NIST SP-800-53 r5 – The Control Reference Layer: Taming the Beast beneath CCM 4.2 to NIST 800-53 Mapping Discussing the Cloud Security Alliance Working Group

Robin Basham, CEO, EnterpriseGRC Solutions

President, ISC2 East Bay Chapter

Presentation to ISACA San Francisco, Wednesday, Aug 25 at 12:00-1:00 PM PDT

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Resources Frequently Mentioned During this presentation

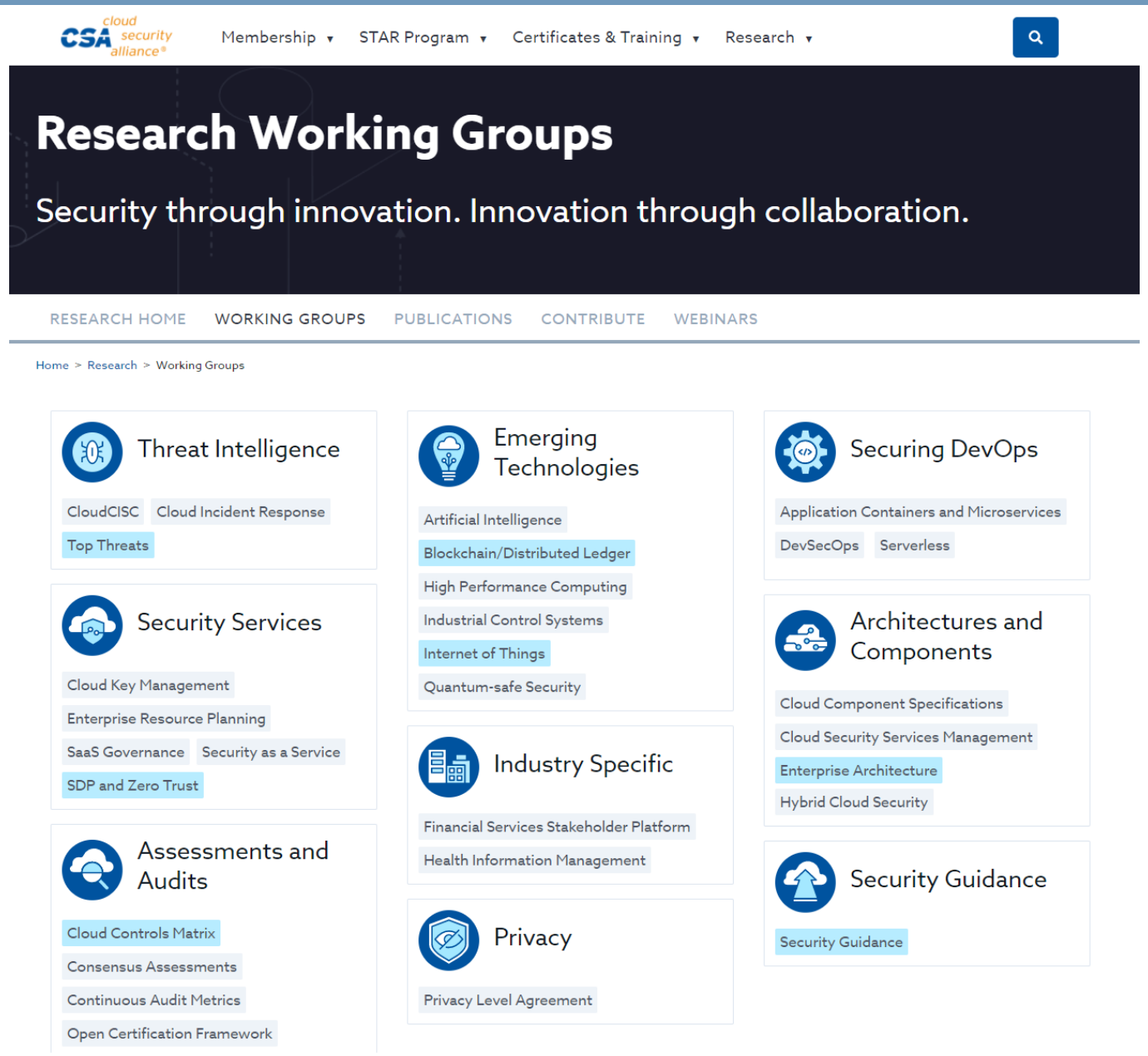
EnterpriseGRC Solutions, Inc.

	Critical Resource Website link	
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY	Homepage | CISA	CIS Center for Internet Security (cisecurity.org)
CSA cloud security alliance®	https://cloudsecurityalliance.org/	How to Become FedRAMP Authorized | FedRAMP.gov
NIST	National Institute of Standards and Technology | NIST	Acquisition.GOV | www.acquisition.gov Location for DFARS

CIS Center for Internet Security®
Confidence in the Connected World®

FedRAMP

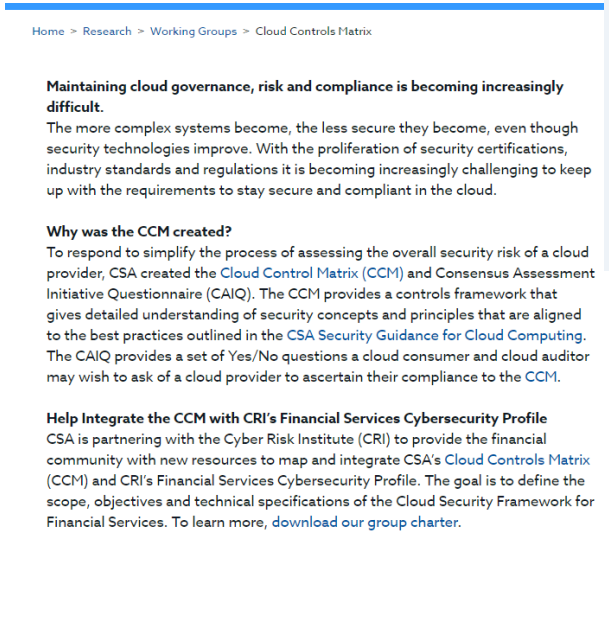
©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com



EnterpriseGRC Solutions, Inc.

People who want to join a Cloud Security Alliance Research Working Group should reach out to [Cloud Controls Matrix Working Group | CSA (cloudsecurityalliance.org)]

I'm very honored to be a lead among the Mapping of NIST 800-53r5 and CCM 4.0 WG



Along with releasing updated versions of the CCM and CAIQ, this working group provides addendums, control mappings and gap analysis between the CCM and other research releases, industry standards, and regulations to keep it continually up to date.

Join Group

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

"We'd like to use Cloud Control Matrix & NIST SP 800-53 r5 Mapping as our Master Control List"

EnterpriseGRC Solutions, Inc.

1. *RESOURCES / REASONS:* Companies using NIST *SP 800-53 r4, must update to Rev 5.1. Cloud Controls Matrix has recently updated to CCM 4.0* – ***We need them both, now.***

2. Problem: NIST SP 800-53 as a **mediating** framework is incompletely or inaccurately mapped in products; It requires updates for CIS CSC 7.1->8.1, CCM 3.1->4.2, NIST SP 800-171 r2 & NIST SP 800-172 (Cybersecurity Enhancement), plus New Tailoring Criteria

3. Opportunity: Leveraging NIST SP 800-53 r5 to complete ©AICPA SOC 2, ©HITRUST, PCI DSS 3.21, CSTAR CCM, DFARS CMMC, ©ISO/IEC 27001 plus Privacy, Processing and Cloud requires detail understanding of these frameworks – i.e., experience completing engagements to do this work, but it can be done.

4. Methodology: Creating *useable* cyber framework mapping is an exercise that drives common language across all Policies and Programs and is necessary to meaningful resilience and compliance.

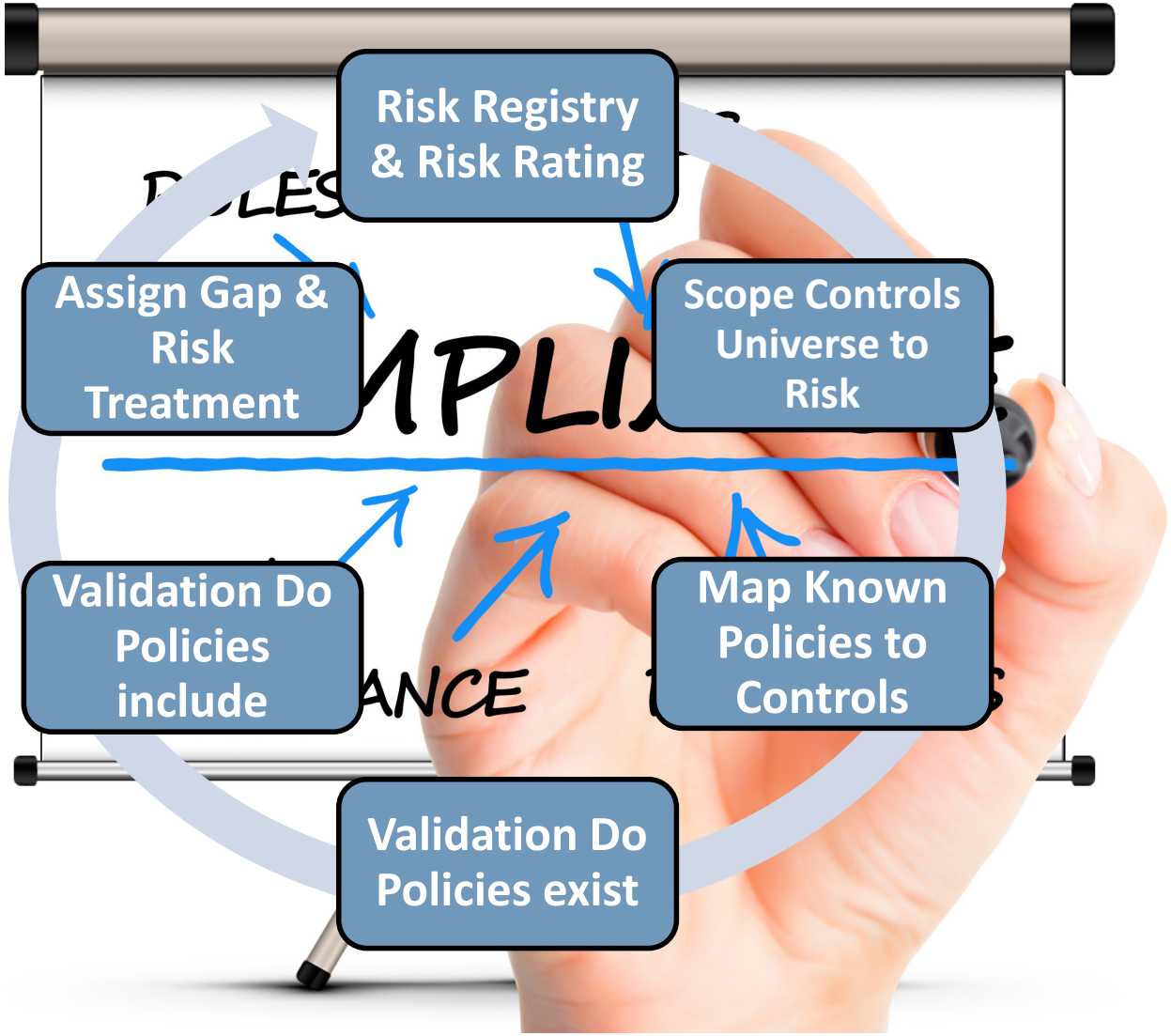
©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

The Rush: Iterative steps maintain Common Controls

EnterpriseGRC Solutions, Inc.

