

Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

References:

- CSF v1.1, ID.GV-2
- PF v1.0, GV.PO-P4

5.2.1: Cybersecurity Organization

Role in the data processing ecosystem identified and communicated.

References:

- CSF v1.1, ID.BE-1
- PF v1.0, ID.BE-P1

5.2.2: Information Security Officer (ISO)

Cybersecurity policy is established and communicated.

References:

- CSF v1.1, ID.GV-1
- PF v1.0, GV.PO-P1

5.3: Incident Management

Incident Response/Business Continuity and Incident Recovery/Disaster Recovery plans are in place and managed.

References:

- CSF v1.1, PR.IP-9
- PF v1.0, PR.PO-P7

Response and recovery plans are tested.

References:

- CSF v1.1, PR.IP-10
- PF v1.0, PR.PO-P8

Roles and responsibilities for detection are well defined to ensure accountability.

References:

- CSF v1.1, DE.DP-1

Response plan is executed during or after an incident.

References:

- CSF v1.1, RS.RP-1

5.3.1 Cybersecurity Incident Response Plan Requirements

Response plans includes lessons learned.

References:

- CSF v1.1, RS.IM-1

Response strategies updated.

References:

- CSF v1.1, RS.IM-2

Incidents are mitigated.

References:

- CSF v1.1, RS.MI-2

Notifications from detection systems are investigated.

References:

- CSF v1.1, RS.AN-1

Impact of the incident is understood.

References:

- CSF v1.1, RS.AN-2

Incidents are categorized consistent with response plans.

References:

- CSF v1.1, RS.AN-4

Incidents are contained.

References:

- CSF v1.1, RS.MI-1

Detection activities comply with all applicable requirements.

References:

- CSF v1.1, DE.DP-2

Detection processes are tested.

References:

- CSF v1.1, DE.DP-3

Event detection information is communicated.

References:

- CSF v1.1, DE.DP-4

Detection processes are continuously improved.

References:

- CSF v1.1, DE.DP-5

Incident alert thresholds are established.

References:

- CSF v1.1, DE.AE-5

5.3.2: Cybersecurity Incident Reporting Requirements

Incidents are reported consistent with established criteria.

References:

- CSF v1.1, RS.CO-25.

Event detection information is communicated.

- CSF v1.1, DE.DP-4

5.3.3: Incident Follow-up Report

Information is shared consistent with response plans.

References:

- CSF v1.1, RS.CO-3

5.3.4: Incidents Involving Personal Information

Personnel know their roles and order of operations when a response is needed.

References:

- CSF v1.1, RS.CO-1, PR.IP-9

Incident Response/Business Continuity and Incident Recovery/Disaster Recovery plans are in place and managed.

References:

- CSF v1.1, PR.IP-9, RS.CO-1
- PF v1.0, PR.PO-P7

5.3.5: USG Computer Security Incident Management Requirements

Personnel know their roles and order of operations when a response is needed.

References:

- CSF v1.1, RS.CO-1

5.3.6: USG Incident Response and Reporting Requirements

Information is shared consistent with response plans.

References:

- CSF v1.1, RS.CO-3

5.4: USG Information Asset Management and Protection

Physical devices and systems within the organization are inventoried.

References:

- CSF v1.1, ID.AM-1
- PF v1.0, ID.IM-P1, P2, P7

Assets are formally managed throughout removal, transfers, and disposition.

References:

- CSF v1.1, PR.DS-3
- PF v1.0, PR.DS-P3

5.4.1: USG Information Asset Management Requirements

Software platforms and applications within the organization are inventoried.

References:

- CSF v1.1, ID.AM-2
- PF v1.0, ID.IM-P1, P7

Asset vulnerabilities are identified and documented.

References:

- CSF v1.1, ID.RA-1

System Development Life Cycle to manage systems is implemented.

References:

- CSF v1.1, PR.IP-2
- PF v1.0, CT.PO-P4

5.4.2: USG Information Asset Protection Requirements

Identities/credentials issued, managed, verified, revoked, and audited for authorized devices, users and processes.

References:

- CSF v1.1, PR.AC-1
- PF v1.0, PR.AC-P1

5.5.1: USG Organizations Responsibilities

Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

References:

- CSF v1.1, ID.GV-2
- PF v1.0, GV.PO-P4

5.5.2: Risk Assessment and Analysis

Critical systems identification plan and communicated.

References:

- CSF v1.1, ID.BE-2

Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

References:

- CSF v1.1, ID.RA-5
- PF v1.0, ID.RA-P4

Threats, both internal and external, are identified and documented.

References:

- CSF v1.1, ID.RA-3

Potential business impacts and likelihoods are identified.

References:

- CSF v1.1, ID.RA-4
- PF v1.0, ID.RA-P4

Risk responses are identified and prioritized.

References:

- CSF v1.1, ID.RA-6
- PF v1.0, ID.RA-P5

Detected events are analyzed to understand attack targets and methods.

References:

- CSF v1.1, DE.AE-2

Event data are collected and correlated from multiple sources and sensors.

References:

- CSF v1.1, DE.AE-3

Impact of events is determined.

References:

- CSF v1.1, DE.AE-4

Newly identified vulnerabilities are mitigated or documented as accepted risks.

References:

- CSF v1.1, RS.MI-3

5.5.3: USG Organizations Risk Management Programs

Governance and risk management processes address cybersecurity risks.

References:

- CSF v1.1, ID.GV-4
- PF v1.0, GV.PO-P6

5.5.4: USG Risk Management Requirements

Governance and risk management processes address cybersecurity risks.

References:

- CSF v1.1, ID.GV-4
- PF v1.0, GV.PO-P6

5.5.5: USG Cybersecurity Risk Management Process

Risk management processes are established, managed, and agreed to by organizational stakeholders.

References:

- CSF v1.1, ID.RM-1
- PF v1.0, GV.RM-P1

The network is monitored to detect potential cybersecurity events.

References:

- CSF v1.1, DE.CM-1

Malicious code is detected.

References:

- CSF v1.1, DE.CM-4

The physical environment is monitored to detect potential cybersecurity events.

References:

- CSF v1.1, DE.CM-2

Personnel activity is monitored to detect potential cybersecurity events.

References:

- CSF v1.1, DE.CM-3

Unauthorized mobile code is detected.

References:

- CSF v1.1, DE.CM-5

5.6: USG Information System Categorization

Policy and regulations regarding the physical operating environment for organizational assets are met.

References:

- CSF v1.1, PR.IP-5
- PF v1.0, PR.PO-P4

5.6.1: Security Categories

Policy and regulations regarding the physical operating environment for organizational assets are met.

References:

- CSF v1.1, PR.IP-5
- PF v1.0, PR.PO-P4

5.6.2: Requirements

Policy and regulations regarding the physical operating environment for organizational assets are met.

References:

- CSF v1.1, PR.IP-5
- PF v1.0, PR.PO-P4

5.7: USG Classification of Information

Resources are prioritized based on their classification, criticality, and business value.

References:

- CSF v1.1, ID.AM-5

5.8: Endpoint Security

Physical devices and systems within the organization are inventoried.

- CSF v1.1, ID.AM-1
- PF v1.0, ID.IM-P1, P2, P7

Monitoring for unauthorized personnel, connections, devices, and software is performed.

- CSF v1.1, DE.CM-7

5.8.1: Purpose

Physical devices and systems within the organization are inventoried.

References:

- CSF v1.1, ID.AM-1
- PF v1.0, ID.IM-P1, P2, P7

5.8.2: Discovery and Inventory

Physical devices and systems within the organization are inventoried.

References:

- CSF v1.1, ID.AM-1
- PF v1.0, ID.IM-P1, P2, P7

5.8.3: Anti-virus, Anti-malware, Anti-spyware Controls

Malicious code is detected.

References:

- CSF v1.1, DE.CM-4

5.8.4: Operating System (OS) / Application Patch Management

Baseline configuration of IT systems created and maintained incorporating concept of least functionality.

- CSF v1.1, PR.IP-1
- PF v1.0, PR.PO-P1

5.8.5 Maintenance

Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

- CSF v1.1, PR.MA-1
- PF v1.0, PR.MA-P1

Remote asset maintenance is approved, logged, and performed in a manner that prevents unauthorized access.

- CSF v1.1, PR.MA-2
- PF v1.0, PR.MA-P2

5.9: Security Awareness, Training and Education

All users are informed and trained.

- CSF v1.1, PR.AT-1
- PF v1.0, GV.AT-P1

5.9.1 Roles and Responsibilities

Privileged/Administrators understand roles & responsibilities.

- CSF v1.1, PR.AT-2
- PF v1.0, GV.AT-P1

3rd Party Users understand roles & responsibilities.

- CSF v1.1, PR.AT-3
- PF v1.0, GV.AT-P4

Senior executives understand their roles & responsibilities.

- CSF v1.1, PR.AT-4
- PF v1.0, GV.AT-P2

Physical and Cybersecurity roles & responsibilities

- CSF v1.1, PR.AT-5

Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

- CSF v1.1, ID.GV-2
- PF v1.0, GV.PO-P4

5.9.2: Security Awareness, Training and Education Requirements

All users are informed and trained.

- CSF v1.1, PR.AT-1
- PF v1.0, GV.AT-P1

5.10: Required Reporting

Response and recovery plans are tested.

References:

- CSF v1.1, PR.IP-10
- PF v1.0, PR.PO-P8

5.10.1: Required Reporting Activities

System Development Life Cycle to manage systems is implemented.

References:

- CSF v1.1, PR.IP-2
- PF v1.0, CT.PO-P4

Event detection information is communicated.

References:

- CSF v1.1, DE.DP-4

5.10.2: Cybersecurity Program Review

Priorities for mission, objectives, and activities established and communicated.