Change is the Constant – ground rules for what we do

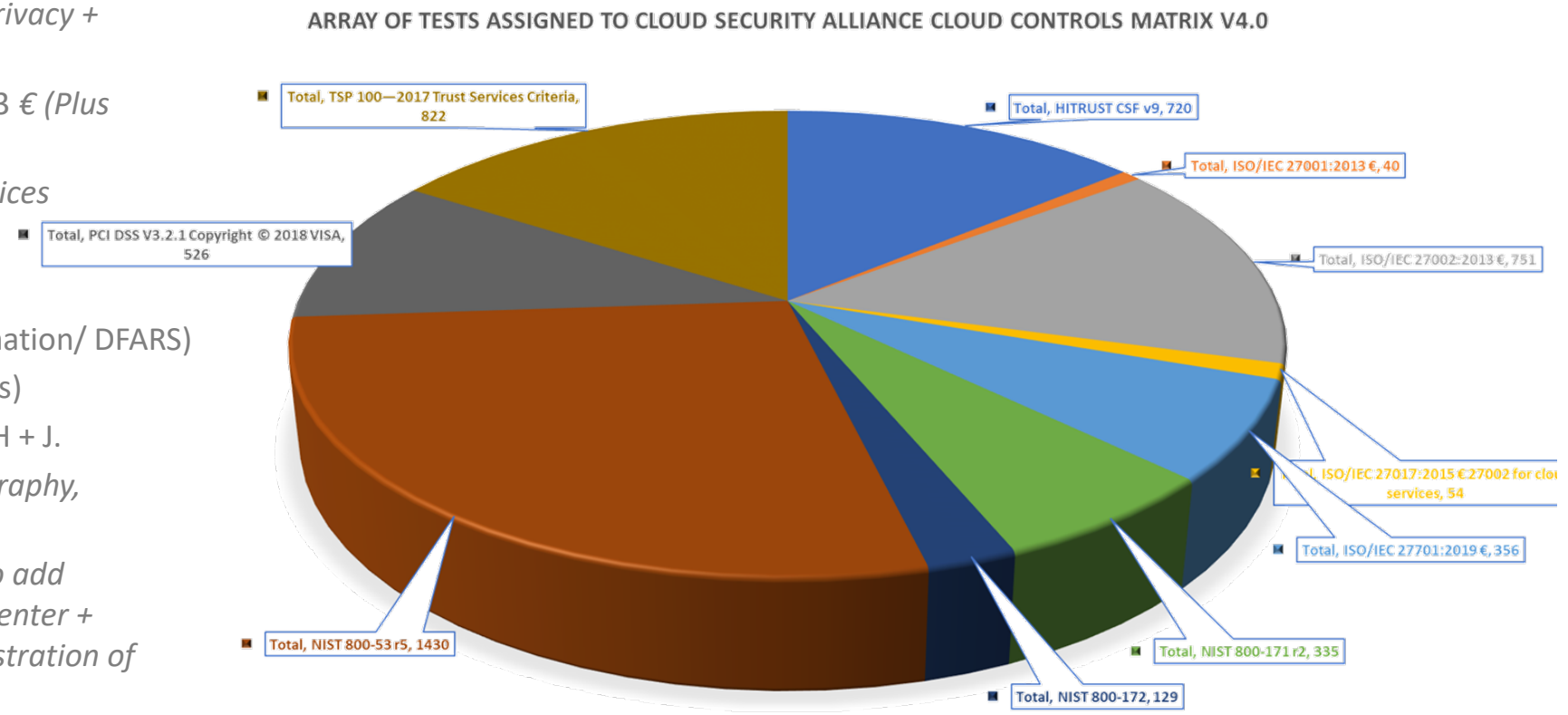
- Controls and Policies map to Risks
- Risk Assessment affects Scope
- Any control or policy modifications introduced by mappings frameworks changes policy requirements
- Adding mapped controls requires validation of policy content and enforcement
- New policy introduces new risk cycle -> takes 1-2 years to fully implement



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Why Now: Cryptographic, Data Center, and Data Security Privacy

- California Consumer Privacy Act of 2018, California Privacy Rights and Enforcement Act of 2020 (CPRA) – *Privacy + Cryptography*
- For the ISO/IEC 27001 using ISO/IEC 27002:2013 *€ (Plus Privacy, Processing, Cloud)*
  - *ISO/IEC 27017:2015 € 27002 for cloud services*
  - *ISO/IEC 27701:2019 € Privacy*
  - *ISO/IEC 27018:2019 € Processing*
- NIST 800-171 r2 (Controlled Unclassified Information/ DFARS)
- NIST 800-172 (Plus Cybersecurity Enhancements)
- NIST 800-53 r5 (NIST-800-53B) replaces Annex H + J.
- PCI DSS V3.2.1 Copyright © 2018 VISA (*Cryptography, Privacy*)
- TSP 100—2017 Trust Services Criteria – *Likely to add Cybersecurity, Healthcare, Supply Chain - Datacenter + Privacy + Cryptography greatly improve demonstration of these controls.*
- HITRUST CSF v9* – *Privacy + Cryptography + Data Center (to operate with HITRUST contact Hitrust.org)*



ISO/IEC 27701:2019 € Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO/IEC 27018:2019 € Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27017:2015 € 27002 for cloud services

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Cloud Control Matrix 17 Domains, 197 Controls, 262 Tests + Implementation Guidance

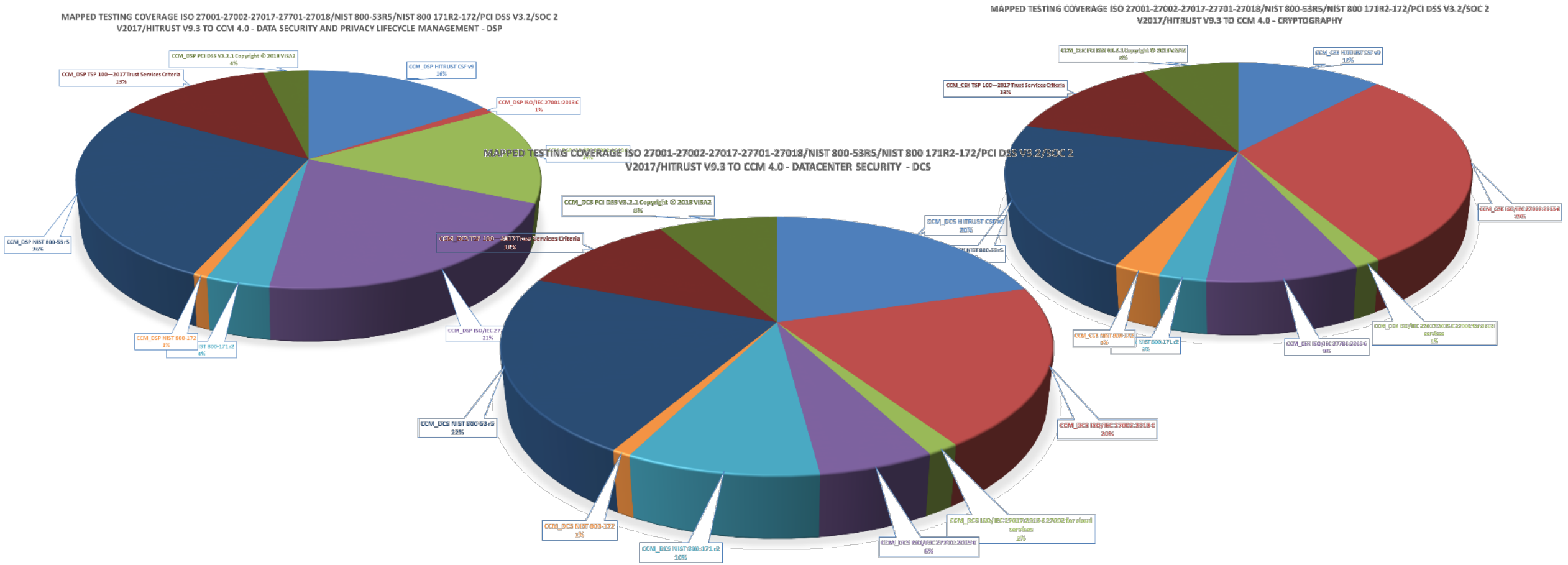
EnterpriseGRC Solutions, Inc.

Audit and Assurance - A&A	Audit and Assurance Policy and Procedures; Independent Assessments; Risk Based Planning Assessment; Requirements Compliance; Audit Management Process; Remediation
Application and Interface Security - AIS	Application and Interface Security Policy and Procedures; Application Security Baseline Requirements; Application Security Metrics; Secure Application Design and Development; Automated Application Security Testing; Automated Secure Application Deployment; Application Vulnerability Remediation
Business Continuity Management and Operational Resilience - BCR	Business Continuity Management Policy and Procedures; Risk Assessment and Impact Analysis; Business Continuity Strategy; Business Continuity Planning; Documentation; Business Continuity Exercises; Communication; Backup; Disaster Response Plan; Response Plan Exercise; Equipment Redundancy
Change Control and Configuration Management - CCC	Change Management Policy and Procedures; Quality Testing; Change Management Technology; Unauthorized Change Protection; Change Agreements; Change Management Baseline; Detection of Baseline Deviation; Exception Management; Change Restoration
Cryptography, Encryption and Key Management - CEK	Encryption and Key Management Policy and Procedures; CEK Roles and Responsibilities; Data Encryption; Encryption Algorithm; Encryption Change Management; Encryption Change Cost Benefit Analysis; Encryption Risk Management; CSC Key Management Capability; Encryption and Key Management Audit; Key Generation; Key Purpose; Key Rotation; Key Revocation; Key Destruction; Key Activation; Key Suspension; Key Deactivation; Key Archival; Key Compromise; Key Recovery; Key Inventory Management
Datacenter Security - DCS	Off-Site Equipment Disposal Policy and Procedures; Off-Site Transfer Authorization Policy and Procedures; Secure Area Policy and Procedures; Secure Media Transportation Policy and Procedures; Assets Classification; Assets Cataloguing and Tracking; Controlled Access Points; Equipment Identification; Secure Area Authorization; Surveillance System; Unauthorized Access Response Training; Cabling Security; Environmental Systems; Secure Utilities; Equipment Location
Data Security and Privacy Lifecycle Management - DSP	Security and Privacy Policy and Procedures; Secure Disposal; Data Inventory; Data Classification; Data Flow Documentation; Data Ownership and Stewardship; Data Protection by Design and Default; Data Privacy by Design and Default; Data Protection Impact Assessment; Sensitive Data Transfer; Personal Data Access, Reversal, Rectification and Deletion; Limitation of Purpose in Personal Data Processing; Personal Data Sub-processing; Disclosure of Data Sub-processors; Limitation of Production Data Use; Data Retention and Deletion; Sensitive Data Protection; Disclosure Notification; Data Location
Governance, Risk and Compliance - GRC	Governance Program Policy and Procedures; Risk Management Program; Organizational Policy Reviews; Policy Exception Process; Information Security Program; Governance Responsibility Model; Information System Regulatory Mapping; Special Interest Groups
Human Resources - HRS	Background Screening Policy and Procedures; Acceptable Use of Technology Policy and Procedures; Clean Desk Policy and Procedures; Remote and Home Working Policy and Procedures; Asset returns; Employment Termination; Employment Agreement Process; Employment Agreement Content; Personnel Roles and Responsibilities; Non-Disclosure Agreements; Security Awareness Training; Personal and Sensitive Data Awareness and Training; Compliance User Responsibility
Identity and Access Management - IAM	Identity and Access Management Policy and Procedures; Strong Password Policy and Procedures; Identity Inventory; Separation of Duties; Least Privilege; User Access Provisioning; User Access Changes and Revocation; User Access Review; Segregation of Privileged Access Roles; Management of Privileged Access Roles; CSCs Approval for Agreed Privileged Access Roles; Safeguard Logs Integrity; Uniquely Identifiable Users; Strong Authentication; Passwords Management; Authorization Mechanisms
Interoperability and Portability - IPY	Interoperability and Portability Policy and Procedures; Application Interface Availability; Secure Interoperability and Portability Management; Data Portability Contractual Obligations
Infrastructure and Virtualization Security - IVS	Infrastructure and Virtualization Security Policy and Procedures; Capacity and Resource Planning; Network Security; OS Hardening and Base Controls; Production and Non-Production Environments; Segmentation and Segregation; Migration to Cloud Environments; Network Architecture Documentation; Network Defense
Logging and Monitoring - LOG	Logging and Monitoring Policy and Procedures; Audit Logs Protection; Security Monitoring and Alerting; Audit Logs Access and Accountability; Audit Logs Monitoring and Response; Clock Synchronization; Logging Scope; Log Records; Log Protection; Encryption Monitoring and Reporting; Transaction/Activity Logging; Access Control Logs; Failures and Anomalies Reporting
Security Incident Management, E-Discovery, and Cloud Forensics - SEF	Security Incident Management Policy and Procedures; Service Management Policy and Procedures; Incident Response Plans; Incident Response Testing; Incident Response Metrics; Event Triage Processes; Security Breach Notification; Points of Contact Maintenance
Supply Chain Management, Transparency, and Accountability - STA	SSRM Policy and Procedures; SSRM Supply Chain; SSRM Guidance; SSRM Control Ownership; SSRM Documentation Review; SSRM Control Implementation; Supply Chain Inventory; Supply Chain Risk Management; Primary Service and Contractual Agreement; Supply Chain Agreement Review; Internal Compliance Testing; Supply Chain Service Agreement Compliance; Supply Chain Governance Review; Supply Chain Data Security Assessment
Threat and Vulnerability Management - TVM	Threat and Vulnerability Management Policy and Procedures; Malware Protection Policy and Procedures; Vulnerability Remediation Schedule; Detection Updates; External Library Vulnerabilities; Penetration Testing; Vulnerability Identification; Vulnerability Prioritization; Vulnerability Management Reporting; Vulnerability Management Metrics
Universal Endpoint Management - UEM	Endpoint Devices Policy and Procedures; Application and Service Approval; Compatibility; Endpoint Inventory; Endpoint Management; Automatic Lock Screen; Operating Systems; Storage Encryption; Anti-Malware Detection and Prevention; Software Firewall; Data Loss Prevention; Remote Locate; Remote Wipe; Third-Party Endpoint Security Posture

© Copyright 2021 Cloud Security Alliance - All rights reserved. Cloud Security Alliance "Cloud Controls Matrix (CCM) Version 4.0" at http://www.cloudsecurityalliance.org subject to the following: (a) the Cloud Controls Matrix v4.0 may be used solely for your personal, informational, non-commercial use; (b) the Cloud Controls Matrix v4.0 may not be modified or altered in any way; (c) the Cloud Controls Matrix v4.0 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed.

CCM 4.0 Framework Coverage (especially Data Center, Data Security & Privacy, and Cryptography) is necessary for current Privacy, Processing and Cloud Cybersecurity Framework Controls

EnterpriseGRC Solutions, Inc.



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

LEGAL Requirement - FISMA PL 113-283
NIST SP 800-53 r5, NIST SP 800-171 r2 and NIST SP 800-172

EnterpriseGRC Solutions, Inc.

Federal Information Security Modernization Act FISMA

Federal Information Security Modernization Act of 2014 (Public Law 113-283; December 18, 2014).