References:

- CSF v1.1, ID.BE-3
- PF v1.0, ID.BE-P2

Governance and risk management processes address cybersecurity risks.

References:

- CSF v1.1, ID.GV-4
- PF v1.0, GV.PO-P6

5.11.2: Anti-virus, Anti-spam, and Anti-phishing Software

Malicious code is detected.

References:

- CSF v1.1, DE.CM-4

5.11.3: Host-based Firewall or Host-based Intrusion Prevention Software

Network integrity is protected, network segregation, network segmentation.

References:

- CSF v1.1, PR.AC-5
- PF v1.0, PR.AC-P5

5.11.4: Passwords

Identities/credentials issued, managed, verified, revoked, and audited for authorized devices, users and processes.

References:

- CSF v1.1, PR.AC-1
- PF v1.0, PR.AC-P1

5.11.5: Encrypted Authentication

Remote access is managed.

References:

- CSF v1.1, PR.AC-3
- PR.AC-P3

5.11.6: Physical Security

Physical access to assets is managed and protected.

References:

- CSF v1.1, PR.AC-2
- PF v1.0, PR.AC-P2

5.11.7: Unnecessary Services

The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

References:

- CSF v1.1, PR.PT-3
- PF v1.0, PR.PT-P2

5.11.8: Integrity and Segmentation

Hardware integrity checking implemented.

References:

- CSF v1.1, PR.DS-8
- PF v1.0, PR.DS-P8

Network integrity is protected, network segregation, network segmentation.

References:

- CSF v1.1, PR.AC-5
- PF v1.0, PR.AC-P5

5.12.1: User Access Controls

Access permissions/authorizations are managed, using principles of least privilege and separation of duties.

References:

- CSF v1.1, PR.AC-4
- PF v1.0, PR.AC-P4

5.12.2: USG Password Authentication Standard

Remote access is managed.

References:

- CSF v1.1, PR.AC-3
- PF v1.0, PR.AC-P3

5.12.3: USG Password Security and Composition Requirement

Remote access is managed.

References:

- CSF v1.1, PR.AC-3
- PF v1.0, PR.AC-P3

5.14: Information Protection Management

Legal, regulatory, privacy, and civil liberties requirements regarding cybersecurity are understood and managed to include identifying, detecting and responding to red flags.

References:

- CSF v1.1, ID.GV-3

- PF v1.0, GV.PO-P5

5.14.5: Protecting Personal Information

Data-at-rest is protected.

References:

- CSF v1.1, PR.DS-1
- PF v1.0, PR.DS-P1

Data in transit is protected.

References:

- CSF v1.1, PR.DS-2
- PF v1.0, PR.DS-P2

Data is destroyed according to policy.

References:

- CSF v1.1, PR.IP-6
- PF v1.0, CT.DM-P5

Protection processes are improved.

References:

- CSF v1.1, PR.IP-7
- PF v1.0, PR.PO-P6

5.15: Email Use and Protection

Communications and control networks are protected.

References:

- CSF v1.1, PR.PT-4
- PF v1.0, PR.PT-P3

SECTION 6. DATA PRIVACY

Purpose, standard, applicability (collection and use) and compliance; Web privacy standard; and data privacy risks.

6.1: USG Data Privacy Standard

Legal, regulatory, privacy, and civil liberties requirements regarding cybersecurity are understood and managed.

- CSF v1.1, ID.GV-3
- PF v1.0, GV.PO-P5

SECTION 8. MOBILE DEVICE MANAGEMENT

Purpose, applicability, standards, non-compliance and declaration.

8.1: General Requirements to Manage Mobile Devices

Remote access is managed.

- CSF v1.1, PR.AC-3
- PF v1.0, PR.AC-P3

Data-at-rest is protected.

- CSF v1.1, PR.DS-1
- PF v1.0, PR.DS-P1

Data in transit is protected.

- CSF v1.1, PR.DS-2
- PF v1.0, PR.DS-P2

NIST CYBERSECURITY FRAMEWORK CROSSWALK TO REFERENCES

IDENTIFY (ID)

ASSET MANAGEMENT (ID.AM)

The data, personnel, devices, systems, and facilities that enable USG organizations to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. To demonstrate this, USG organizations must ensure:

ID.AM-1: Physical Inventory

Physical devices and systems within the organization are inventoried.

References:

- CIS CSC V8, 1.1
- COBIT 5, BAI09.01-02
- FERPA (PTAC), Inventory of Assets
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)
- ISO/IEC 27001:2013, A.8.1.1-2
- NIST Privacy Framework V1.0, ID.IM-P1, P2, P7
- NIST SP 800-53 Rev. 4, CM-8, PM-5
- NIST SP 800-171 Rev. 1, 3.4.1
- PCI DSS V3.2.1, 2.4, 9.9, 11.1.1, 12.3.3
- State PSG, PS-08-002
- USG IT Handbook V2.9.7, 5.4, 5.8

ID.AM-2: Software Inventory

Software platforms and applications within the organization are inventoried.

References:

- CIS CSC V8, 2.1-2, 16.4
- COBIT 5, BAI09.01-02, 05
- FERPA (PTAC), Inventory of Assets
- GLBA (NIST SP 800-171 REV. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A)&(E)
- ISO/IEC 27001:2013, A.8.1.1-2, A.12.5.1
- NIST Privacy Framework V1.0, ID.IM-P1, P7
- NIST SP 800-53 Rev. 4, CM-8
- NIST SP 800-171 Rev. 1, 3.4.1
- PCI DSS V3.2.1, 2.4, 12.3.7
- State PSG, PS-08-002
- USG IT Handbook V2.9.7, 5.4.1

ID.AM-3: Data Flow Diagram

Organizational communication and data flows are mapped.

References:

- CIS CSC V8, 3.8
- COBIT 5, DSS05.02
- GLBA (NIST SP 800-171 REV. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)
- ISO/IEC 27001:2013, A.13.2.1
- NIST Privacy Framework V1.0, ID.IM-P8
- NIST SP 800-53 Rev. 4, AC-4, CA-3, CA-9, PL-8
- NIST SP 800-171 Rev. 1, 3.1.3, 3.13.1
- PCI DSS 3.2.1, 1.1.2-3
- USG IT Handbook V2.9.7, 5.1.3

ID.AM-4: Systems Catalogue

External information systems are catalogued.

References:

- CIS CSC V8, 12.4
- COBIT 5, APO02.02, APO10.4, DSS01.02
- GLBA (NIST SP 800-171 REV. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)
- ISO/IEC 27001:2013, A.11.2.6
- NIST Privacy Framework V1.0, ID.IM-P2, P7
- NIST SP 800-53 Rev. 4, AC-20, SA-9
- NIST SP 800-171 Rev. 1, 3.1.20-21
- PCI DSS V3.2.1, 1.1.1-3, 2.4

ID.AM-5: Prioritize Resource

Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.

References:

- CIS CSC V8, 3.2, 3.7
- COBIT 5, APO03.03-04, APO12.01, BAI04.02, BAI09.02
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)
- ISO/IEC 27001:2013, A.8.2.1
- NIST SP 800-53 Rev. 4, CP-2, RA-2, SA-14, SC-6
- PCI DSS V3.2.1, 9.6.1, 12.2
- State PSG, SS-08-002, SS-08-014, PS-08-012,
- USG Business Procedures Manual, 12
- USG IT Handbook V2.9.7, 5.7

ID.AM-6: Role and Responsibility

Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.

References:

- CIS CSC V8, 14.1
- COBIT 5, APO01.02, APO07.06, APO13.01, DSS06.03
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2)-(4), 164.308(b)(1), 164.314
- ISO/IEC 27001:2013, A.6.1.1
- NIST Privacy Framework V1.0, GV.PO-P3
- NIST SP 800-53 Rev. 4, CP-2, PS-7, PM-11
- PCI DSS V3.2.1, 12.4-5, 12.8-9
- USG IT Handbook V2.9.7, 5.1.3

BUSINESS ENVIRONMENT (ID.BE)

USG organization's must understand and prioritize its mission, objectives, stakeholders, and activities; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. To achieve this, USG organizations must verify:

ID.BE-1: Supply Chain Role

USG organization's role in the supply chain is identified and communicated where applicable.

References:

- COBIT 5, APO08.01,04-05, APO10.03-5
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
- ISO/IEC 27001:2013, A.15.1.1-3, A.15.2.1-2
- NIST Privacy Framework V1.0, ID.BE-P1
- NIST SP 800-53 Rev. 4, CP-2, SA-12
- USG IT Handbook V2.9.7, 5.2.1

ID.BE-2: Critical Infrastructure

USG organization's role in the critical infrastructure is identified and communicated where applicable.

References:

- COBIT 5, APO02.06, APO03.01
- FERPA (PTAC), Layered Defense
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
- ISO/IEC 27001:2013 Clause 4.1
- NIST SP 800-53 Rev. 4, PM-8
- USG IT Handbook V2.9.7, 3.1, 5.5

ID.BE-3: Mission, Objectives and Activities

Priorities for organizational mission, objectives, and activities are established and communicated.

References:

- COBIT 5, APO02.01, APO02.06, APO03.01
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.316

- NIST Privacy Framework V1.0, ID.BE-P2
- NIST SP 800-53 Rev. 4, PM-11, SA-14
- USG IT Handbook V2.9.7, 5.1, 5.10

ID.BE-4: Dependencies

Dependencies and critical functions for delivery of critical services are established.

References:

- COBIT 5, BAI03.02, DSS04.02
- FERPA (PTAC), Layered Defense
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308.(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)
- ISO/IEC 27001:2013, A.11.2.2, A.11.2.3, A.12.1.3
- NIST SP 800-53 Rev. 4, CP-8, PE-9, PE-11, PM-8, SA-14
- USG IT Handbook V2.9.7, 3.3.1

ID.BE-5: Contingency Planning

Resilience requirements to support delivery of critical services are established.

References:

- COBIT 5, BAI03.02, DSS04.02
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(b)(2)(i)
- ISO/IEC 27001:2013, A.11.1.4, A.17.1.1-2, A.17.2.1
- NIST SP 800-53 Rev. 4, CP-2, CP-11, SA-13-14

GOVERNANCE (ID.GV)

USG policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk by ensuring:

ID.GV-1: Policy, Plans and Procedures

Organizational cybersecurity policy is established.

References:

- CIS CSC V8, 4.1
- COBIT 5, APO01.03, APO13.01, EDM01.01-2
- FERPA (PTAC), Policy and Governance
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.316
- NIST Privacy Framework V1.0, GV.PO-P1
- NIST SP 800-53 Rev. 4, Controls from all families
- PCI DSS V3.2.1, 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
- State PSG, SS-08-001, PS-08-003.2
- USG IT Handbook V2.9.7, 5.1, 5.2

ID.GV-2: Roles and Responsibilities

Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners.

References:

- CIS CSC V8, 15.2, 17.4
- COBIT 5, APO01.02, APO10.03, APO13.12, DSS05.04
- FERPA (PTAC), Personnel Security
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2)-(4), 164.308(b), 164.314
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.1, A.15.1.1
- NIST Privacy Framework V1.0, GV.PO-P4
- NIST SP 800-53 Rev. 4, PM-1-2, PS-7
- PCI DSS v3.2.1 12.4, 12.5, 12.8, 12.9
- State PSG, SS-08-001, PS-08-003.2
- USG Business Procedures Manual, 12
- USG IT Handbook V2.9.7, 5.1, 5.5, 5.9

ID.GV-3: Compliance Management

Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

References:

- COBIT 5, BAI02.01, MEA03.01, MEA03.04
- HIPAA Security Rule 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, 164.314, 164.316
- ISO/IEC 27001:2013, A.18.1.1-5
- NIST Privacy Framework V1.0, GV.PO-P5
- NIST SP 800-53 Rev. 4, Controls from all families
- PCI DSS v3.2.1, 3.1, 12.10
- State PSG, SS-08-001, PS-08-003.2
- USG Business Procedures Manual, 12
- USG IT Handbook V2.9.7, 5.14, 6.1, 6.2

ID.GV-4: Risk Management Plan

Governance and risk management processes address cybersecurity risks.

References:

- COBIT 5, EDM03.02, APO12.03,05, DSS04.02
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1), 164.308(b)
- ISO/IEC 27001:2013, Clause 6
- NIST Privacy Framework V1.0, GV.PO-P6
- NIST SP 800-53 Rev. 4, SA-2, PM-3,7,9-11
- PCI DSS v3.2.1, 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1, 12.2
- USG IT Handbook V2.9.7, 5.5, 5.10

RISK ASSESSMENT (ID.RA)

USG organizations must understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. This is achieved by verifying:

ID.RA-1: Vulnerability Assessment

Asset vulnerabilities are identified and documented.

References:

- CIS CSC V8, 7.1-2, 7.4
- COBIT 5, APO12.01-04, DSS05.01-02
- FERPA (PTAC), Audit and Compliance Monitoring, Secure Configuration, Automated Vulnerability Scanning
- GLBA (NIST SP 800-171 REV. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)
- ISO/IEC 27001:2013, A.12.6.1, A.18.2.3
- NIST SP 800-53 Rev. 4, CA-2,7-8, RA-3,5, SA-5,11, SI-2,4-5
- NIST SP 800-171 Rev. 1, 3.11.1-2, 3.12.1, 3.12.3, 3.14.1, 3.14.3, 3.14.6-7
- PCI DSS v3.2.1, 6.1, 11.2, 11.3, 12.2
- State PSG, PS-08-031
- USG IT Handbook V2.9.7, 5.4.1

ID.RA-2: Information Sharing

Threat and vulnerability information is received from information sharing forums and sources.

References:

- COBIT 5, BAI08.01
- GLBA (NIST SP 800-171 REV. 1)
- ISO/IEC 27001:2013, A.6.1.4
- NIST SP 800-53 Rev. 4, PM-15-16, SI-5
- NIST SP 800-171 Rev. 1, 3.14.1, 3.14.3
- PCI DSS v3.2.1, 6.1
- State PSG, PS-08-031

ID.RA-3: Threat Assessment)

Threats, both internal and external, are identified and documented.

References:

- COBIT 5, APO12.01-4, PS-08-031
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316
- ISO/IEC 27001:2013, Clause 6.1.2
- NIST SP 800-53 Rev. 4, RA-3, SI-5, PM-12,16
- NIST SP 800-171 Rev. 1, 3.11.1, 3.14.1, 3.14.3

- PCI DSS v3.2.1, 12.2
- State PSG, PS-08-031
- USG IT Handbook V2.9.7, 5.5

ID.RA-4: Impact and Likelihood Assessment

Potential business impacts and likelihoods are identified.

References:

- COBIT 5, DSS04.02
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.316(a)
- ISO/IEC 27001:2013, A16.1.6, Clause 6.1.2
- NIST Privacy Framework V1.0, ID.RA-P4
- NIST SP 800-171 Rev. 1, 3.11.1
- NIST SP 800-53 Rev. 4, RA-2-3, PM-9,11, SA-14
- PCI DSS v3.2.1, 6.1
- State PSG, PS-08-031
- USG IT Handbook V2.9.7, 5.5

ID.RA-5: Risk Assessment

Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

References:

- CIS CSC V8, 3.7, 7.6
- COBIT 5, APO12.02
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.316(a)
- ISO/IEC 27001:2013, A.12.6.1
- NIST Privacy Framework V1.0, ID.RA-P4
- NIST SP 800-53 Rev. 4, RA-2-3, PM-16
- NIST SP 800-171 Rev. 1, 3.11.1
- PCI DSS v3.2.1, 12.2
- State PSG, PS-08-031
- USG IT Handbook V2.9.7, 5.5

ID.RA-6: Response Assessment

Risk responses are identified and prioritized.

References:

- COBIT 5, APO12.04-05, APO13.02
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)
- ISO/IEC Clause 6.1.3
- NIST Privacy Framework V1.0, ID.RA-P5
- NIST SP 800-53 Rev. 4, PM-4,9
- PCI DSS v3.2.1, 12.10.1

- State PSG, PS-08-031
- USG IT Handbook V2.9.7, 5.5

RISK MANAGEMENT STRATEGY (ID.RM)

USG organizations must ensure priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. This is demonstrated by showing:

ID.RM-1: Risk Management Procedures

Risk management processes are established, managed, and agreed to by organizational stakeholders.

References:

- COBIT 5, APO12.04-05, APO13.02, BAI02.03, BAI04.02
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)
- ISO/IEC 27001: 2013, Clause 6.1.3, Clause 8.3, Clause 9.3
- NIST Privacy Framework V1.0, GV.RM-P1
- NIST SP 800-53 Rev. 4, PM-9
- PCI DSS v3.2.1, 12.2
- State PSG, PS-08-031, SS-08-041
- USG IT Handbook V2.9.7, 5.5

ID.RM-2: Risk Tolerance

Organizational risk tolerance is determined and clearly expressed.

References:

- COBIT 5, APO12.06
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)
- ISO/IEC 27001:2013, Clause 6.1.3, Clause 8.3
- NIST Privacy Framework V1.0, GV.RM-P2
- NIST SP 800-53 Rev. 4, PM-9
- PCI DSS v3.2.1, 12.2
- State PSG, PS-08-031

ID.RM-3: Strategic Analysis

The organization's determination of risk tolerance is informed by its role in the IHE sector specific risk analysis.

References:

- COBIT 5 APO12.02
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C),164.308(a)(7)(ii)(E), 164.310(a)(2)(i)
- ISO/IEC 27001:2013, Clause 6.1.3, Clause 8.3
- NIST Privacy Framework V1.0, GV.RM-P3
- NIST SP 800-53 Rev. 4, PM-8-9,11, SA-14
- PCI DSS v3.2.1, 12.2
- State PSG, PS-08-031

PROTECT (PR)

ACCESS CONTROL (PR.AC)

USG organizations must demonstrate access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. This is achieved by ensuring:

PR.AC-1: Identities and Credentials

Identities and credentials are managed for authorized devices and users.

References:

- CIS CSC V8, 7.7, 5.1, 5.3, 5.5, 6.1-2, 6.6-7, 13.9, 15.7
- COBIT 5, DSS05.04, DSS06.03
- FERPA (PTAC), Authentication
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
- ISO/IEC 27001:2013, A.9.2.1-2,4, A.9.3.1, A.9.4.2-3
- NIST Privacy Framework V1.0, PR.AC-P1
- NIST SP 800-53 Rev.4, AC-1-2, IA-1-11
- NIST SP 800-171 Rev. 1, 3.5.1-2, 3.5.5-11
- PCI DSS v3.2.1, 2.1, 8.1, 8.2, 8.5, 8.6, 12.3
- USG IT Handbook V2.9.7, 3.1, 5.4, 5.11

PR.AC-2: Physical Access

Physical access to assets is managed and protected.

References:

- COBIT 5, DSS01.04, DSS05.05
- FERPA (PTAC), Physical Security, Secure Configuration
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)
- ISO/IEC 27001:2013, A.11.1.1-6, A.11.2.1,3,5-8
- NIST Privacy Framework V1.0, PR.AC-P2
- NIST SP 800-53 Rev.4, PE-2-6,9
- NIST SP 800-171 Rev. 1, 3.10.1-5
- PCI DSS v3.2.1, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.9, 9.10
- State PSG, PS-08-009, PS-08-013
- USG IT Handbook V2.9.7, 5.11

PR.AC-3: Remote Access

Remote access is managed.