The original FISMA was *Federal Information Security Management Act of 2002* (Public Law 107-347 (Title III); December 17, 2002), in the E-Government Act of 2002.

RELATED NEWS

Assessing Enhanced Security Requirements for CUI
April 27, 2021
NIST has released Draft Special Publication (SP) 800-172A, "Assessing Enhanced Security Requirements...

NISTIR 8212: ISCM Program Assessment and Tool
March 31, 2021
NIST has published NISTIR 8212, "An Information Security Continuous Monitoring Program Assessment,"...

NIST Publishes SP 800-172
February 2, 2021
NIST announces the release of Special Publication (SP) 800-172, "Enhanced Security Requirements for...

Draft NIST SP 800-47 Rev. 1 Available for Comment
January 26, 2021
Draft NIST SP 800-47 Revision 1, "Managing the Security of Information Exchanges," is now available...

Control Catalog and Baselines as Spreadsheets
January 26, 2021
New supplemental materials are available for SP 800-53 Rev. 5 and SP 800-53B: spreadsheets for the...

FOR
Information Security Management Act

CS
- rity and Privacy
- ryptography
- yber supply chain risk management
- eneral security & privacy
- + identity & access management
- + privacy
- + risk management
- + security & behavior
- + security measurement
- + security programs & operations
- + systems security engineering
- zero trust
- + **Technologies**
- + **Applications**
- − **Laws and Regulations**
  - + executive documents
  - − laws
    - Cyber Security R&D Act
    - Cybersecurity Enhancement Act
    - E-Government Act
    - Energy Independence and Security Act
    - Federal Information Security Modernization Act
    - First Responder Network Authority
    - Health Insurance Portability and Accountability Act
    - Help America Vote Act
  - + regulations
- + **Activities and Products**
- + **Sectors**

RELATED TOPICS
Laws and Regulations: E-Government Act

Assessing Enhanced Security Requirements for Controlled Unclassified Information: Draft NIST SP 800-172A Available for Comment

April 27, 2021

The protection of controlled unclassified information (CUI) in nonfederal systems and organizations—especially CUI associated with a critical program or high value asset—is important to federal agencies and can directly impact the ability of the Federal Government to successfully carry out its assigned missions and business operations. To determine if the enhanced security requirements in NIST Special Publication (SP) 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, have been satisfied, organizations develop assessment plans and conduct assessments.

Draft NIST SP 800-172A, ***Assessing Enhanced Security Requirements for Controlled Unclassified Information***, provides federal agencies and nonfederal organizations with assessment procedures that can be used to carry out assessments of the requirements in NIST SP 800-172. The generalized assessment procedures are flexible, provide a framework and starting point to assess the enhanced security requirements, and can be tailored to the needs of organizations and assessors. Organizations tailor the assessment procedures by selecting specific assessment methods and objects to achieve the assessment objectives and by determining the scope of the assessment and the degree of rigor applied during the assessment process. The assessment procedures can be employed in self-assessments, independent third-party assessments, or assessments conducted by sponsoring organizations (e.g., government agencies). Such approaches may be specified in contracts or in agreements by participating parties. The findings and evidence produced during assessments can be used by organizations to facilitate risk-based decisions related to the CUI enhanced security requirements. In addition to developing determination statements for each enhanced security requirement, Draft NIST SP 800-172A introduces an updated structure to incorporate organization-defined parameters into the determination statements.

NIST is seeking feedback on the assessment procedures, including the assessment objectives, determination statements, and the usefulness of the assessment objects and methods provided for each procedure. We are also interested in the approach taken to incorporate organization-defined parameters into the determination statements for the assessment objectives.

A public comment period for this document is open through June 11, 2021. See the publication details for a copy of the draft publication and instructions for submitting comments, preferably using the comment template provided. For any questions, please contact sec-cert@nist.gov.

NOTE: A call for patent claims is included on page iv of this draft. For additional information, see the Information Technology Laboratory (ITL) Patent Policy--Inclusion of Patents in ITL Publications.

RELATED TOPICS
Security and Privacy: controls assessment, security controls
Laws and Regulations: Federal Information Security Modernization Act, OMB Circular A-130

https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/FISMA
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

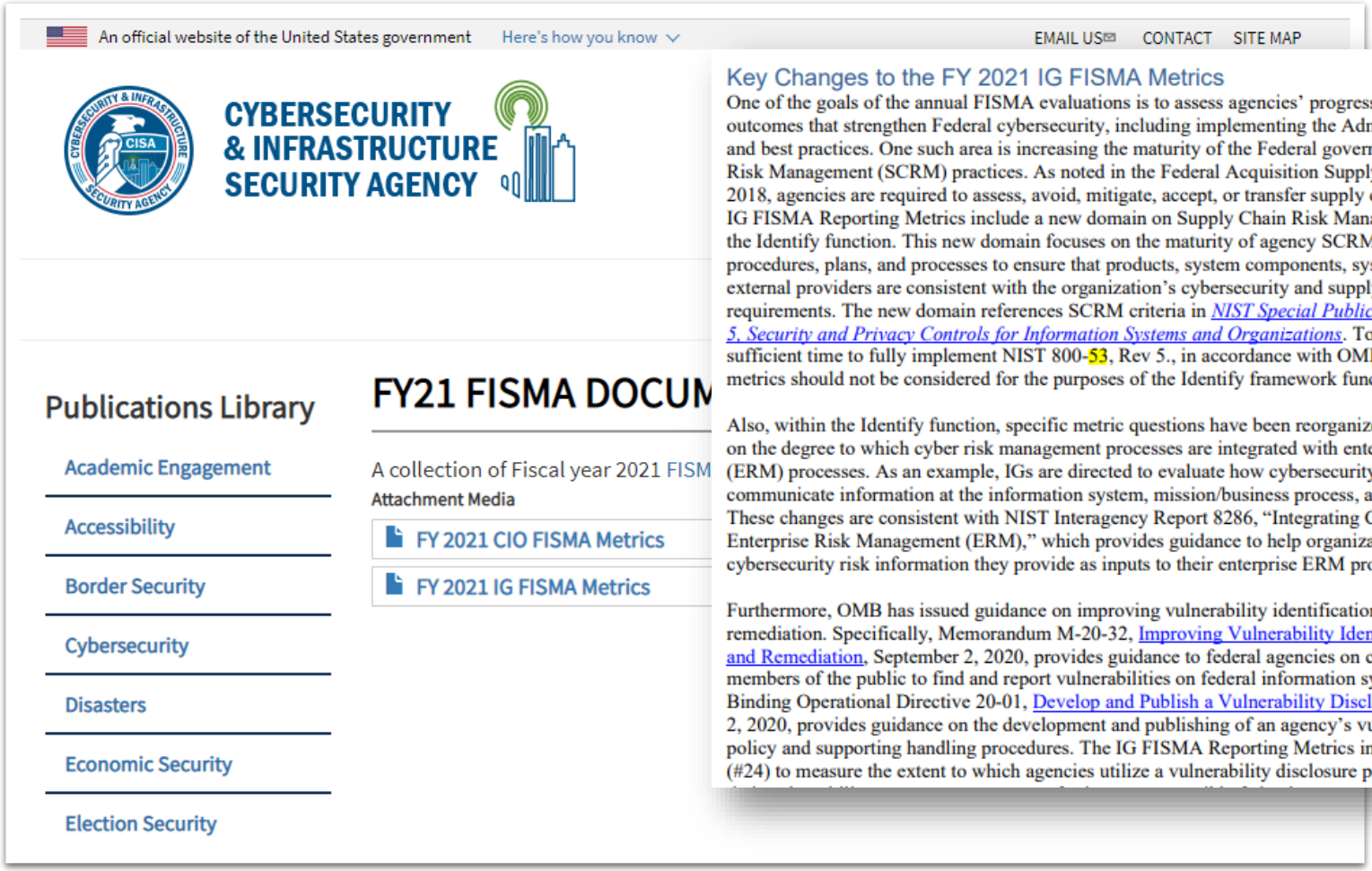
FY 2021 IG METRICS DEPEND ON NIST SP 800-53 r5 - https://www.cisa.gov/

EnterpriseGRC Solutions, Inc.

FY21 FISMA Documents | CISA

FY 2021 Inspector General FISMA Reporting Measures v1.1 (cisa.gov)

FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1 **May 12, 2021**



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

SP 800-53 R5 New Families, Attributes, and Outcomes

- Two new control families: (PT) Personally Identifiable Information Processing and Transparency, (SR) Supply Chain Risk Management
- Consolidates Program Management to main catalog (PM)
- Attributes: Control or control enhancement is implemented by “S” System, or “O” organization, or both “O/S”
- Integrated Privacy controls across the entire catalog notated by “P”
- ALL controls shift from descriptive to outcome - based criteria:
  - Example “The information system *enforces approved*” v. “***Enforce approved authorization***”

EnterpriseGRC Solutions, Inc.

Transition to NIST SP 800-53 r5.1, you must.

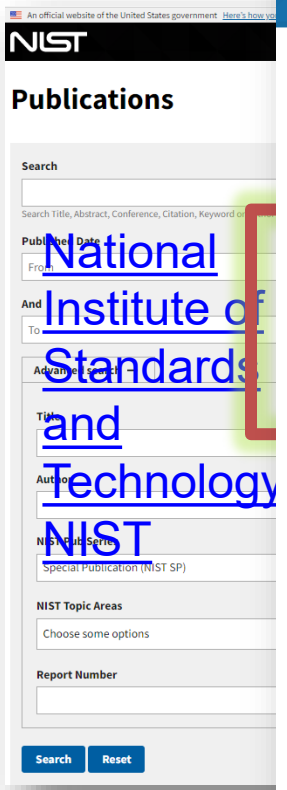
-Yoda

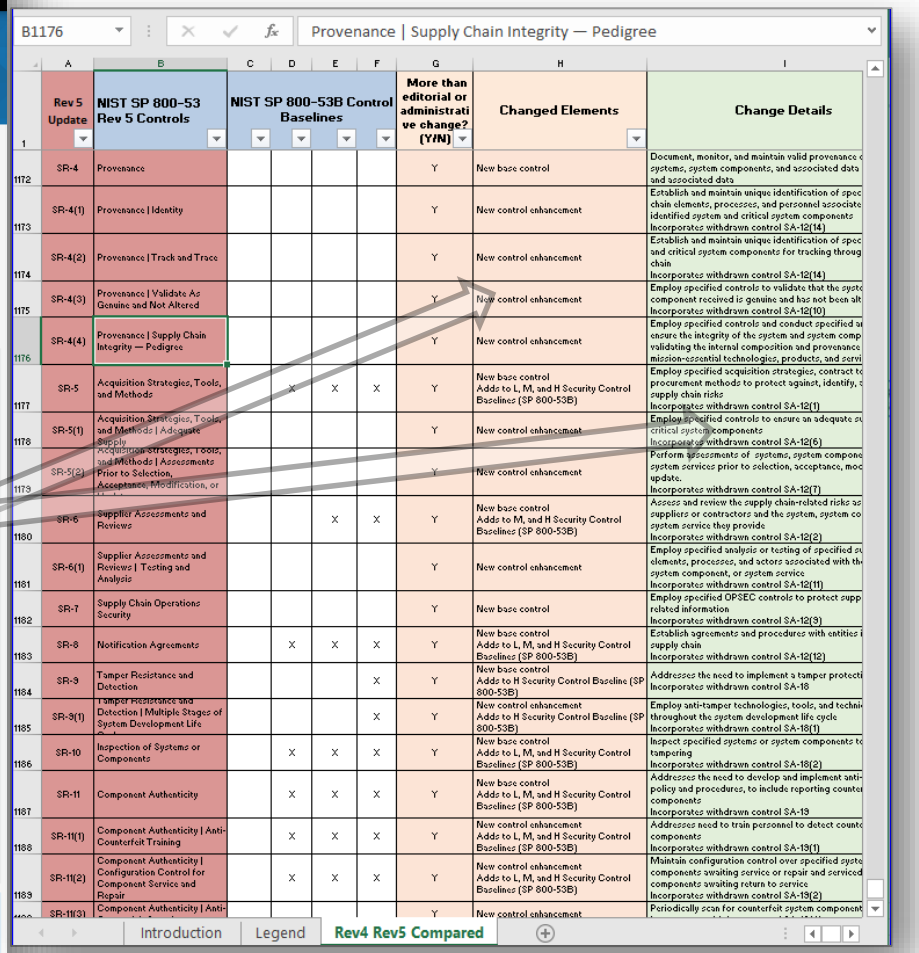
©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

NIST.GOV NIST SP 800-53 Rev. 5 final updates DECEMBER 2020

EnterpriseGRC Solutions, Inc.

National Institute of Standards and Technology NIST





©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

20 Families (Two New Domains)

EnterpriseGRC Solutions, Inc.

AC - ACCESS CONTROL	AT - AWARENESS AND TRAINING	AU - AUDIT AND ACCOUNTABILITY	CA - ASSESSMENT, AUTHORIZATION, AND MONITORING
CM - CONFIGURATION MANAGEME	CP - CONTINGENCY PLANNING	IA - IDENTIFICATION AND AUTHENTICATION	IR - INCIDENT RESPONSE
MA - MAINTENANCE	MP - MEDIA PROTECTION	PE - PHYSICAL AND ENVIRONMENTAL PROTECTION	PL - PLANNING
PM - PROGRAM MANAGEMENT	PS - PERSONNEL SECURITY	PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	RA - RISK ASSESSMENT
SA - SYSTEM AND SERVICES ACQUISITION	SC - SYSTEM AND COMMUNICATIONS PROTECTION	SI - System and Information Integrity	SR - SUPPLY CHAIN RISK MANAGEMENT

- The total number of tracked items since the start of NIST SP 800-53 is 1,189 items. That includes everything withdrawn and everything active. *Green boxes are the Control Families used for SP 800-171r2 and NIST SP 800-172.