References:

- CIS CSC V8, 4.11, 6.4, 6.6, 12.7, 13.5
- COBIT 5, APO13.01, DSS01.04, DSS05.03
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)
- ISO/IEC 27001:2013, A.6.2.1-2, A.11.2.6, A.13.1.1, A.13.2.1
- NIST Privacy Framework V1.0, PR.AC-P3
- NIST SP 800-53 Rev.4, AC-1,17,19-20, SC-15
- NIST SP 800-171 Rev. 1, 3.1.1-2, 3.1.14-15, 3.1.18, 3.1.20, 3.13.9, 3.13.12
- PCI DSS v3.2.1, 2.3, 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9, 12.3.10
- State PSG, PS-08-009, SS-08-048, PS-08-023, SS-08-038
- USG IT Handbook V2.9.7, 5.11, 5.12, 8.0

PR.AC-4: Access Permissions

Access permissions are managed, incorporating the principles of least privilege and separation of duties.

References:

- CIS CSC V8, 3.2, 5.4, 6.8
- COBIT 5, DSS05.04
- FERPA (PTAC), Access Control
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1,4-5
- NIST Privacy Framework V1.0, PR.AC-P4
- NIST SP 800-53 Rev.4, AC-1-3,5-6,14,16,24
- NIST SP 800-171 Rev. 1, 3.1.1-2, 3.1.4-8, 3.1.10-11, 3.5.3-4, 3.13.3-4
- PCI DSS v3.2.1, 6.4.2, 7.1, 7.2, 8.7, 9.3
- State PSG, PS-09-009, SS-08-010, SS-08-048
- USG Business Procedures Manual, 12
- USG IT Handbook V2.9.7, 3.1, 5.12

PR.AC-5: Segregation and Segmentation

Network integrity is protected, incorporating network segregation where appropriate.

References:

- CIS CSC V8, 3.12, 9.2-3, 9.6, 12.2, 12.8, 13.4, 16.4
- COBIT 5, DSS01.05, DSS05.02
- FERPA (PTAC), Firewalls and IDPS
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)
- ISO/IEC 27001:2013, A.13.1.1,3, A.13.2.1, A.14.1.2,3
- NIST Privacy Framework V1.0, PR.AC-P5
- NIST SP 800-53 Rev.4, AC-4,10, SC-7
- NIST SP 800-171 Rev. 1, 3.1.3, 3.13.1-2, 3.13.5-7
- PCI DSS v3.2.1, 1.1, 1.2, 1.3, 2.2, 6.2, 10.8, 11.3

- State PSG, SS-08-047
- USG IT Handbook V2.9.7, 5.11

PR.AC-6: Identity Proofing

Identities are proofed (verified) and bound to credentials and asserted in interactions.

References:

- COBIT 5, DSS05.04-05, 07, DSS06.03
- FERPA (PTAC), Authentication, Personnel Security
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)
- ISO/IEC 27001:2013, A.7.1.1, A.9.2.1
- NIST Privacy Framework V1.0, PR.AC-P6
- NIST SP 800-53 Rev.4, AC-1-3, 16, 19, 24, IA-1-2, 4-5, 8, PE-2, PS-3
- PCI DSS v3.2.1 7.1.4, 8.1, 8.2.2
- USG IT Handbook V2.9.7, 3.1

PR.AC-7: User and Device Authentication

Users, devices, and other assets are authenticated (e.g., single factor with multifactor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

References:

- CIS CSC V8, 6.3-5, 12.3, 12.6-7, 13.5
- COBIT 5, DSS05.04, 10, DSS06.10
- FERPA (PTAC), Authentication, Mobile Devices
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)
- ISO/IEC 27001:2013, A.9.2.1,4, A.9.3.1, A.9.4.2-3, A.18.1.4
- NIST Privacy Framework V1.0, PR.AC-P6
- NIST SP 800-53 Rev.4, AC-7-9,11-12,14, IA-1-5,8-11
- PCI DSS v3.2.1, 8.2, 8.3
- State PSG, PS-19-001, PS-08-006, SS-08-007, SS-08-008
- USG IT Handbook V2.9.7, 3.1

AWARENESS AND TRAINING (PR.AT)

USG organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. To demonstrate this, USG organizations must show:

PR.AT-1: Awareness Training

All users are informed and trained.

References:

- CIS CSC V8, 14.1-9, 16.9, 17.3
- COBIT 5, APO07.03, BAI05.07
- FERPA (PTAC), Personnel Security

- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(5)
- ISO/IEC 27001:2013, A.7.2.2, A.12.2.1
- NIST Privacy Framework V1.0, GV.AT-P1
- NIST SP 800-53 Rev.4, AT-2, PM-13
- NIST SP 800-171 Rev. 1, 3.2.1-3
- PCI DSS v3.2.1, 6.7, 7.3, 8.4, 9.9.3, 12.4, 12.6
- State PSG, PS-08-010, SS-08-012
- USG IT Handbook V2.9.7, 5.9

PR.AT-2: Roles-Based Training – Privilege Users

Privileged users understand roles & responsibilities.

References:

- CIS CSC V8, 5, 14.9, 16.9
- COBIT 5, APO07.02, DSS05.04, DSS06.03
- FERPA (PTAC), Emailing Confidential Data
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.2
- NIST Privacy Framework V1.0, GV.AT-P1
- NIST SP 800-53 Rev.4, AT-3, PM-13
- NIST SP 800-171 Rev. 1, 3.2.1-2
- PCI DSS v3.2.1, 1.1.5, 7.1, 7.2, 7.3, 12.4, 12.6
- USG IT Handbook V2.9.7, 5.9

PR.AT-3: Roles-Based Training – 3rd Party Stakeholders

Third-party stakeholders (e.g., suppliers, customers, and partners) understand roles & responsibilities.

References:

- CIS CSC V8, 15.4
- COBIT 5, APO07.03,06, APO10.04-05
- FERPA (PTAC), Emailing Confidential Data
- HIPAA Security Rule 45 C.F.R. §§ 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.1-2
- NIST Privacy Framework V1.0, GV.AT-P4
- NIST SP 800-53 Rev.4, PS-7, SA-9,16
- PCI DSS v3.2.1, 12.8.2, 12.9
- USG IT Handbook V2.9.7, 5.9

PR.AT-4: Roles-Based Training – Senior Executives

Senior executives understand roles & responsibilities.

References:

- CIS CSC V8, 14.9
- COBIT 5, EDM01.01, APO01.02, APO07.03

- FERPA (PTAC), Emailing Confidential Data
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.2
- NIST Privacy Framework V1.0, GV.AT-P2
- NIST SP 800-53 Rev.4, AT-3, PM-13
- NIST SP 800-171 Rev. 1, 3.2.1-2
- PCI DSS v3.2.1, 12.4, 12.5
- USG IT Handbook V2.9.7, 5.9

PR.AT-5: Roles-Based Training – Cybersecurity

Physical and information security personnel understand roles & responsibilities.

References:

- CIS CSC V8, 14.9
- COBIT 5, APO07.03
- FERPA (PTAC), Emailing Confidential Data
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.2
- NIST Privacy Framework V1.0, GV.AT-P3
- NIST SP 800-53 Rev.4, AT-3, IR-3, PM-13
- NIST SP 800-171 Rev. 1, 3.2.1-2
- PCI DSS v3.2.1, 12.4, 12.5
- USG IT Handbook V2.9.7, 5.9

DATA SECURITY (PR.DS)

Information and records (data) are managed consistent with the USG organization's risk strategy to protect the confidentiality, integrity, and availability of information. To accomplish this, USG organizations must ensure:

PR.DS-1: Data-at-Rest Protections

Data-at-rest is protected.

References:

- CIS CSC V8, 3.11, 16.11
- COBIT 5, APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)
- ISO/IEC 27001:2013, A.8.2.3
- NIST Privacy Framework V1.0, PR.DS-P1
- NIST SP 800-53 Rev.4, MP-8, SC-12,28
- NIST SP 800-171 Rev. 1, 3.1.19, 3.8.1, 3.8.9, 3.13.10, 3.13.16

- PCI DSS v3.2.1, 3 (all), 8.2.1
- State PSG, SS-08-003, SS-15-002, PS-08-026
- USG IT Handbook V2.9.7, 5.1, 5.14, 8.3

PR.DS-2: Data-in-Transit Protections

Data-in-transit is protected.

References:

- CIS CSC V8, 3.10, 12.3, 12.6, 16.11
- COBIT 5, APO01.06, DSS05.02, DSS06.06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)
- ISO/IEC 27001:2013, A.8.2.3, A.13.1.1, A.13.2.1,3, A.14.1.2-3
- NIST Privacy Framework V1.0, PR.DS-P2
- NIST SP 800-53 Rev.4, SC-8,11-12
- NIST SP 800-171 Rev. 1, 3.1.13, 3.1.17, 3.8.5, 3.13.8, 3.13.10
- PCI DSS v3.2.1, 3 (all), 8.2.1
- State PSG, SS-08-003, PS-08-026
- USG IT Handbook V2.9.7, 5.14, 8.3

PR.DS-3: Inventory, Sanitation and Physical Access

Assets are formally managed throughout removal, transfers, and disposition.

References:

- CIS CSC V8, 1.1, 3.5
- COBIT 5, BAI09.03
- FERPA (PTAC), Inventory of Assets
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
- ISO/IEC 27001:2013, A.8.2.3, A.8.3.1-3, A.11.2.5,7
- NIST Privacy Framework V1.0, PR.DS-P3
- NIST SP 800-53 Rev.4, CM-8, MP-6, PE-16
- NIST SP 800-171 Rev. 1, 3.4.1, 3.8.1-3, 3.8.5
- PCI DSS v3.2.1, 2.4, 9.5, 9.6, 9.7, 9.8, 9.9
- State PSG, SS-08-003, GM-13-001
- USG IT Handbook V2.9.7, 5.4

PR.DS-4: Capacity, Contingency and Protection

Adequate capacity to ensure availability is maintained.