	Rev 5 Update	NIST SP 800-53 Rev 5 Controls	NIST SP 800-53B Control Baselines			More than editorial or administrative change? (Y/N)	Changed Elements	Change Details
1179	SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update				Y	New control enhancement	Perform assessments of systems, system components, or system services prior to selection, acceptance, modification, or update. Incorporates withdrawn control SA-12(7)
1180	SR-6	Supplier Assessments and Reviews			X	X	Y	New base control Adds to M, and H Security Control Baselines (SP 800-53B)	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide Incorporates withdrawn control SA-12(2)
1181	SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis					Y	New control enhancement	Employ specified analysis or testing of specified supply chain elements, processes, and actors associated with the system, system component, or system service Incorporates withdrawn control SA-12(11)
1182	SR-7	Supply Chain Operations Security					Y	New base control	Employ specified OPSEC controls to protect supply chain-related information Incorporates withdrawn control SA-12(9)
1183	SR-8	Notification Agreements		X	X	X	Y	New base control Adds to L, M, and H Security Control Baselines (SP 800-53B)	Establish agreements and procedures with entities involved in the supply chain Incorporates withdrawn control SA-12(12)
1184	SR-9	Tamper Resistance and Detection				X	Y	New base control Adds to H Security Control Baseline (SP 800-53B)	Addresses the need to implement a tamper protection program. Incorporates withdrawn control SA-18
1185	SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle				X	Y	New control enhancement Adds to H Security Control Baseline (SP 800-53B)	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle Incorporates withdrawn control SA-18(1)
1186	SR-10	Inspection of Systems or Components		X	X	X	Y	New base control Adds to L, M, and H Security Control Baselines (SP 800-53B)	Inspect specified systems or system components to detect tampering Incorporates withdrawn control SA-18(2)
1187	SR-11	Component Authenticity		X	X	X	Y	New base control Adds to L, M, and H Security Control Baselines (SP 800-53B)	Addresses the need to develop and implement anti-counterfeit policy and procedures, to include reporting counterfeit system components Incorporates withdrawn control SA-19
1188	SR-11(1)	Component Authenticity | Anti-Counterfeit Training		X	X	X	Y	New control enhancement Adds to L, M, and H Security Control Baselines (SP 800-53B)	Addresses need to train personnel to detect counterfeit system components Incorporates withdrawn control SA-19(1)
1189	SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair		X	X	X	Y	New control enhancement Adds to L, M, and H Security Control Baselines (SP 800-53B)	Maintain configuration control over specified system components awaiting service or repair and serviced or repaired components awaiting return to service Incorporates withdrawn control SA-19(2)
1190	SR-11(3)	Component Authenticity | Anti-Counterfeit Scanning					Y	New control enhancement	Periodically scan for counterfeit system components Incorporates withdrawn control SA-19(4)
1191	SR-12	Component Disposal		X	X	X	Y	New base control Adds to L, M, and H Security Control Baselines (SP 800-53B)	Dispose of specified data, documentation, tools, or system components using the specified techniques and methods Incorporates withdrawn control SA-19(3)

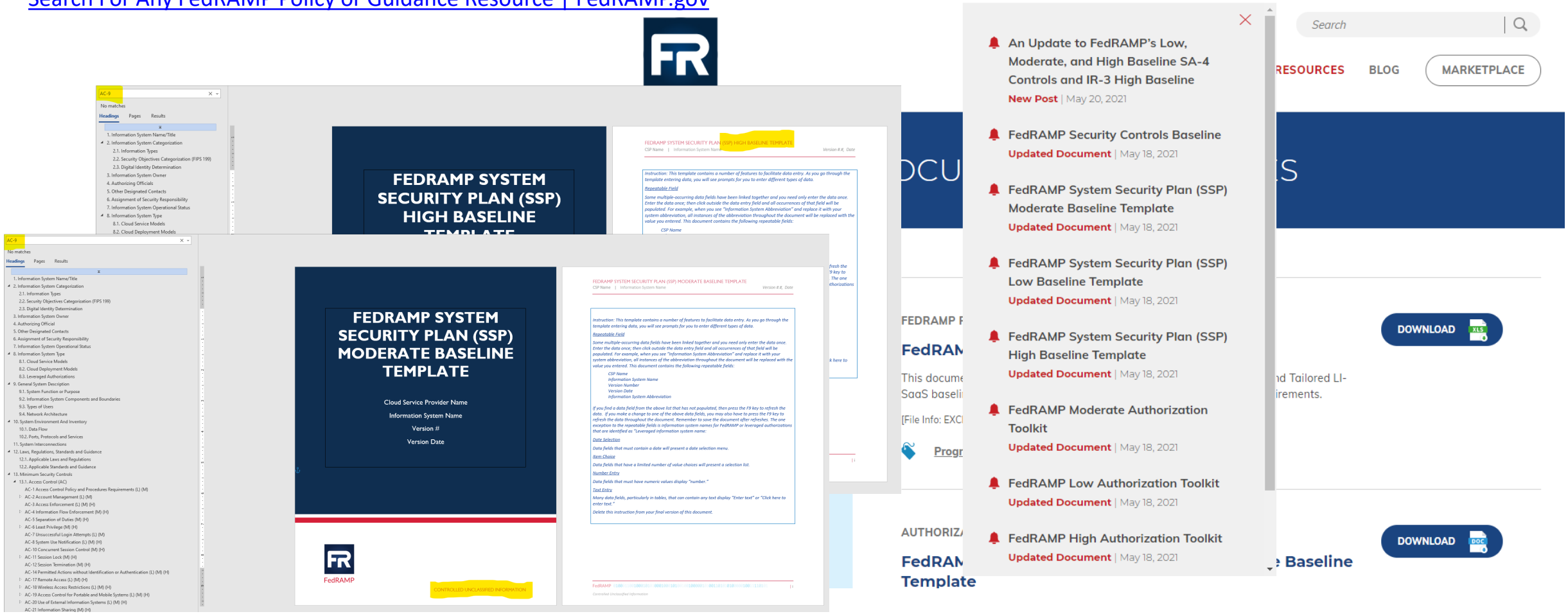
- Big Domains/Families 20
- Medium Controls/Universe 298
- Small Tests Enhancements Detail 709

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Some of the New Controls Affect the SSP Baselines
Some Controls Do Not appear in any Baseline

EnterpriseGRC Solutions, Inc.

[Search For Any FedRAMP Policy or Guidance Resource | FedRAMP.gov]



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

These Controls Are Not Part of any Baseline

EnterpriseGRC Solutions, Inc.

Ctrl ID	Control Name				
AC-9	Previous Logon Notification	PE-22	Component Marking	SC-40	Wireless Link Protection
AC-16	Security and Privacy Attributes	PE-23	Facility Location	SC-41	Port and I/O Device Access
AC-23	Data Mining Protection	PL-7	Concept of Operations	SC-42	Sensor Capability and Data
AC-24	Access Control Decisions	RA-6	Technical Surveillance Countermeasures Survey	SC-43	Usage Restrictions
AC-25	Reference Monitor	RA-10	Threat Hunting	SC-44	Detonation Chambers
AT-6	Training Feedback	SA-20	Customized Development of Critical Components	SC-45	System Time Synchronization
AU-13	Monitoring for Information Disclosure	SA-23	Specialization	SC-46	Cross Domain Policy Enforcement
AU-14	Session Audit	SC-6	Resource Availability	SC-47	Alternate Communications Paths
AU-16	Cross-organizational Audit Logging	SC-11	Trusted Path	SC-48	Sensor Relocation
CM-13	Data Action Mapping	SC-16	Transmission of Security and Privacy Attributes	SC-49	Hardware-enforced Separation and Policy Enforcement
CM-14	Signed Components	SC-25	Thin Nodes	SC-50	Software-enforced Separation and Policy Enforcement
CP-11	Alternate Communications Protocols	SC-26	Decoys	SC-51	Hardware-based Protection
CP-12	Safe Mode	SC-27	Platform-independent Applications	SI-13	Predictable Failure Prevention
CP-13	Alternative Security Mechanisms	SC-29	Heterogeneity	SI-14	Non-persistence
IA-9	Service Identification and Authentication	SC-30	Concealment and Misdirection	SI-15	Information Output Filtering
IA-10	Adaptive Authentication	SC-31	Covert Channel Analysis	SI-17	Fail-safe Procedures
IR-9	Information Spillage Response	SC-32	System Partitioning	SI-20	Tainting
MA-7	Field Maintenance	SC-34	Non-modifiable Executable Programs	SI-21	Information Refresh
MP-8	Media Downgrading	SC-35	External Malicious Code Identification	SI-22	Information Diversity
PE-19	Information Leakage	SC-36	Distributed Processing and Storage	SI-23	Information Fragmentation
PE-20	Asset Monitoring and Tracking	SC-37	Out-of-band Channels	SR-4	Provenance
PE-21	Electromagnetic Pulse Protection	SC-38	Operations Security	SR-7	Supply Chain Operations Security

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

These Controls & Enhancements are withdrawn / replaced

EnterpriseGRC Solutions, Inc.

CTRL ID	Control Name				
AT-3.4	AT-3.4 Suspicious Communications and Anomalous System Behavior	IA-9.2	IA-9.2 Transmission of Decisions	SA-12.15	SA-12.15 Processes to Address Weaknesses or Deficiencies
AU-2.3	AU-2.3 Reviews and Updates	IR-9.1	IR-9.1 Responsible Personnel	SA-18.1	SA-18.1 Multiple Phases of System Development Life Cycle
AU-3.2	AU-3.2 Centralized Management of Planned Audit Record Content	PE-5.1	PE-5.1 Access to Output by Authorized Individuals	SA-18.2	SA-18.2 Inspection of Systems or Components
AU-7.2	AU-7.2 Automatic Sort and Search	PE-5.3	PE-5.3 Marking Output Devices	SA-19.1	SA-19.1 Anti-counterfeit Training
AU-8.1	AU-8.1 Synchronization with Authoritative Time Source	PE-18.1	PE-18.1 Facility Site	SA-19.2	SA-19.2 Configuration Control for Component Service and Repair
AU-8.2	AU-8.2 Secondary Authoritative Time Source	PL-2.3	PL-2.3 Plan and Coordinate with Other Organizational Entities	SA-19.3	SA-19.3 Component Disposal
AU-14.2	AU-14.2 Capture and Record Content	SA-12.1	SA-12.1 Acquisition Strategies / Tools / Methods	SA-19.4	SA-19.4 Anti-counterfeit Scanning
CA-3.1	CA-3.1 Unclassified National Security System Connections	SA-12.2	SA-12.2 Supplier Reviews	SA-22.1	SA-22.1 Alternative Sources for Continued Support
CA-3.2	CA-3.2 Classified National Security System Connections	SA-12.5	SA-12.5 Limitation of Harm	SC-34.3	SC-34.3 Hardware-based Protection
CA-3.3	CA-3.3 Unclassified Non-national Security System Connections	SA-12.7	SA-12.7 Assessments Prior to Selection / Acceptance / Update	SC-42.3	SC-42.3 Prohibit Use of Devices
CA-3.4	CA-3.4 Connections to Public Networks	SA-12.8	SA-12.8 Use of All-source Intelligence	SI-2.1	SI-2.1 Central Management
CA-3.5	CA-3.5 Restrictions on External System Connections	SA-12.9	SA-12.9 Operations Security	SI-3.1	SI-3.1 Central Management
CM-5.2	CM-5.2 Review System Changes	SA-12.10	SA-12.10 Validate as Genuine and Not Altered	SI-3.9	SI-3.9 Authenticate Remote Commands
CM-5.3	CM-5.3 Signed Components	SA-12.11	SA-12.11 Penetration Testing / Analysis of Elements, Processes, and Actors	SI-7.11	SI-7.11 Confined Environments with Limited Privileges
CM-8.5	CM-8.5 No Duplicate Accounting of Components	SA-12.12	SA-12.12 Inter-organizational Agreements	SI-7.13	SI-7.13 Code Execution in Protected Environments
CP-2.4	CP-2.4 Resume All Mission and Business Functions	SA-12.14	SA-12.14 Identity and Traceability	SI-7.14	SI-7.14 Binary or Machine Executable Code
IA-9.1	IA-9.1 Information Exchange			SI-8.1	SI-8.1 Central Management

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

268 New & Substantially changed Enhancements and Controls

EnterpriseGRC Solutions, Inc.

- 20 (Big) Family Domains PT, SR
- 298 (Medium) Control Family /Universe (example AC-2)
- 709 (Child Small) Tests Enhancements (example AC-2(3))

A	B	C	D	E	F	G	H	I
Rev 5 Update	**NIST SP 800-53 Rev 5 Controls**	**NIST SP 800-53B Control Baselines**				**More than editorial or administrative change? (Y/N)**	**Changed Elements**	**Change Details**
CA-3(6)	Information Exchange | Transfer Authorizations				X	Y	New control enhancement Adds to H Security Control Baseline (SP 800-53B)	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations
CA-3(7)	Information Exchange | Transitive Information Exchanges					Y	New control enhancement	Identify transitive (downstream) information exchanges with other systems and take measures to ensure that transitive information exchanges cease when the controls cannot be verified or validated
CA-6(1)	Authorization | Joint Authorization — Intra - Organization					Y	New control enhancement	Employ a joint authorization process that includes multiple authorizing officials from the same organization
CA-6(2)	Authorization | Joint Authorization — Inter - Organizations					Y	New control enhancement	Employ a joint authorization process that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization
CA-7(4)	Continuous Monitoring | Risk Monitoring	X	X	X	X	Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B) Adds to L, M, and H Security Control Baselines (SP 800-53B)	Ensure risk monitoring is an integral part of the continuous monitoring strategy
CA-7(5)	Continuous Monitoring | Consistency Analysis					Y	New control enhancement	Employ specific actions to validate that policies are established and implemented controls operate in a consistent manner
CA-7(6)	Continuous Monitoring | Automation Support for Monitoring					Y	New control enhancement	Ensure the accuracy, currency, and availability of monitoring results for the system using specified automated mechanisms
CA-8(3)	Penetration Testing | Facility Penetration Testing					Y	New control enhancement	Employ a penetration testing process that includes defined frequency of announced and unannounced attempts to bypass or circumvent physical access point controls
CM-3(7)	Configuration Change Control | Review System Changes					Y	New control enhancement	Review changes to the system at a specific frequency or for specific circumstances to determine whether unauthorized changes have occurred Incorporates withdrawn control CM-5(2)
CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes					Y	New control enhancement	Prevent or restrict changes to the configuration of the system under the specific circumstances
CM-7(6)	Least Functionality | Confined Environments With Limited Privileges					Y	New control enhancement	Requires specified user-installed software execute in a confined physical or virtual machine environment with limited privileges Incorporates withdrawn control SI-7(11)

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

75 Changes have implications in the Baselines, NIST 800-53B

EnterpriseGRC Solutions, Inc.

- Privacy Attribute (P)
- Part of Low, Medium, High
- Changes to details and modifications to the baselines used for FedRamp
- Addition of S/O/SO attribute
- Associated Tailoring Criteria

Rev 5 Update	NIST SP 800-53 Rev 5 Controls	NIST SP 800-53B Control Baselines				More than editorial or administrative change? (Y/N)	Changed Elements	Change Details
AC-3(14)	Access Enforcement | Individual Access	X				Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B)	Mechanisms for individuals to have access to PII Incorporates individual access elements of withdrawn App J control IP-2
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining			X	X	Y	New control enhancement Adds to M and H Security Control Baselines (SP 800-53B)	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining
AT-3(5)	Role-Based Training | Processing Personally Identifiable Information	X				Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B)	Provide specific personnel or roles with initial and at a specific frequency training in the employment and operation of PII processing and transparency controls Incorporates training elements of withdrawn App J control UL-2
AU-3(3)	Content of Audit Records | Limit Personally Identifiable Information Elements	X				Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B)	Limit PII contained in audit records to the specific elements identified in the privacy risk assessment
CA-3(6)	Information Exchange | Transfer Authorizations				X	Y	New control enhancement Adds to H Security Control Baseline (SP 800-53B)	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations
CA-7(4)	Continuous Monitoring | Risk Monitoring	X	X	X	X	Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B) Adds to L, M, and H Security Control Baselines (SP 800-53B)	Ensure risk monitoring is an integral part of the continuous monitoring strategy
CM-12	Information Location			X	X	Y	New base control Adds to M and H Security Control Baselines (SP 800-53B)	Identify and document the location of specific information and the specific system components on which the information resides; the users who have access; and changes to the location where the information resides
CM-12(1)	Information Location | Automated Tools to Support Information Location			X	X	Y	New control enhancement Adds to M and H Security Control Baselines (SP 800-53B)	Use automated tools to identify specific information by information type on specific system components to ensure controls are in place to protect organizational information and individual privacy
CP-9(8)	System Backup | Cryptographic Protection			X	X	Y	New control enhancement Adds to M and H Security Control Baselines (SP 800-53B)	Requires implementing cryptographic mechanisms to prevent unauthorized disclosure and modification of specified backup information
IA-12	Identity Proofing			X	X	Y	New base control Adds to M and H Security Control Baselines (SP 800-53B)	Identity proof users for logical access based on identity assurance level requirements
IA-12(2)	Identity Proofing | Identity Evidence			X	X	Y	New control enhancement Adds to M and H Security Control Baselines (SP 800-53B)	Requiring evidence of individual identification be presented to the registration authority reduces the likelihood of individuals using fraudulent identification to establish an identity Incorporates withdrawn control IA-4(3)

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Three Tiers – Domain, Control, Test

EnterpriseGRC Solutions, Inc.

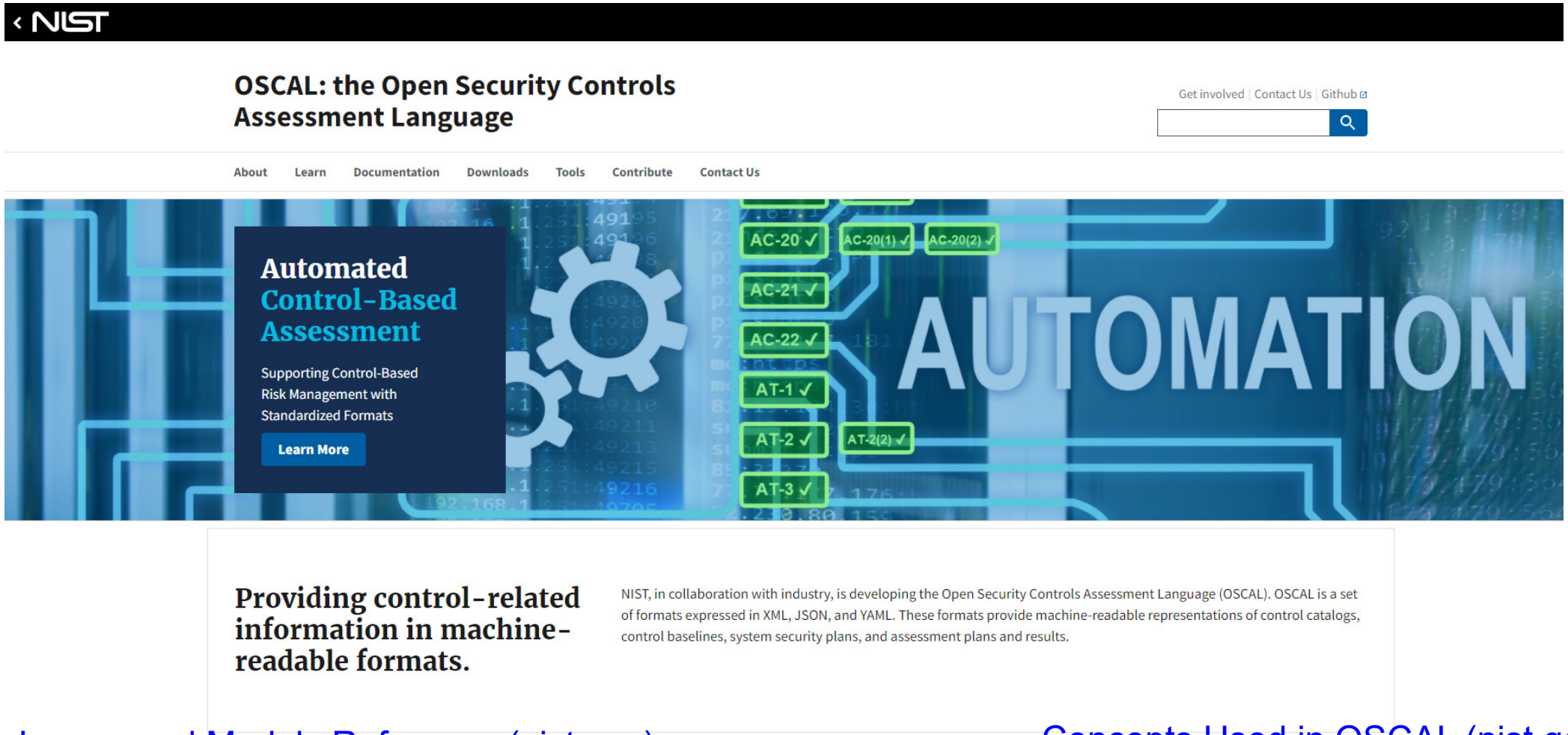
Assessment Edition or Source	Assessment Domain ID	Assessment Domain Name	Assessment Control ID	Assessment Universe.Control Control Objective	Assessment Universe.Control Control Objective Description	Assessment Universe.Risk Risk	Assessment Universe.TestingPro TestingProcedure	Assessment Universe.Test ID Test ID	Assessment Unified Testing Map	Assessment Unified Universe Mapping	Assessment Privacy Control Baseline	Assessment IMPLEMENTED BY	Assessment Assurance	Assessment Baseline Low	Assessment Baseline Medium	Assessment Baseline High	Assessment Testing.Test_ID Test_ID	Assessment Testing.Detail Detail Control Objective	Assessment Testing.Detail Control Description (UCF) Detail Control Description (UCF)	Assessment Testing.Problem Problem Metadata	Assessment Testing.Privac Privacy	Assessment Testing.Assurance Assurance
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-1	AC-1 Access Control Policy and Procedures	Control: a. Develop, document, and disseminate to [Assignment:	Discussion: Access control policy and procedures address the controls in the AC	References: [SP 800-162], [SP 800-178], [SP 800-192].		A.5.1.1, A.6.1.1, A.9.1.1, A.12.1.1,	A.6.1, A.9.1, A.12.1, GMP5_6.												
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.1 Automated System Account Management	AC-2.1 Automated System Account Management	ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT Employ automated mechanisms to support the management of system accounts. Supplemental Guidance: The use of automated	AUTOMATIC NOTIFICATION; MONITOR ACCOUNT USAGE; TELEPHONE NOTIFICATION; EMAIL		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.2 Automated Temporary and Emergency Account Management	AC-2.2 Automated Temporary and Emergency Account Management	ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY AND EMERGENCY ACCOUNTS Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time-period for each type of account].	AUTOMATICALLY REMOVE; AUTOMATICALLY DISABLE; TEMPORARY ACCOUNTS		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.3 Disable Accounts	AC-2.3 Disable Accounts	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS Automatically disable accounts when the accounts: (a) Have expired; (b) Are no longer associated to a user; (c) Are in violation of organizational policy;	AUTOMATICALLY DISABLE; INACTIVE ACCOUNTS		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.4 Automated Audit Actions	AC-2.4 Automated Audit Actions	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS Automatically audit account creation, modification, enabling, disabling, and removal actions, and notify [Assignment: organization-defined personnel or roles]. Supplemental Guidance: None.	AUTOMATED AUDIT; ACCOUNT CREATION; ACCOUNT MODIFICATION; ACCOUNT ENABLING;		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.5 Inactivity Logout	AC-2.5 Inactivity Logout	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT Require that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]. Supplemental Guidance: This control enhancement is	INACTIVITY; LOGOUT		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.6 Dynamic Privilege Management	AC-2.6 Dynamic Privilege Management	ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT Implement the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities].	DYNAMIC PRIVILEGE MANAGEMENT; DYNAMIC ACCESS CONTROL; RESILIENCY; RESILIENCE		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.7 Privileged User Accounts	AC-2.7 Privileged User Accounts	ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed system access and privileges into roles;	PRIVILEGED USER ACCOUNTS; PRIVILEGED ROLE ASSIGNMENTS; ROLE BASED ACCESS		
NIST 800-53 r5	AC 800-53-R5	AC - ACCESS CONTROL	AC-2	AC-2 Account Management	Control: a. Define and document the types of system accounts allowed for use	Discussion: Examples of system account types include individual, shared, group,	References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(6), AC-2(7), AC-2(8), AC-2(9), AC-2(11), AC-	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	A.9.2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-		O		AC-2	AC-2	AC-2	AC-2.8 Dynamic Account Management	AC-2.8 Dynamic Account Management	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically. Supplemental Guidance: Approaches for dynamically	DYNAMIC ACCOUNT CREATION; TRUST RELATIONSHIPS; RESILIENCY; RESILIENCE		

Is This Part of Privacy, Cyber, Data Baseline

At issue in mapping: Source Documents Control ID v. Enhancement – Detail IDs without meaningful identifiers Attributes added under certification conditions, v. core control statement

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

You CANNOT do this by hand - OSCAL (nist.gov)



Layers and Models Reference (nist.gov)

Concepts Used in OSCAL (nist.gov)

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Attribute Changes Manual & Automation Resources

EnterpriseGRC Solutions, Inc.