References:

- COBIT 5, APO13.01, BAI04.04
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, A.12.1.3, A.17.2.1

- NIST Privacy Framework V1.0, PR.DS-P4
- NIST SP 800-53 Rev.4, AU-4, CP-2, SC-5
- USG IT Handbook V2.9.7, 1.5

PR.DS-5: Data Leak Protection

Protections against data leaks are implemented.

References:

- CIS CSC V8, 3.13, 16.4
- COBIT 5, APO01.06, DSS05.04,07, DSS06.02
- FERPA (PTAC), Firewalls and IDPS
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)
- ISO/IEC 27001:2013, A.6.1.2, A.7.1.1-2, A.7.3.1, A.8.2.2-3, A.9.1.1-2, A.9.2.3, A.9.4.1,4-5, A.13.1.3, A.13.2.1,3-4, A.14.1.2-3
- NIST Privacy Framework V1.0, PR.DS-P5
- NIST SP 800-53 Rev.4, AC-4-6, PE-19, PS-3,6, SC-7-8,13,31, SI-4
- NIST SP 800-171 Rev. 1, 3.1.4, 3.1.13, 3.2.3, 3.9.2, 3.13.1, 3.13.5-8, 3.13.11, 3.13.16, 3.14.6
- PCI DSS v3.2.1, 10.6

PR.DS-6: Information Integrity Checking

Integrity checking mechanisms are used to verify software, firmware, and information integrity.

References:

- CIS CSC V8, 11.5
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)
- ISO/IEC 27001:2013, A.12.2.1, A.12.5.1, A.14.1.2-3, A.14.2.4
- NIST Privacy Framework V1.0, PR.DS-P6
- NIST SP 800-53 Rev.4, SC-16, SI-7
- PCI DSS v3.2.1, 11.5

PR.DS-7: Testing and Development

The development and testing environment(s) are separate from the production environment.

References:

- CIS CSC V8, 16.8
- COBIT 5, BAI03.08, BAI07.04
- FERPA (PTAC), Network Mapping
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(4)
- ISO/IEC 27001:2013, A.12.1.4
- NIST Privacy Framework V1.0, PR.DS-P7
- NIST SP 800-53 Rev.4, CM-2
- PCI DSS v3.2.1, 6.4.1, 6.4.2
- State PSG, SS-08-031, PS-08-020

PR.DS-8: Integrity Checking Hardware

Integrity checking mechanisms are used to verify hardware integrity.

References:

- CIS CSC V8, 16.14
- COBIT 5, BAI03.05
- ISO/IEC 27001:2013, A.11.2.4
- NIST Privacy Framework V1.0, PR.DS-P8
- NIST SP 800-53 Rev.4, SA-10, SI-7
- PCI DSS v3.2.1, 9.9.2
- USG IT Handbook V2.9.7, 5.11

INFORMATION PROTECTION PROCESSES AND PROCEDURES (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among USG organizations), processes, and procedures are maintained and used to manage protection of information systems and assets. This is accomplished by ensuring:

PR.IP-1: Baselining Configurations

A baseline configuration of information technology is created and maintained.

References:

- CIS CSC V8, 2.7, 4.1-3, 9.4, 9.4, 16.7, 17.7
- COBIT 5, BAI10.01-03,05
- FERPA (PTAC), Network Mapping, Secure Configurations
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)
- ISO/IEC 27001:2013, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2-4
- NIST Privacy Framework V1.0, PR.PO-P1
- NIST SP 800-53 Rev.4, CM-2-7,9, SA-10
- NIST SP 800-171 Rev. 1, 3.4.1-2, 3.4.6-8
- PCI DSS v3.2.1, 1.2, 2.2
- USG IT Handbook V2.9.7, 5.8

PR.IP-2: Life-Cycle Development

A System Development Life Cycle to manage systems is implemented.

References:

- CIS CSC V8, 16.5, 16.10, 16.12
- COBIT 5, APO13.01, BAI03.01-03
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(i)
- ISO/IEC 27001:2013, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
- NIST Privacy Framework V1.0, PR.PO-P4
- NIST SP 800-53 Rev.4, SA-3-4,8,10-12,15,17, PL-8
- PCI DSS v3.2.1, 6.3, 6.4, 6.5, 6.6, 6.7
- State PSG, PM-14-009, SS-08-025, PS-08-018.02
- USG IT Handbook V2.9.7, 1.4, 5.4, 5.10

PR.IP-3: Change Control

Configuration change control processes are in place.

References:

- COBIT 5, BAI01.06, BAI06.01
- FERPA (PTAC), Secure Configurations
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(8)
- ISO/IEC 27001:2013, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2-4
- NIST Privacy Framework V1.0, PR.PO-P2
- NIST SP 800-53 Rev.4, CM-3-4, SA-10
- NIST SP 800-171 Rev. 1, 3.4.3-5
- PCI DSS v3.2.1, 6.4
- State PSG, GM-17-001, PS-08-015, SS-08-026
- USG IT Handbook V2.9.7, 5.1

PR.IP-4: Backup and Recovery

Backups of information are conducted, maintained, and tested periodically.

References:

- CIS CSC v8, 11.2-3
- CMMC v0.6, RE-CO29-P1137
- COBIT 5, APO13.01, DSS01.01, DSS04.07
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)
- ISO/IEC 27001:2013, A.12.3.1, A.17.1.2-3, A.18.1.3
- NIST Privacy Framework V1.0, PR.PO-P3
- NIST SP 800-53 Rev.4, CP-4, CP-6, CP-9
- PCI DSS v3.2.1, 9.5.1, 12.10.1, 12.10.2
- State PSG, PS-08-025, PS-08-026, GM-13-001
- USG IT Handbook V2.9.7, 3.1

PR.IP-5: Compliance

Policy and regulations regarding the physical operating environment for organizational assets are met.

References:

- COBIT 5, DSS01.04, DSS05.05
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)
- ISO/IEC 27001:2013, A.11.1.4, A.11.2.1-3
- NIST Privacy Framework V1.0, PR.PO-P4
- NIST SP 800-53 Rev.4, PE-10,12-15,18
- PCI DSS v3.2.1, 9 (all)
- USG IT Handbook V2.9.7, 5.6

PR.IP-6: Data Destruction

Data is destroyed according to policy.

References:

- CIS CSC V8, 3.1, 3.5
- COBIT 5, BAI09.03, DSS05.06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)
- ISO/IEC 27001:2013, A.8.2.3, A.8.3.1-2, A.11.2.7
- NIST Privacy Framework V1.0, CT.DM-P5
- NIST SP 800-53 Rev.4, MP-6
- NIST SP 800-171 Rev. 1, 3.8.3
- PCI DSS v3.2.1, 3.1, 9.8
- State PSG, SS-08-035
- USG IT Handbook V2.9.7, 5.14

PR.IP-7: Process Improvement

Protection processes are continuously improved.

References:

- CIS CSC V8, 16.14, 18.1
- COBIT 5, APO11.06, APO12.06, DSS04.05
- FERPA (PTAC), Audit and Compliance Monitoring
- HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
- ISO/IEC 27001:2013, A.16.1.6, Clause 9-10
- NIST Privacy Framework V1.0, PR.PO-P6
- NIST SP 800-53 Rev.4, CA-2,7, CP-2, IR-8, PL-2, PM-6
- PCI DSS v3.2.1, 10.8, 12.10.6, 12.11
- State PSG, GM-17-001
- USG IT Handbook V2.9.7, 5.14

PR.IP-8: Information Sharing

Effectiveness of protection technologies is shared with appropriate parties.

References:

- COBIT 5, BAI08.04, DSS03.04
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
- ISO/IEC 27001:2013, A.16.1.6
- NIST Privacy Framework V1.0, PR.PO-P7
- NIST SP 800-53 Rev.4, AC-21, CA-7, SI-4
- State PSG, PM-07-003
- USG IT Handbook V2.9.7, 5.0

PR.IP-9: Incident, Disaster and Business Continuity Plans Implemented

Response plans (Incident Response) and recovery plans (Disaster Recovery) are in place and managed.

References:

- CIS CSC V8, 11.1, 17.1, 17.3-4
- COBIT 5, APO12.06, DSS04.03
- GLBA (NIST SP 800-171 Rev. 1)

- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, A.16.1.1, A.17.1.1-3
- NIST Privacy Framework V1.0, PR.PO-P7
- NIST SP 800-53 Rev.4, CP-2,7,12-13, IR7-9,17
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 11.1.2, 12.5.3, 12.10
- State PSG, SS-08-045, SS-08-046
- USG IT Handbook V2.9.7, 3.3, 5.3

PR.IP-10: Incident, Disaster and Business Continuity Plans Tested

Response and recovery plans are tested.

References:

- CIS CSC V8, 17.7
- COBIT 5, DSS04.04
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(D)
- ISO/IEC 27001:2013, A.17.1.3
- NIST Privacy Framework V1.0, PR.PO-P8
- NIST SP 800-53 Rev.4, CP-4, IR-3, PM-14
- NIST SP 800-171 Rev. 1, 3.6.3
- PCI DSS v3.2.1, 12.10.2
- State PSG, SS-08-046
- USG IT Handbook V2.9.7, 5.3, 5.10

PR.IP-11: Human Resources Practices

Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

References:

- CIS CSC V8, 6.2
- COBIT 5, APO07.01-05
- FERPA (PTAC), Personnel Security
- GLBA (NIST SP 800-171 REV. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(C), 164.308(a)(3)
- ISO/IEC 27001:2013, A.7.1.1-2, A.7.2.1-3, A.7.3.1, A.8.1.4
- NIST Privacy Framework V1.0, PR.PO-P9
- NIST SP 800-53 Rev.4, PS-1-8, SA-21
- NIST SP 800-171 Rev. 1, 3.9.1-2
- PCI DSS v3.2.1, 8.1.3, 9.3, 12.7
- USG IT Handbook V2.9.7, 3.1

PR.IP-12: Vulnerability Management Plan

A vulnerability management plan is developed and implemented.