Tailoring Criteria for NIST 171 Depend Upon 800-53

- (171r2) security controls are taken from NIST Special Publication 800-53, Revision 4. These ***tables will be updated upon publication of [SP 800-53B]*** which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements
- The same *tailoring criteria* were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements
- There is a close relationship between the security objectives of confidentiality and integrity. Therefore, the security controls in the [SP 800-53] moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.
- 39 The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

FedRAMP OSCAL Resources and Templates

FedRAMP has published resources to aid stakeholders and vendors in the digitization of FedRAMP authorization package content. Located on the FedRAMP Automation GitHub Repository, these include:

- *New* - **Guide to OSCAL-based FedRAMP Content**. Guidance and concepts common to all FedRAMP deliverables when using OSCAL.
- *Revised* - **Guide to OSCAL-based FedRAMP System Security Plans (SSP)**.
- *New* - **Guide to OSCAL-based FedRAMP Security Assessment Plans (SAP)**.
- *New* - **Guide to OSCAL-based FedRAMP Security Assessment Reports (SAR)**.
- *New* - **Guide to OSCAL-based FedRAMP Plan of Action and Milestones (POA&M)**.
- *Revised* - **Updated FedRAMP OSCAL Registry**.
  Revised - **OSCAL-based FedRAMP SSP Templates/Samples**.
  FedRAMP SSP Template in both XML and JSON formats.
- *New* - **OSCAL-based FedRAMP Templates/Samples**.
  There are now three additional templates/samples covering the SAP, SAR, and POA&M. These exist in both XML and JSON formats.
- *Revised* - **FedRAMP Baselines**. (XML and JSON formats)
  The baselines now include a "CORE" property, enabling tools to identify the FedRAMP core controls; as well as the assessment objectives and methods (Examine, Interview, Test) found in a blank test case workbook (TCW).
- *New* - **Experimental Resources**.
  FedRAMP is offering additional support files to aid tool developers. These provide content in XML and JSON that is relevant to FedRAMP authorization packages yet does not fit in the official OSCAL syntax.

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

ISACA San Francisco Chapter | ISC² Silicon Valley | ISC² Chapter

Mapping Guidance for ISO/IEC 27001:2013 does not consider additional content for ISO/IEC 27017 Cloud, 27701 Privacy, 27018 Processing – IT NEEDS TO

EnterpriseGRC Solutions, Inc.

Table 1 provides a mapping from the security controls in NIST Special Publication 800-53 to the security controls in ISO/IEC 27001. Please review the introductory text above before employing the mappings in Table 1.

TABLE 1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
AC-1	Access Control Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Access Enforcement	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	Information Flow Enforcement	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	Separation of Duties	A.6.1.2
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Unsuccessful Logon Attempts	A.9.4.2
AC-8	System Use Notification	A.9.4.2
AC-9	Previous Logon Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Device Lock	A.11.2.8, A.11.2.9
AC-12	Session Termination	None
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	**Withdrawn**	---
AC-16	Security and Privacy Attributes	None
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	Wireless Access	A.6.2.1, A.13.1.1, A.13.2.1
AC-19	Access Control for Mobile Devices	A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1
AC-20	Use of External Systems	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.9.4.1*
AC-25	Reference Monitor	None
AT-1	Awareness and Training Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	Literacy Training and Awareness	7.3, A.7.2.2, A.12.2.1
AT-3	Role-Based Training	A.7.2.2*
AT-4	Training Records	None
AT-5	**Withdrawn**	---
AT-6	Training Feedback	None
AU-1	Audit and Accountability Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	Event Logging	None
AU-3	Content of Audit Records	A.12.4.1*
AU-4	Audit Log Storage Capacity	A.12.1.3
AU-5	Response to Audit Logging Process Failures	None
AU-6	Audit Record Review, Analysis, and Reporting	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	Audit Record Reduction and Report Generation	None
AU-8	Time Stamps	A.12.4.4
AU-9	Protection of Audit Information	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.12.1.3
AU-12	Audit Record Generation	A.12.4.1, A.12.4.3
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	A.12.4.1*
AU-15	**Withdrawn**	---
AU-16	Cross-Organizational Audit Logging	None
CA-1	Assessment, Authorization, Policies and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
CA-2	Control Assessments	8.3, 9.2, A.18.2.2, A.18.2.3*
CA-3	Information Exchange	A.13.1.2, A.13.2.1, A.13.2.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	8.3, 9.2, 10.1*
CA-6	Authorization	9.3*
CA-7	Continuous Monitoring	9.1, 9.2, A.18.2.2, A.18.2.3*
CA-8	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM-2	Baseline Configuration	None
CM-3	Configuration Change Control	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM-4	Impact Analyses	A.14.2.3
CM-5	Access Restrictions for Change	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM-6	Configuration Settings	None
CM-7	Least Functionality	A.12.5.1*
CM-8	System Component Inventory	A.8.1.1, A.8.1.2
CM-9	Configuration Management Plan	A.6.1.1
CM-10	Software Usage Restrictions	A.18.1.2
CM-11	User-Installed Software	A.12.5.1, A.12.6.2
CM-12	Information Location	None
CM-13	Data Action Mapping	None
CM-14	Signed Components	None
CP-1	Contingency Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.17.1.1, A.17.2.2
CP-2	Contingency Plan	7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1
CP-3	Contingency Training	A.7.2.2*
CP-4	Contingency Plan Testing	A.17.1.3
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.11.1.6, A.17.1.2, A.17.2.1
CP-7	Alternate Processing Site	A.11.1.6, A.17.1.2, A.17.2.1
CP-8	Telecommunications Services	A.11.2.2, A.17.1.2
CP-9	System Backup	A.12.3.1, A.17.1.2, A.18.1.3
CP-10	System Recovery and Reconstitution	A.17.1.2
CP-11	Alternate Communications Protocols	A.17.1.2*
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.17.1.2*
IA-1	Identification and Authentication Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
PE-9	Power Equipment and Cabling	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
PE-10	Emergency Shutoff	A.11.2.2*
PE-11	Emergency Power	A.11.2.2*
PE-12	Emergency Lighting	A.11.2.2*
PE-13	Fire Protection	A.11.1.4, A.11.2.1
PE-14	Environmental Controls	A.11.1.4, A.11.2.1, A.11.2.2
PE-15	Water Damage Protection	A.11.1.4, A.11.2.1, A.11.2.2
PE-16	Delivery and Removal	A.8.2.3, A.11.1.6, A.11.2.5
PE-17	Alternate Work Site	A.6.2.2, A.11.2.6, A.13.2.1
PE-18	Location of System Components	A.11.2.1
PE-19	Information Leakage	A.11.1.4, A.11.2.1
PE-20	Asset Monitoring and Tracking	A.8.2.3*
PE-21	Electromagnetic Pulse Protection	None
PE-22	Component Marking	A.8.2.2
PE-23	Facility Location	A.11.1.4, A.11.2.1
PL-1	Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL-2	System Security and Privacy Plans	7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.7.1.2, A.7.2.1, A.8.1.3
PL-5	**Withdrawn**	---
PL-6	**Withdrawn**	---
PL-7	Concept of Operations	8.1, A.14.1.1
PL-8	Security and Privacy Architectures	A.14.1.1*
PL-9	Central Management	None
PL-10	Baseline Selection	None
PL-11	Baseline Tailoring	None
PM-1	Information Security Program Plan	4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3, 10.2, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
PM-2	Information Security Program Leadership Role	5.1, 5.3, A.6.1.1
PM-3	Information Security and Privacy Resources	5.1, 6.2, 7.1
PM-4	Plan of Action and Milestones Process	6.1.1, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.2, 9.3, 10.1
PM-5	System Inventory	None
PM-6	Measures of Performance	5.3, 6.1.1, 6.2, 9.1,
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.3, 10.2
PM-10	Authorization Process	9.3, A.6.1.1*
PM-11	Mission and Business Process Definition	4.1
PM-12	Insider Threat Program	None
PM-13	Security and Privacy Workforce	7.2.2*
PM-14	Testing, Training, and Monitoring	
PM-15	Security and Privacy Groups and Associations	7.4, A.6.1.4
PM-16	Threat Awareness Program	None
PM-17	Protecting Controlled Unclassified Information on External Systems	None
PM-18	Privacy Program Plan	None
PM-19	Privacy Program Leadership Role	None
PM-20	Dissemination of Privacy Program Information	None

PE-7	**Withdrawn**	---
PE-8	Visitor Access Records	None

For the ISO/IEC 27001 using ISO/IEC 27002:2013 € *(Plus Privacy, Processing, Cloud)*
ISO/IEC 27017:2015 € 27002 for cloud services
ISO/IEC 27701:2019 € Privacy
ISO/IEC 27018:2019 € Processing

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

ISACA San Francisco Chapter | ISO Silicon Valley Chapter | ISO San Diego Chapter

Misunderstood Content – due to lack of a control library and lack of subject matter experience by domain and assessment.

EnterpriseGRC Solutions, Inc.

Test_ID	Edition or Source	Control ID:Co...	Policy Review Status	Detail Control Description (UCF)	Mapped testing or practices	Mapping Status	PIMS Specification ISO/IEC 277...	Policies Standards
ISO2701_C6.1.1 General	ISO/IEC 27001:2013 €	C.6.1 Actions to addre...	PIMS Applied 27701/27018	6.1.1 General When planning for the information security management system, the organization shall consi...	A.12.6.1; A.18.2.1; A.12.7.1; A.16.1.4; CA-2(2); CA-9...	ISO27001/27002/27017/27...	ISO/IEC 27701:2019(E) 5.4.1 Actions to ...	Information Security a
ISO2701_C6.1.2 Information security risk assessment	ISO/IEC 27001:2013 €	C.6.1 Actions to addre...	PIMS Applied 27701/27018	6.1.2 Information security risk assessment The organization shall define and apply an information security ri...	A.12.6.1; A.18.2.1; A.12.7.1; A.16.1.4; CA-2(2); CA-9...	ISO27001/27002/27017/27...	ISO/IEC 27701:2019(E) 5.4.1 Actions to ...	Code of Conduct Polic
ISO2701_C6.1.3 Information security risk treatment	ISO/IEC 27001:2013 €	C.6.1 Actions to addre...	PIMS Applied 27701/27018	6.1.3 Information security risk treatment The organization shall define and apply information security *and p...*	A.12.6.1; A.18.2.1; A.12.7.1; A.16.1.4; CA-2(2); CA-9...	ISO27001/27002/27017/27...	ISO/IEC 27701:2019(E) 5.4.1.3 Informat...	CAPA Log Form; CAPA
ISO2701_C7.5.1 General - Documented information	ISO/IEC 27001:2013 €	C.7.5 Documented inf...	PIMS Applied 27701/27018	7.5.1 General - Documented information The organization's information security *and privacy* management s...	A.12.1.1; ISO13485_7.5.1; CM-3(1); CM-3(2); SA-8(2...	ISO27001/27002/27017/27...	ISO/IEC 27701:2019(E) 5.5.5.1 General ...	Document Manageme
ISO2701_C7.5.2 Creating and updating documented informa...	ISO/IEC 27001:2013 €	C.7.5 Documented inf...	PIMS Applied 27701/27018	7.5.2 Creating and updating - Documented information When creating and updating documented informati...	A.12.1.1; A.12.7.1; ISO13485_7.5.1; CM-3(1); CM-3(...	ISO27001/27002/27017/27...	ISO/IEC 27701:2019(E) 5.5.5.2 Creating ...	Document Manageme
ISO2701_C7.5.3 Control of documented information	ISO/IEC 27001:2013 €	C.7.5 Documented inf...	PIMS Applied 27701/27018	7.5.3 Control of documented information Documented information required by the information security *an...*	A.12.1.1; A.12.7.1; ISO13485_7.5.1; CM-3(1); CM-3(...	ISO27001/27002/27017/27...	ISO/IEC 27701:2019(E) 5.5.5.3 Control ...	Document Manageme
A.5.1.1 Policies for information security	ISO/IEC 27002:2013 €	A.5.1 Management dir...	PIMS Applied 27701/27018	Policy: The Information Security and Privacy Policy outlines the high-level policies and principles that must ...	A.6.1.1; HT_4.a; HT_4.b; HT_6.b; HT_6.d; HT_6.e; HT...	ISO27001/27002/27017/27...	ISO/IEC 27018:2019(E) 5.1.1 Policies for...	Acceptable Use Policy;
A.5.1.2 Review of the policies for information security	ISO/IEC 27002:2013 €	A.5.1 Management dir...	PIMS Applied 27701/27018	Policy: The CIO, (Chief Information Officer) and CSO (Chief Security Officer) are responsible for the mainten...	HT_6.b; HT_6.d; HT_6.e; HT_6.f; GMP5_ADX_O11-4....	ISO27001/27002/27017/27...	ISO/IEC 27018:2019(E) 5.1.2 Review of ...	Information Security a
A.6.1.1 Information security roles and responsibilities	ISO/IEC 27002:2013 €	A.6.1 Internal organiz...	PIMS Applied 27701/27018	Policy: Allocation of information security *and privacy* responsibilities is done in accordance with the informa...	HT_2.a; HT_2.d; HT_2.e; HT_5.c; GMP5_ADX_ M1-5....	ISO27001/27002/27017/27...	ISO/IEC 27018:2019(E) 6.1.1 Informati...	Code of Conduct Polic
A.6.1.2 Segregation of duties	ISO/IEC 27002:2013 €	A.6.1 Internal organiz...	PIMS Applied 27701/27018	Policy: Assets used in the path of critical business operations, such as those related to revenue, provisioning ...	A.13.1.2; A.13.1.3; SC-7(20); HT_9.ab; HT_9.c; HT_9....	ISO27001/27002/27017/27...	ISO/IEC 27018:2019(E) (E) 6.1.2 Segreg...	Asset Life Cycle Manag
A.6.1.3 Contact with authorities	ISO/IEC 27002:2013 €	A.6.1 Internal organiz...	PIMS Applied 27701/27018	Policy: Cooperation between organizations The CSO must maintain appropriate contacts with such agencies ...	HT_5.a; HT_5.b; HT_5.c; HT_5.d; HT_5.e; HT_5.f; HT_...	ISO27001/27002/27017/27...	ISO/IEC 27018:2019(E) 6.1.3 Contact wi...	Incident Management
A.6.1.4 Contact with special interest groups	ISO/IEC 27002:2013 €	A.6.1 Internal organiz...	PIMS Applied 27701/27018	Policy: Information Security Privacy and Risk Management personnel are required to maintain appropriate c...	HT_5.a; HT_5.b; HT_5.c; HT_5.d; HT_5.e; HT_5.f; HT_...	ISO/NIST/LSHC up to dat	ISO/IEC 27018:2019(E) 6.1.4 Contact wi...	Information Security a
A.6.1.5 Information security in project management	ISO/IEC 27002:2013 €	A.6.1 Internal organiz...	PIMS Applied 27701/27018	Policy: Information Security must be addressed in project management, regardless of the type of project. Inf...	SA-3(3); SA-9(1); SA-9(2); SA-9(3); SA-9(4); SA-9(...	ISO/NIST/LSHC up to dat	ISO/IEC 27018:2019(E) 6.1.5 Informa...	Information Technolog
A.6.2.1 Mobile device policy	ISO/IEC 27002:2013 €	A.6.2 Mobile devices ...	PIMS Applied 27701/27018	Policy: The company allows the use of mobile devices to access email and wireless networks. The Mobile De...	AC-4(25); AC-7(2); SI-4(3); 11.10(h); AC-19(4); AC-1...	ISO/NIST/LSHC up to dat	ISO/IEC 27018:2019(E) 6.2 Mobile de...	Bring Your Own Device
A.6.2.2 Teleworking	ISO/IEC 27002:2013 €	A.6.2 Mobile devices ...	PIMS Applied 27701/27018	Policy: Company management determines the location for work as a part of job description. Once a location...	A.11.2.6; HT_1.y; N171_3.10.6; AC-17(1); SC-7(7); ...	ISO/NIST/LSHC up to dat	ISO/IEC 27018:2019(E) 6.2 Mobile de...	Bring Your Own Device
A.7.1.1 Screening	ISO/IEC 27002:2013 €	A.7.1 Prior to employ...	PIMS Applied 27701/27018	Policy: Employee and consultant new hire verification is coordinated by HR. In conjunction with the inputs fro...	12.7.0 MISP; A.15.1.2; PS-3(1); PS-3(2); PS-3(3); P...	ISO/NIST/LSHC up to dat	ISO/IEC 27018:2019(E) 7.1 Prior to emp...	Acceptable Use Policy;
A.7.1.2 Terms and conditions of employment	ISO/IEC 27002:2013 €	A.7.1 Prior to employ...	PIMS Applied 27701/27018	Policy: The contractual obligations for employees or contractors should reflect the organization's policies fo...	GMP5_ADX_S5-2.2.5; HT_2.c; HT_5.e; PL-4(1); PS-3(...	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 7.1 Prior to emp...	Acceptable Use Policy;
A.7.2.1 Management responsibilities	ISO/IEC 27002:2013 €	A.7.2 During employ...	PIMS Applied 27701/27018	Policy: Management responsibilities should include ensuring that employees and contractors: are properly b...	A.7.2.1; A.7.2.2; HT_2.a; HT_2.d; HT_2.e; GMP5_4.3....	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 7.2.1 Managem...	Security and Privacy A
A.7.2.2 Information security awareness, education and traini...	ISO/IEC 27002:2013 €	A.7.2 During employ...	PIMS Applied 27701/27018	Policy: An information security and privacy awareness program is in place to make employees and, where re...	A.7.2.1; A.7.2.2; HT_2.a; HT_2.d; HT_2.e; GMP5_4.3....	ISO27001/27002/27017/27...	ISO/IEC 27018:2019(E) 7.2.2 Informatio...	Security and Privacy A
A.7.2.3 Disciplinary process	ISO/IEC 27002:2013 €	A.7.2 During employ...	PIMS Applied 27701/27018	Policy: The disciplinary process should not be commenced without prior verification that an information sec...	11.10(i); A.7.2.1; A.7.2.2; A.16.1.6; AT-2(1); AT-2(2);...	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 7.2.3 Disciplinar...	Code of Conduct Polic
A.7.3.1 Termination or change of employment responsibilities	ISO/IEC 27002:2013 €	A.7.3 Termination and...	PIMS Applied 27701/27018	Policy: The communication of termination responsibilities including ongoing information security requirem...	A.7.3.1; CLD.8.1.5; AC-2(12); AC-2(14); PS-4	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 7.3 Termination ...	Access and Administr

Test level – Source, Clause/Section, Control, Test

Source

Updates base on additional certifications (blue)

Additional detail based upon PIMS

Only relevant when mapped to your policies and standards

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

ISACA San Francisco Chapter · Silicon Valley

NIST 171 r2 and NIST 172 use NIST 800-53 Rev5 as Parent/Family

EnterpriseGRC Solutions, Inc.

https://doi.org/10.6028/NIST.SP.800-172

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations 171 r2

Enhanced Security Requirements for Protecting Controlled Unclassified Information = 172 A Supplement to NIST Special Publication 800-171

https://doi.org/10.6028/NIST.SP.800-172

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

NIST SP800 171r2 and 172 add Protection Strategy and Mapped Meta Data

EnterpriseGRC Solutions, Inc.

Test_ID	Control ID	Edition or Sou...	Mapping...	Risk Drivers	PROTECTION STRATEGY	Detail Control Description (UCF)	Mapped testing or practices	Mapped testi...	Mapped Processes	Mapped Processes:Control Objective	Mapped testing or practices:Problem Metadata
N171_3.1.1 Limit information ...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add AC-2(1);AC-2(2);AC-...		Basic Security Requirements Limit system access to authorized ...	A.6.2.1; A.6.2.2; A.9.1.2; A.9.2.1; A.9.2.2; A....	A.6.2.1 Mobile device...	A.6.2; A.9.1; A.9.2; A.9.4; A.1...	A.6.2 Mobile devices and teleworking; A.9.1 Busin...	AUTOMATIC NOTIFICATION; ...ITOR ACCOUNT USAGE; TELEPHONE NOTIFICATION; EMAIL ALERT ...
N172_3.1.1e Employ dual aut...	N171_3.1	NIST 800-172	NIST800-53...	**Add A.6.1;CA-6 A.6.1.1;...**	Cyber Resiliency Survivability (CRS)	Employ dual authorization to execute critical or sensitive syste...	A.6.1.1; AC-3(2); AU-9(5); CA-6(2); CM-5(...	A.6.1.1 Information s...	A.6.1; CA-6; CM-5; CP-9; M...	A.6.1 Internal organization; CA-6 Authorization; C...	DUAL AUTHORIZATION; PRIVILEGED COMMANDS; TWO-PERSON CONTROL; RESILIENCY; RESILIENCE
N172_3.1.2e Restrict access to...	N171_3.1	NIST 800-172	NIST800-53...	Add A.9.2.1	Penetration Resistant Architecture (PRA)	Restrict access to systems and system components to only thos...	AC-20(3); A.9.2.1	AC-20.3 Non-organiz...	AC-20; A.9.2	AC-20 Use of External Systems; A.9.2 User access ...	BYOD; EXTERNALLY OWNED; RESTRICTIONS; FORENSIC ANALYSIS; BRING YOUR OWN DEVICE
N171_3.1.2 Limit information ...	N171_3.1	NIST 800-171 r2	NIST800-53...	**FIX THIS - "users" is cri...**		Limit system access to the types of transactions and functions t...	A.9.4.1; A.14.1.2; AC-3(3); AC-3(4); AC-3(7...	A.9.4.1 Information a...	A.9.4; A.14.1; AC-3; AC-17	A.9.4 System and application access control; A.14...	MANDATORY ACCESS CONTROL; MAC; MANDATORY ACCESS CONTROL POLICY; LEAST PRIVILEGE; TP
N171_3.1.3 Control the flow o...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add AC-4(10)		Derived Security Requirements Control the flow of CUI in accor...	A.13.1.3; A.13.2.1; A.14.1.2; A.14.1.3; AC-4...	A.13.1.3 Segregation ...	AC-4; A.13.1; A.13.2; A.14.1	AC-4 Information Flow Enforcement; A.13.1 Netw...	DISABLE SECURITY POLICY FILTERS; ENABLE SECURITY POLICY FILTERS
N172_3.1.3e Employ organiza...	N171_3.1	NIST 800-172	NIST800-53...	Add A.13.2.1	Penetration Resistant Architecture (PRA)	Employ [Assignment: organization-defined secure information ...	AC-4(1); AC-4(6); AC-4(8); AC-4(13); AC-4...	AC-4.1 Object Securit...	AC-4; A.13.2	AC-4 Information Flow Enforcement; A.13.2 Infor...	SECURITY ATTRIBUTES; INFORMATION FLOW ENFORCEMENT; METADATA; SECURITY POLICY FILTERS;
N171_3.1.4 Separate the dutie...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add SA-17(7)		Separate the duties of individuals to reduce the risk of malevol...	A.6.1.2; SA-17(7)	A.6.1.2 Segregation o...	AC-5; A.6.1; SA-17	AC-5 Separation of Duties; A.6.1 Internal organiz...	LEAST PRIVILEGE; RESILIENCY; RESILIENCE
N171_3.1.5 Employ the princi...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.9.1.2;A.9.2.3;A.9.4....		Employ the principle of least privilege, including for specific sec...	A.9.1.2; A.9.2.3; A.9.4.4; A.9.4.5; AC-6(1); ...	A.9.1.2 Access to net...	AC-6; A.9.1; A.9.2; A.9.4	AC-6 Least Privilege; A.9.1 Business requirements...	EXPLICIT AUTHORIZATION; ...SSIONS; PRIVILEGES; INTRUSION DETECTION PARAMETERS; RESILI
N171_3.1.6 Use non-privilege...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.9.2.3		Use non-privileged accounts or roles when accessing nonsecuri...	AC-6(2); A.9.2.3	AC-6.2 Non-privilege...	AC-6; A.9.2	AC-6 Least Privilege; A.9.2 User access managem...	ROLE-BASED ACCESS CONTROL; RBAC; PRIVILEGED ACCOUNTS; NON-PRIVILEGED ACCOUNTS; RESIL
N171_3.1.7 Prevent non-privil...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add CM-7(2)		Prevent non-privileged users from executing privileged functio...	AC-6(9); AC-6(10); CM-7(2)	AC-6.9 Log Use of Pri...	AC-6; A.9.2; CM-7	AC-6 Least Privilege; A.9.2 User access managem...	AUDITING PRIVILEGED FUNCTIONS; NON-PRIVILEGED USERS; PRIVILEGED FUNCTIONS; SECURITY SA
N171_3.1.8 Limit unsuccessful...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add AC-9; A.9.4.2; AC-7(2...		Limit unsuccessful logon attempts. DISCUSSION This requirem...	A.9.4.2; AC-7(2); AC-7(3); AC-7(4); AC-9(1...	A.9.4.2 Secure log-on...	AC-7; A.9.4; AC-9	AC-7 Unsuccessful Logon Attempts; A.9.4 System...	MOBILE DEVICE; WIPING; PURGING; UNSUCCESSFUL LOGON; BIOMETRIC; LOGON ATTEMPT LIMIT; A
N171_3.1.9 Provide privacy an...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add PT-4(1);PT-4(2);PT-4...		Provide privacy and security notices consistent with applicable ...	A.9.4.2; PT-4(1); PT-4(2); PT-4(3); PT-5(1); ...	A.9.4.2 Secure log-on...	AC-8; A.9.4; PT-4; PT-5	AC-8 System Use Notification; A.9.4 System and a...	Tailored Consent; Just-in-time Consent; Revocation Revoke Consent; Just-in-time Notice; Privacy Act S
N171_3.1.10 Use session lock ...	N171_3.1	NIST 800-171 r2	NIST800-53...			Use session lock with pattern-hiding displays to prevent access...	AC-11(1); A.11.2.8; A.11.2.9	AC-11.1 PATTERN-HI...	AC-11; A.11.2	AC-11 Device Lock; A.11.2 Equipment	SCREEN CONCEALMENT; SESSION LOCK
N171_3.1.11 Terminate (auto...	N171_3.1	NIST 800-171 r2	NIST800-53...	NIST (SP) 800-171 rev ...		Terminate (automatically) a user session after a defined conditi...	AC-12(3); MA-4(7); A.9.4.2	AC-12.3 Timeout War...	AC-12; MA-4; A.9.4	AC-12 Session Termination; MA-4 Nonlocal Main...	SESSION TERMINATION; REMOTE DISCONNECT VERIFICATION; REMOTE CONNECTION TERMINATIO
N171_3.1.12 Monitor and con...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.12.4.1		Monitor and control remote access sessions. DISCUSSION Rem...	AC-17(1); A.12.4.1	AC-17.1 AUTOMATED...	AC-17; A.12.4	AC-17 Remote Access; A.12.4 Logging and monit...	AUTOMATED MONITORING; AUTOMATED CONTROL
N171_3.1.13 Employ cryptogr...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.9.1.2		Employ cryptographic mechanisms to protect the confidentialit...	AC-17(2); A.9.1.2	AC-17.2 PROTECTIO...	AC-17; A.9.1	AC-17 Remote Access; A.9.1 Business requiremen...	ENCRYPTION; SESSION CONFIDENTIALITY; SESSION INTEGRITY; SECURITY CATEGORIZATION
N171_3.1.14 Route remote ac...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.1...; C... A...		Route remote access via managed access control points. DISCU...	AC-17(3); A.13.2.1; CA-3(6); SC-7(4)	AC-17.3 MANAGED A...	AC-17; A.13.2; CA-3; SC-7	AC-17 Remote Access; A.13.2 Information transfe...	ACCESS CONTROL POINTS; TRUSTED INTERNET CONNECTIONS; HIGH-VALUE ASSETS; SECONDARY C
N171_3.1.15 Authorize remot...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.1...2...		Authorize remote execution of privileged commands and remo...	AC-17(4); A.13.2.1	AC-17.4 PRIVILEGED ...	AC-17; A.13.2	AC-17 Remote Access; A.13.2 Information transfer	PRIVILEGED COMMANDS
N171_3.1.16 Authorize wirele...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add AC-18(1);AC-18(4...		Authorize wireless access prior to allowing such connections. D...	A.6.2.1; A.13.1.1; A.13.2.1; AC-18(1); AC-1...	A.6.2.1 Mobile device...	AC-18; A.6.1; A.13.2	AC-18 Wireless Access; A.6.1 Internal organizatio...	WIRELESS AUTHENTICATION; ENCRYPTION; AUTHORIZED USER; CONFIGURING WIRELESS NETWORK
N171_3.1.17 Protect wireless ...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.1...1		Protect wireless access using authentication and encryption. DI...	AC-18(1); AC-18(5); A.13.1.2	AC-18.1 Authenticati...	AC-18; A.13.1	AC-18 Wireless Access; A.13.1 Network security ...	WIRELESS AUTHENTICATION; ENCRYPTION; WIRELESS TRANSMISSIONS; REDUCE TRANSMISSION PO
N171_3.1.18 Control connecti...	N171_3.1	NIST 800-171 r2	NIST800-53...	**FIX THI...**		Control connection of mobile devices. DISCUSSION A mobile d...	A.6.2.1; AC-7(2); AC-19(4); AC-19(5); CM-...	A.6.2.1 Mobile device...	A.6.2; AC-7; SC-18; SC-28; ...	A.6.2 Mobile devices and teleworking; AC-7 Unsu...	MOBILE DEVICE; WIPING; PURGING; UNSUCCESSFUL LOGON; UNCLASSIFIED MOBILE DEVICES; CLAS
N171_3.1.19 Encrypt CUI on ...	N171_3.1	NIST 800-171 r2	NIST800-53...			Encrypt CUI on mobile devices and mobile computing platform...	AC-19(5)	AC-19.5 Full Device o...	AC-19	AC-19 Access Control for Mobile Devices	FULL-DEVICE ENCRYPTION; CONTAINER-BASED ENCRYPTION
N171_3.1.20 Verify and contr...	N171_3.1	NIST 800-171 r2	NIST800-53...			Verify and control/limit connections to and use of external syst...	A.11.2.6; A.13.1.1; A.13.2.1; AC-20(1)	A.11.2.6 Security of e...	AC-20; A.11.2; A.13.1; A.13.2	AC-20 Use of External Systems; A.11.2 Equipment...	CONNECTION AGREEMENT; PROCESSING AGREEMENT; LIMITS; SECURITY ASSESSMENT; EXTERNAL S
N171_3.1.21 Limit use of orga...	N171_3.1	NIST 800-171 r2	NIST800-53...	This isn't addressed in IS...		Limit use of portable storage devices on external systems. DISC...	A.12.3.1; AC-20(2); AC-20(5)	A.12.3.1 Information ...	AC-20	AC-20 Use of External Systems	PORTABLE STORAGE DEVICES, RESTRICT; PROHIBIT; Portable Storage Devices — Prohibited Use
N171_3.1.22 Control informat...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add PL-4(1); PM-20(1		Control CUI posted or processed on publicly accessible system...	PL-4(1); PM-20(1)	PL-4.1 Social Media a...	AC-22; PL-4; PM-20	AC-22 Publicly Accessible Content; PL-4 Rules ...	...NETWORK RESTRICTIONS; PUBLIC WEBSITE; Dissemination of Privacy Program Inform
N171_3.2.1 Ensure that mana...	N171_3.2	NIST 800-171 r2	NIST800-53...	Add A.7.2.2; A.12.2.1; AT-...		AWARENESS AND TRAINING Basic Security Requirements Ensu...	A.7.2.2; A.12.2.1; AT-2(1); AT-2(2); AT-2(3)...	A.7.2.2 Information s...	AT-2; A.7.2; A.12.2	AT-2 SECURITY AWARENESS TRAINING; A.7.2 Dur...	PHISHING; MALICIOUS LINKS; PRACTICAL EXERCISES; PRIVACY; INSIDER THREAT; INDICATORS; INAPP