References:

- CIS CSC V8, 7.6
- COBIT 5, BAI03.10, BAI05.01-02

- FERPA (PTAC), Automated Vulnerability Scanning, Secure Configuration
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)
- ISO/IEC 27001:2013, A.12.6.1, A.14.2.3, A.6.1.3, A.18.2.2-3
- NIST Privacy Framework V1.0, PR.PO-P10
- NIST SP 800-53 Rev.4, RA-3,5, SI-2
- NIST SP 800-171 Rev. 1, 3.11.2-3, 3.12.2-3, 3.14.1-3
- PCI DSS v3.2.1, 6.1, 6.2, 6.5, 11.2
- State PSG, SA-10-010
- USG IT Handbook V2.9.7, 5.1

MAINTENANCE (PR.MA)

Maintenance and repairs of information system components is performed consistent with policies and procedures. USG organizations must show:

PR.MA-1: Maintenance Program

Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.

References:

- COBIT 5, BIA03.10, BAI09.02-03
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)
- ISO/IEC 27001:2013, A.11.1.2, A.11.2.4-6
- NIST Privacy Framework V1.0, PR.MA-P1
- NIST SP 800-53 Rev.4, MA-2-3,5-6
- NIST SP 800-171 Rev. 1, 3.7.1-4, 3.7.6
- PCI DSS v3.2.1, 6.2, 9.9.3
- USG IT Handbook V2.9.7, 2.1, 3.2, 5.8

PR.MA-2: Remote Maintenance Program

Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

References:

- CIS CSC V8, 13.5
- COBIT 5, DSS05.04
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)
- ISO/IEC 27001:2013, A.11.2.4, A.15.1.1, A.15.2.1
- NIST Privacy Framework V1.0, PR.MA-P2
- NIST SP 800-53 Rev.4, MA-4
- NIST SP 800-171 Rev. 1, 3.7.5
- PCI DSS v3.2.1, 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9

- USG IT Handbook V2.9.7, 5.8

PROTECTIVE TECHNOLOGY (PR.PT)

Technical cybersecurity solutions are managed to ensure the cybersecurity and resilience of USG systems and assets, consistent with related policies, procedures, and agreements. USG organizations shall ensure:

PR.PT-1: Log Management

Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

References:

- CIS CSC V8, 8.2, 8.4, 8.8. 8.11
- COBIT 5, APO11.04, BAI03.05, DSS05.04,07, MEA02.01
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)
- ISO/IEC 27001:2013, A.12.4.1-4, A.12.7.1
- NIST Privacy Framework V1.0, CT.DM-P8
- NIST SP 800-53 Rev.4, AU Family
- NIST SP 800-171 Rev. 1, 3.3.1-9
- PCI DSS v3.2.1, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6.1, 10.6.2, 10.7
- State PSG, SS-08-036, PS-08-022
- USG IT Handbook V2.9.7, 3.2

PR.PT-2: Removable Media

Removable media is protected, and its use restricted according to policy.

References:

- CIS CSC V8, 3.9, 10.3
- COBIT 5, APO13.01, DSS05.02,06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)
- ISO/IEC 27001:2013, A.8.2.1-3, A.8.3.1, A.8.3.3, A.11.2.9
- NIST Privacy Framework V1.0, PR.PT-P1
- NIST SP 800-53 Rev.4, MP-2-5,7-8
- NIST SP 800-171 Rev. 1, 3.8.1-8
- PCI DSS v3.2.1, 3.4, 9.5, 9.6, 9.7, 9.8, 12.3, 12.3.10
- State PSG, SS-08-048
- USG IT Handbook V2.9.7, 5.1

PR.PT-3: Least Functionality

Access to systems and assets is controlled, incorporating the principle of least functionality.

References:

- CIS CSC V8, 2.7, 13.10
- COBIT 5, DSS05.02,05-06

- FERPA (PTAC), Unnecessary Services
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)
- ISO/IEC 27001:2013, A.9.1.2
- NIST Privacy Framework V1.0, PR.PT-P2
- NIST SP 800-53 Rev.4, AC-3, CM-7
- NIST SP 800-171 Rev. 1, 3.1.1-2, 3.4.6-8
- PCI DSS v3.2.1, 2.2, 7.1, 7.2, 9.3
- State PSG, SS-08-047
- USG IT Handbook V2.9.7, 5.1, 5.11

PR.PT-4: Network Access Control

Communications and control networks are protected.

References:

- COBIT 5, DSS05.02, APO13.01
- FERPA (PTAC), Firewalls and IDPS
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)
- ISO/IEC 27001:2013, A.13.1.1, A.13.2.1, A.14.1.3
- NIST Privacy Framework V1.0, PR.PT-P3
- NIST SP 800-53 Rev.4, AC-4,17-18, CP-8, SC-7,19-25,29,32,36-41,43
- NIST SP 800-171 Rev. 1, 3.1.16-17, 3.13.1-2, 3.13.5-7, 3.13.15
- PCI DSS v3.2.1, 1 (all), 2 (all)
- State PSG, SS-08-040, PS-08-27
- USG IT Handbook V2.9.7, 3.4, 5.15

PR.PT-5: Fault Tolerance Mechanisms

Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal or adverse situations.

References:

- CIS CSC V8, 11.4
- COBIT 5, BAI04.01-5, DSS01.05
- ISO/IEC 27001:2013, A.17.1.2, A.17.2.1
- NIST Privacy Framework V1.0, PR.PT-P4
- NIST SP 800-53 Rev.4, CP-7-8,11,13, PL-8, SA-14, SC-6
- State PSG, PS-08-026

DETECT (DE)

ANOMALIES AND EVENTS (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood. This is accomplished by showing:

DE.AE-1: Baselines and Diagrams

A baseline of network operations and expected data flows for users and systems is established and managed.

References:

- CIS CSC V8, 3.8
- COBIT 5, DSS03.01
- FERPA (PTAC), Network Mapping
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)
- ISO/IEC 27001:2013, A.12.1.1-2, A.13.1.1-2
- NIST SP 800-53 Rev.4, AC-4, CA-3, CM-2, SI-4
- PCI DSS v3.2.1, 1.1.1, 1.1.2, 1.1.3
- USG IT Handbook V2.9.7, 5.1

DE.AE-2: Analysis

Detected events are analyzed to understand attack targets and methods.

References:

- CIS CSC V8, 8.11
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(6)(i)
- ISO/IEC 27001:2013, A.12.4.1, A.16.1.1, A.16.1.4
- NIST SP 800-53 Rev.4, AU-6, CA-7, IR-4, SI-4
- NIST SP 800-171 Rev. 1, 3.3.1-2, 3.3.5, 3.6.1, 3.14.6-7
- PCI DSS v3.2.1, 10.6 (all), 12.5.2
- USG IT Handbook V2.9.7, 5.5

DE.AE-3: Aggregation and Correlation

Event data are aggregated and correlated from multiple sources and sensors.

References:

- CIS CSC V8, 8.2, 8.5-8, 8.12
- COBIT 5, BAI08.02
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
- NIST SP 800-53 Rev.4, AU-6, CA-7, IR-4-5,8, SI-4
- NIST SP 800-171 Rev. 1, 3.3.5
- PCI DSS v3.2.1, 10.1, 12.10.5, 10.6
- USG IT Handbook V2.9.7, 5.5

DE.AE-4: Impact assessment

Impact of events is determined.

References:

- COBIT 5, APO12.06, DSS03.01
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
- NIST SP 800-53 Rev.4, CP-2, IR-4, RA-3, SI -4
- NIST SP 800-171 Rev. 1, 3.11.1
- PCI DSS v3.2.1, 10.6.3, 12.5.2
- USG IT Handbook V2.9.7, 5.5

DE.AE-5) Incident Alerts

Incident alert thresholds are established.

References:

- CIS CSC V8, 13.11
- COBIT 5, APO12.06, DSS03.01
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)
- ISO/IEC 27001:2013, A.16.1.4
- NIST SP 800-53 Rev.4, IR-4-5, IR-8
- NIST SP 800-171 Rev. 1, 3.6-2
- PCI DSS v3.2.1, 12.5.2
- USG IT Handbook V2.9.7, 5.3

SECURITY CONTINUOUS MONITORING (DE.CM)

USG information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. This is achieved by ensuring:

DE.CM-1: Network Monitoring

The network is monitored to detect potential cybersecurity events.

References:

- COBIT 5, DSS01.03, DSS03.05, DSS05.07
- FERPA (PTAC), Firewalls and IDPS, Secure Configurations
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)
- NIST SP 800-53 Rev.4, AC-2, AU-12, CA-7, CM-3, SC-5,7, SI-4
- NIST SP 800-171 Rev. 1, 3.13.1, 3.14.6-7
- PCI DSS v3.2.1, 10.6.1, 10.6.2, 11.4
- USG IT Handbook V2.9.7, 5.5

DE.CM-2: Facilities Monitoring

The physical environment is monitored to detect potential cybersecurity events.

References:

- COBIT 5, DSS01.04-05
- FERPA (PTAC), Physical Security, Secure Configurations
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)
- ISO/IEC 27001:2013, A11.1.1-2
- NIST SP 800-53 Rev.4, CA-7, PE-3,6,20
- NIST SP 800-171 Rev. 1, 3.10.2-3
- PCI DSS v3.2.1, 9.1.1
- USG IT Handbook V2.9.7, 5.5

DE.CM-3: Logging Monitoring)

Personnel activity is monitored to detect potential cybersecurity events.

References:

- COBIT 5, DSS05.07
- FERPA (PTAC), Access Controls
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
- ISO/IEC 27001:2013, A.12.4.1,3
- NIST SP 800-53 Rev.4, AC-2, AU-12-13, CA-7, CM-10-11
- NIST SP 800-171 Rev. 1, 3.1.12, 3.3.1-2, 3.4.9
- PCI DSS v3.2.1, 9.1.1
- USG IT Handbook V2.9.7, 5.5

DE.CM-4: End-Point Monitoring

Malicious code is detected.

References:

- CIS CSC V8, 10.1-2, 10.4-7
- COBIT 5, DSS05.01
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
- ISO/IEC 27001:2013, A.12.2.1
- NIST SP 800-53 Rev.4, SI-3,8
- NIST SP 800-171 Rev. 1, 3.14.1-5, 3.13.13
- PCI DSS v3.2.1, 5 (all)
- State PSG, SS-08-033, PS-08-021
- USG IT Handbook V2.9.7, 5.5, 5.8, 5.11

DE.CM-5: Mobile Code Monitoring

Unauthorized mobile code is detected.

References:

- COBIT 5, DSS05.01
- FERPA (PTAC), Mobile Devices
- GLBA (NIST SP 800-171 Rev. 1)

- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
- ISO/IEC 27001:2013, A.12.5.1, A.12.6.2
- NIST SP 800-53 Rev.4, SC-18, SI-4, SC-44
- NIST SP 800-171 Rev. 1, 3.13.13
- PCI DSS v3.2.1, 5 (all)
- State PSG, PS-08-021
- USG IT Handbook V2.9.7, 5.5

DE.CM-6: 3rd Part Service Monitoring

External service provider activity is monitored to detect potential cybersecurity events.

References:

- CIS CSC V8, 15.6
- COBIT 5, APO07.06, APO10.05
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(D)
- ISO/IEC 27001:2013, A.14.2.7, A.15.2.1
- NIST SP 800-53 Rev.4, CA-7, PS-7, SA-4,9, SI-4
- NIST SP 800-171 Rev. 1, 3.14.6-7
- PCI DSS v3.2.1, 8.1.5, 10.6

DE.CM-7: Access Monitoring

Monitoring for unauthorized personnel, connections, devices, and software is performed.

References:

- CIS CSC V8, 1.3-5, 2.3-6, 9.6
- COBIT 5, DSS05.02,05
- FERPA (PTAC), Inventory of Assets, Physical Security, Secure Configurations
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
- ISO/IEC 27001:2013, A.12.4.1, A.14.2.7, A.15.2.1
- NIST SP 800-53 Rev.4, AU-12, CA-7, CM-3,8, PE-3,6,20, SI-4
- NIST SP 800-171 Rev. 1, 3.1.12, 3.3.1, 3.10.2-3, 3.14.6-7
- PCI DSS v3.2.1, 10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5
- USG IT Handbook V2.9.7, 5.8

DE.CM-8: Vulnerability Scanning

Vulnerability scans are performed.

References:

- CIS CSC V8, 7.5
- FERPA (PTAC), Automated Vulnerability Scanning, Secure Configurations
- COBIT 5, BAI03.10, DSS05.01
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)

- ISO/IEC 27001:2013, A.12.6.1
- NIST SP 800-53 Rev.4, RA-5
- NIST SP 800-171 Rev. 1, 3.11.2
- PCI DSS v3.2.1, 11.2
- State PSG, PS-08-021
- USG IT Handbook V2.9.7, 5.1

DETECTION PROCESSES (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. USG organizations must demonstrate:

DE.DP-1: Roles and Responsibilities

Roles and responsibilities for detection are well defined to ensure accountability.

References:

- CIS CSC V8, 17.1, 17.4
- COBIT 5, APO01.02, DSS05.01, DSS06.03
- FERPA (PTAC), Audit and Compliance Monitoring
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.2
- NIST SP 800-53 Rev.4, CA-2,7, PM-14
- PCI DSS v3.2.1, 9.9.3, 12.5.2, 12.10
- USG IT Handbook V2.9.7, 5.3

DE.DP-2: Monitoring

Detection activities comply with all applicable requirements.

References:

- COBIT 5, DSS06.01, MEA03.03-04
- FERPA (PTAC), Audit and Compliance Monitoring
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
- ISO/IEC 27001:2013, A.18.1.4, A.18.2.2-3
- NIST SP 800-53 Rev.4, AC-25, CA-2,7, SA-18, SI-4, PM-14
- NIST SP 800-171 Rev. 1, 3.12.1, 3.12.3, 3.14.6-7
- PCI DSS v3.2.1, 10.9, 11.2, 11.3, 11.4, 12.10.1
- USG IT Handbook V2.9.7, 5.3

DE.DP-3: Testing

Detection processes are tested .

References:

- COBIT 5, APO13.02, DSS05.02
- FERPA (PTAC), Audit and Compliance Monitoring, Physical Security
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.306(e)

- ISO/IEC 27001:2013, A.14.2.8
- NIST SP 800-53 Rev.4, CA-2,7, PE-3, PM-14, SI-3-4
- NIST SP 800-171 Rev. 1, 3.10.4, 3.12.1, 3.12.3
- PCI DSS v3.2.1, 10.6.1, 10.9, 11.2, 11.3, 12.10
- USG IT Handbook V2.9.7, 5.3

DE.DP-4: Information Sharing

Event detection information is communicated to appropriate parties.

References:

- CIS CSC V8, 17.5
- COBIT 5, APO08.04, APO12.06, DSS05.02
- FERPA (PTAC), Audit and Compliance Monitoring
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
- ISO/IEC 27001:2013, A.16.1.2-3
- NIST SP 800-53 Rev.4, AU-6, CA-2,7, RA-5, SI-4
- PCI DSS v3.2.1, 12.10
- USG IT Handbook V2.9.7, 5.3, 5.10

DE.DP-5: Continuous Improvement

Detection processes are continuously improved.

References:

- COBIT 5, APO11.06, APO12.06, DSS04.05
- FERPA (PTAC), Audit and Compliance Monitoring
- HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(8)
- ISO/IEC 27001:2013, A.16.1.6
- NIST SP 800-53 Rev.4, CA-2,7, PL-2, RA-5, SI-4, PM-14
- PCI DSS v3.2.1, 12.10.6
- USG IT Handbook V2.9.7, 5.3

RESPOND (RS)

ANALYSIS (RS.AN)

USG organization shall conduct analysis of adequate response and support recovery activities to ensure:

RS.AN-1: Investigation

Notifications from detection systems are investigated.

References:

- CIS CSC V8, 8.11, 16.3, 16.6
- COBIT 5, DSS02.04,07
- FERPA (PTAC), Incident Handling, Secure Configuration
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(b)

- ISO/IEC 27001:2013, A.12.4.1,3, A.16.1.5
- NIST SP 800-53 Rev.4, AU-6, CA-7, IR-4-5, PE-6, SI-4
- NIST SP 800-171 Rev. 1, 3.3.5, 3.6.1-2
- PCI DSS v3.2.1, 10.6.3, 11.5.1, 12.5.2, 12.10.5
- USG IT Handbook V2.9.7, 5.3

RS.AN-2: Impact Understood

The impact of the incident is understood.

References:

- COBIT 5, DSS02.02
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E)
- ISO/IEC 27001:2013, A.16.1.4,6
- NIST SP 800-53 Rev.4, CP-2, IR-4
- NIST SP 800-171 Rev. 1, 3.11.1
- PCI DSS v3.2.1, 10.6.3, 11.5.1, 12.5.2
- USG IT Handbook V2.9.7, 5.3

RS.AN-3: Forensics

Forensics are performed.

References:

- COBIT 5, APO12.06, DSS03.02, DSS05.07
- FERPA (PTAC), Incident Handling
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)
- ISO/IEC 27001:2013, A.16.1.7
- NIST SP 800-53 Rev.4, AU-7, IR-4
- PCI DSS v3.2.1, 11.5.1, 12.5.2

RS.AN-4: Incident Categorized

Incidents are categorized consistent with response plans.

References:

- CIS CSC V8, 17.9
- COBIT 5, DSS02.02
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
- ISO/IEC 27001:2013, A.16.1.4
- NIST SP 800-53 Rev.4, CP-2, IR-4-5,8
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 11.5.1, 12.5.2
- USG IT Handbook V2.9.7, 5.3

RS.AN-5: Vulnerability Disclosure Response

Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal and external testing, security bulletins, or security researchers).

- CIS CSC V8, 16.2
- CMMC v0.6, SII-CO41-P1214
- COBIT 5, EDM03.02, DSS05.07
- NIST SP 800-53 Rev.4, SI-5, PM-15
- PCI DSS v3.2.1, 6.1, 6.2

COMMUNICATIONS (RS.CO)

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. This is achieved by ensuring:

RS.CO-1: Roles and Responsibilities

Personnel know their roles and order of operations when a response is needed.

References:

- CIS CSC V8, 17.2, 17.4
- COBIT 5, APO01.02, APO12.03, EDM03.02
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.308(a)(6)(i), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, A.6.1.1, A.7.2.2, A.16.1.1
- NIST SP 800-53 Rev.4, CP-2-3, IR-3,8
- NIST SP 800-171 Rev. 1, 3.6.3
- PCI DSS v3.2, 12.10
- USG IT Handbook V2.9.7, 5.3

RS.CO-2: Event Notification

Events are reported consistent with established criteria.

References:

- CIS CSC V8, 17.5
- COBIT 5, DSS01.03
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
- ISO/IEC 27001:2013, A.6.1.3, A.16.1.2
- NIST SP 800-53 Rev.4, AU-6, IR-6, IR-8
- NIST SP 800-171 Rev. 1, 3.6.2
- PCI DSS v3.2.1, 10.8, 12.10
- USG IT Handbook V2.9.7, 5.3

RS.CO-3: Information Sharing – Internal

Information is shared consistent with response plans.

References:

- CIS CSC V8, 17.5
- COBIT 5, DSS03.04
- Audit and Compliance Monitoring, Incident Handling, Secure Configurations
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C)
- ISO/IEC 27001:2013, A.16.1.2, Clause 7.4, Clause 16.1.2
- NIST SP 800-53 Rev.4, CA-2,7, CP-2, IR-4,8, PE-6, RA-5, SI-4
- PCI DSS v3.2.1, 12.10
- USG IT Handbook V2.9.7, 5.3

RS.CO-4: Coordination

Coordination with stakeholders occurs consistent with response plans.

References:

- CIS CSC V8, 17.5
- COBIT 5, DSS03.04
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, Clause 7.4
- NIST SP 800-53 Rev. 4, CP-2, IR-4,8
- NIST SP 800-171 Rev. 1, 3.6.1
- PCI DSS v3.2.1, 12.10.1

RS.CO-5: Information Sharing – External

Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

References:

- COBIT 5, BAI08.04
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)
- NIST SP 800-53 Rev.4, PM-15, SI-5
- PCI DSS 3.0, 12.10

IMPROVEMENTS (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. USG organizations must show:

RS.IM-1: Lessons Learned

Response plans incorporate lessons learned.

References:

- CIS CSC V8, 17.8
- COBIT 5, BAI01.13
- FERPA (PTAC), Incident Handling

- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii))
- ISO/IEC 27001:2013, A.16.1.6, Clause 10
- NIST SP 800-53 Rev.4, CP-2, IR-4, IR-8
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 12.10.6
- USG IT Handbook V2.9.7, 5.3

RS.IM-2: Procedures Updated

Response strategies are updated.

References:

- CIS CSC V8, 17.8
- COBIT 5, BAI01.13, DSS04.08
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
- ISO/IEC 27001:2013, A.16.1.6, Clause 10
- NIST SP 800-53 Rev.4, CP-2, IR-4, IR-8
- NIST SP 800-171 Rev. 1, 3.6.2
- PCI DSS v3.2.1, 12.10.6
- USG IT Handbook V2.9.7, 5.3

MITIGATION (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. USG organizations must verify:

RS.MI-1: Incident Containment

Incidents are contained.

References:

- COBIT 5, APO12.06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
- ISO/IEC 27001:2013, A.12.2.1, A.16.1.5
- NIST SP 800-53 Rev.4, IR-4
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 11.5.1, 12.5.2
- USG IT Handbook V2.9.7, 5.3

RS.MI-2: Incident Mitigation

Incidents are mitigated.

References:

- COBIT 5, APO12.06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
- ISO/IEC 27001:2013, A.12.2.1, A.16.1.5

- NIST SP 800-53 Rev.4, IR-4
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 11.5.1, 12.5.2
- USG IT Handbook V2.9.7, 5.3

RS.MI-3: Vulnerability Mitigation

Newly identified vulnerabilities are mitigated or documented as accepted risks.

References:

- COBIT 5, APO12.06
- FERPA (PTAC), Automated Vulnerability Monitoring, Secure Configuration
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii)
- ISO/IEC 27001:2013, A.12.6.1
- NIST SP 800-53 Rev.4, CA-7, RA-3, RA-5
- NIST SP 800-171 Rev. 1, 3.11.1-3, 3.12.2, 3.12.4, 3.14.1
- PCI DSS v3.2.1, 6.1, 6.2, 10.6.3, 11.2, 11.5.1, 12.5.2, 12.10
- USG IT Handbook V2.9.7, 5.5

RESPONSE PLANNING (RS.RP)

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. To achieve this, USG organizations must verify:

RS.RP-1: Incident Response Plans and Procedures

Response plans are executed during or after an event.

References:

- COBIT 5, APO12.06, BAI01.10
- FERPA (PTAC), Incident Handling
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)
- ISO/IEC 27001:2013, A.16.1.5
- NIST SP 800-53 Rev.4, CP-2,10, IR-4,8
- NIST SP 800-171 Rev. 1, 3.6.2
- PCI DSS v3.2.1, 12.10
- State PSG, PS-08-004
- USG IT Handbook V2.9.7, 5.3

RECOVER (RC)

RECOVERY PLANNING (RC.RP)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. This is demonstrated by showing:

RC.RP-1: Recovery Plans Executed and Tested

Recovery plans are executed during or after an event.

References:

- COBIT 5, APO12.06, DSS02.05, DSS03.04
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i)
- ISO/IEC 27001:2013, A.16.1.5
- NIST SP 800-53 Rev.4, CP-10, IR-4, IR-8
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 12.10.6
- State PSG, PS-08-025, SS-08-004, SS-08-046
- USG IT Handbook V2.9.7, 3.3.1

IMPROVEMENTS (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1: Lessons Learned

Recovery plans incorporate lessons learned.

References:

- COBIT 5, APO12.06, BAI05.07, DSS04.08
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
- ISO/IEC 27001:2013, A.16.1.6, Clause 10
- NIST SP 800-53 Rev.4, CP-2, IR-4, IR-8
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 12.10.6
- USG IT Handbook V2.9.7, 3.3.1

RC.IM-2: Procedures Updated

Recovery strategies are updated.

References:

- COBIT 5, APO12.06, BAI07.08
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
- ISO/IEC 27001:2013, A.16.1.6, Clause 10
- NIST SP 800-53 Rev.4, CP-2, IR-4, IR-8
- NIST SP 800-171 Rev. 1, 3.6.1-2
- PCI DSS v3.2.1, 12.10.6
- USG IT Handbook V2.9.7, 3.3.1

COMMUNICATIONS (RC.CO)

Restoration activities are coordinated with internal and external parties, such USO/ITS/USG Cybersecurity, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendor-partners. This is achieved by ensuring:

RC.CO-1: Enterprise Communications

Public relations are managed.

References:

- COBIT 5, EDM03.02
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)
- ISO/IEC 27001:2013, A.16.1.4, Clause 7.4
- USG IT Handbook V2.9.7, 3.3.1

RC.CO-2: Reputation Management

Reputation after an event is repaired.

References:

- COBIT 5, MEA03.02
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)
- ISO/IEC 27001:2013, Clause 7.4
- USG IT Handbook V2.9.7, 3.3.1

RC.CO-3: Recovery Communications

Recovery activities are communicated to internal stakeholders and executive and management teams.

References:

- COBIT 5, APO12.06
- GLBA (NIST SP 800-171 Rev. 1)
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.314(a)(2)(i)(C)
- ISO/IEC 27001:2013, Clause 7.4
- NIST SP 800-53 Rev.4, CP-2, IR-4
- NIST SP 800-171 Rev. 1, 3.6.1-2
- USG IT Handbook V2.9.7, 3.3.1

SECTION 12: DATA GOVERNANCE AND MANAGEMENT

Governance structures and procedures; management documentation, elements, definitions, availability and lifecycle; cybersecurity safeguards, classification, access and segregation; compliance regulations, training, monitoring and audit; and privacy management, inventory, documentation, awareness and communication.

12.2.1 GOVERNANCE AND ORGANIZATIONAL STRUCTURE - DATA OWNER

Cybersecurity roles and responsibilities (data owner, data trustee, data stewards) are coordinated and aligned with internal roles and external partners.

- CSF v1.1, ID.GV-2
- PF v1.0, GV.PO-P4

12.4.2 Data Classification

Resources are prioritized based on their classification, criticality, and business value.

- CSF v1.1, ID.AM-5

12.4.3 Access Procedures

Access permissions/authorizations are documented and managed, using principles of least privilege and separation of duties.

- CSF v1.1, PR.AC-4
- PF v1.0, PR.AC-P4

12.5.1 Regulatory Compliance

Legal, regulatory, privacy, and civil liberties requirements regarding cybersecurity are understood and managed.

- CSF v1.1, ID.GV-3
- PF v1.0, GV.PO-P5

APPENDIX A: REFERENCES

CIS	Critical Security Controls for Effective Cyber Defense v8 https://www.cisecurity.org
CMMC	DoD Cybersecurity Maturity Model Certification v0.6 https://wwwcomplianceforge.com
CSF	Cybersecurity Framework https://www.nist.gov/cyberframework
FERPA	FERPA (PTAC): Data Security Checklist https://studentprivacy.ed.gov/resources/data-security-checklist
GLBA	GLBA "Safeguards Rule" https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule
HIPAA	DHHS Office for Civil Rights | HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework, 45 CFR 160, 162, and 164. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf
ISO/IEC 27001	Information Technology-Security Techniques… Requirements https://www.iso.org/standards/54534.html
Privacy Framework	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management https://nist.gov/privacy-framework
NIST SP 800-53	NIST SP 800-53 Rev4, Security and Privacy Controls https://csrc.nist.gov/publications/sp800
NIST SP 800-171	NIST SP 800-171 Rev. 1 Informative Reference Details https://www.nist.gov/nist-sp-800-171-rev-1-informative-reference-details -OR- https://www.nist.gov/document/csf-sp800-171mappingxlsx
PCI DSS 3.2.1	Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1 https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf

APPENDIX B: ACRONYMS (COMMON ABBREVIATIONS)

CIS	Center for Internet Security
CMMC	Cybersecurity Maturity Model Certification
CSF	Cybersecurity Framework
FERPA	Family Educational Rights and Privacy Act
FSA	Federal Student Aid
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IHE	Institutes of Higher Education
ISO/	International Organization for Standardization
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PTAC	Privacy Technical Assistance Center
SP	Special Publication