3rd level

Source Document

Update Mappings

New Attribute

R5 draft list of attribute keywords

Polling Question #4

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

CSF Tools Depends upon Framework Updates

FRAMEWORKS AND CONTROLS

NIST Cybersecurity Framework

- CSF Version 1.1 [Summary]

NIST Special Publication 800-53

- NIST SP 800-53, Revision 4 [Summary]
- NIST SP 800-53, Revision 5 [Summary]

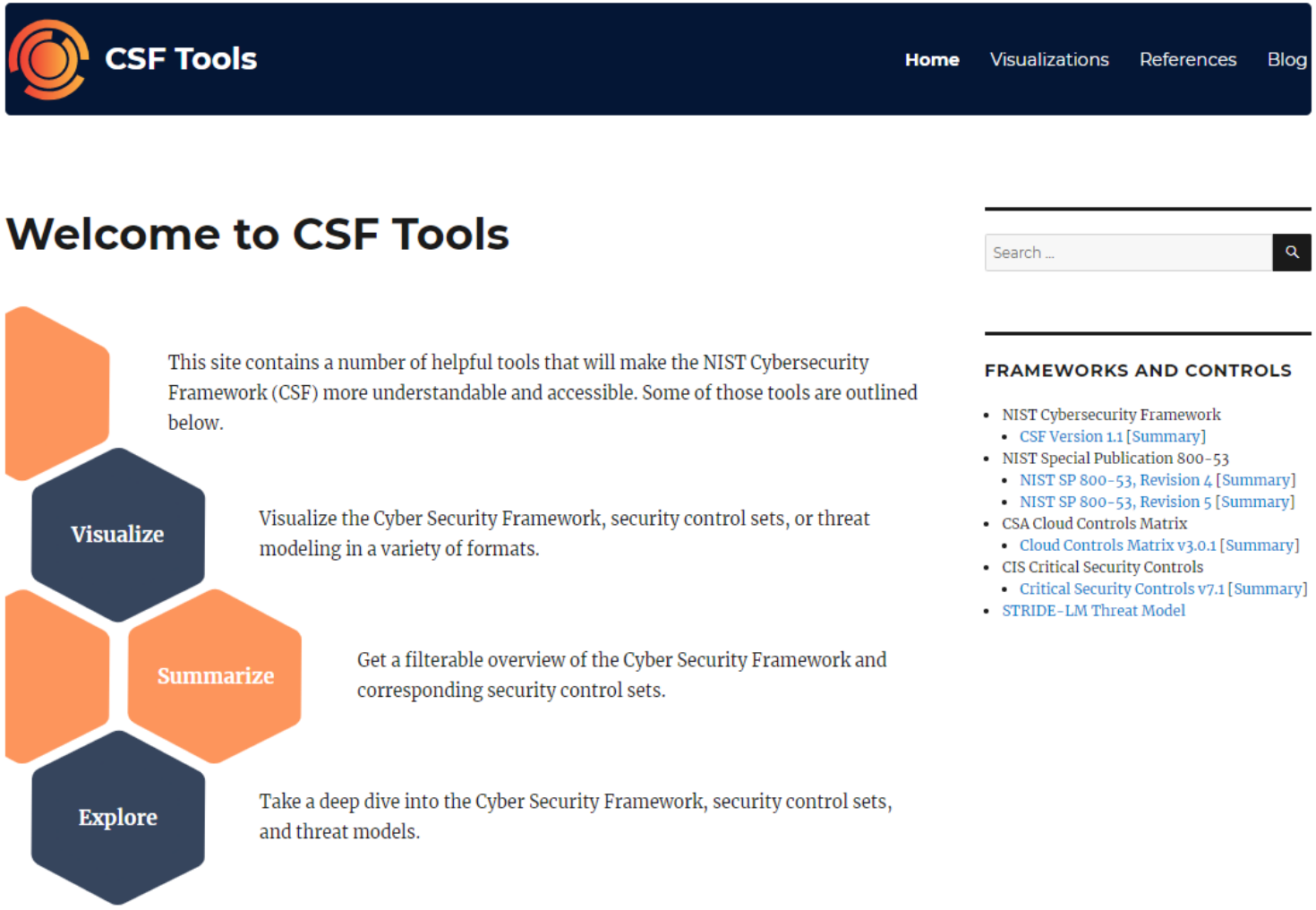
CSA Cloud Controls Matrix

- Cloud Controls Matrix v3.0.1 [Summary] (Update to CCM 4 in process)

CIS Critical Security Controls

- Critical Security Controls v7.1 [Summary] (Update to CSC 8.1 in process)

STRIDE-LM Threat Model



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

NIST Cyber Security Framework CSF

Control Enhancements

RA-5(2): Update Vulnerabilities to Be Scanned
BASELINE(S): Low Moderate High
Update the system vulnerabilities to be scanned [Assignment (one or more): [Assignment: organization-defined frequency] , prior to a new scan, when new vulnerabilities are identified and reported].

RA-5(3): Breadth and Depth of Coverage
BASELINE(S): (Not part of any baseline)
Define the breadth and depth of vulnerability scanning coverage.

RA-5(4): Discoverable Information
BASELINE(S): High
Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].

RA-5(5): Privileged Access
BASELINE(S): Moderate High
Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].

RA-5(6): Automated Trend Analyses
BASELINE(S): (Not part of any baseline)
Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].

RA-5(8): Review Historic Audit Logs
BASELINE(S): (Not part of any baseline)
Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

RA-5(10): Correlate Scanning Information
BASELINE(S): (Not part of any baseline)
Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

RA-5(11): Public Disclosure Program
BASELINE(S): Low Moderate High
Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

EnterpriseGRC Solutions, Inc.

RA-5: Vulnerability Monitoring and Scanning

Control Family: Risk Assessment

CSF Relationships:
ID.RA-1: Asset vulnerabilities are identified and documented
PR.IP-12: A vulnerability management plan is developed and implemented
DE.AE-2: Detected events are analyzed to understand attack targets...
DE.CM-8: Vulnerability scans are performed
DE.DP-4: Event detection information is communicated
DE.DP-5: Detection processes are continuously improved
RS.AN-1: Notifications from detection systems are investigated
RS.MI-3: Newly identified vulnerabilities are mitigated or documented...

Baselines:

Low	RA-5 (2) (11)
Moderate	RA-5 (2) (5) (11)
High	RA-5 (2) (4) (5) (11)
Privacy	N/A

Previous Version: NIST Special Publication 800-53 Revision 4 (RA-5)

Incorporates the following control from the previous version: RA-5 (1): Update Tool Capability.

Control

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

STRIDE – CSF Tool Depends Upon Updates to NIST SP 800-53 Rev 5, CSA CCM 4.0, CIS CSC 8.1

NIST Special Publication 800-53 Revision 5

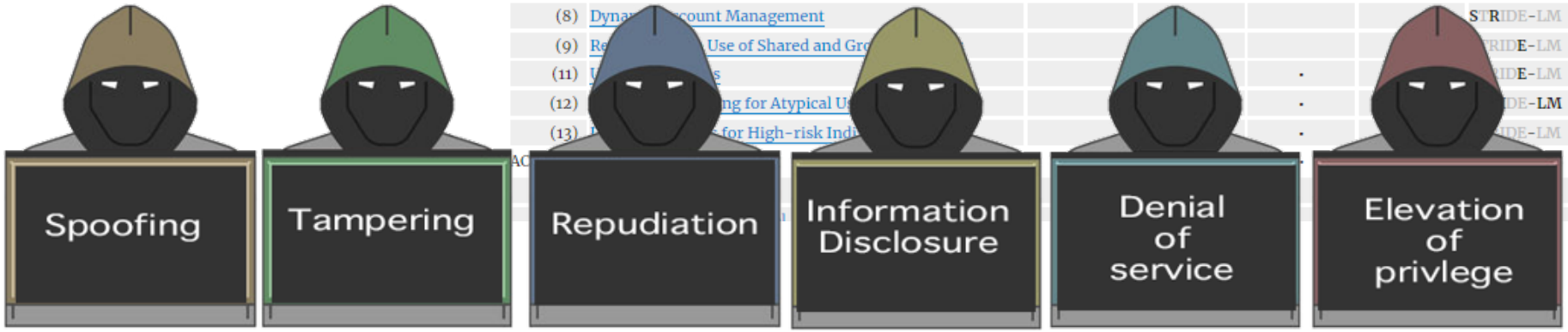
This page contains an overview of the controls provided by NIST to protect organization personnel and assets. NIST includes baselines for various security levels. The "Low" security level is applicable to all assets.

Filter Controls

Name contains: ☐ Include control lanuage in search

Family: (any) Baseline: (any) Threat: (any) APPLY CLEAR

ID	Name	Low	Moderate	High	Privacy	Threats
AC-1	Policy and Procedures	·	·	·	·	STRIDE-LM
AC-2	Account Management	·	·	·		STRIDE-LM
(1)	Automated System Account Management		·	·		STRIDE-LM
(2)	Automated Temporary and Emergency Account Management		·	·		STRIDE-LM
(3)	Disable Accounts		·	·		STRIDE-LM
(4)	Automated Audit Actions		·	·		STRIDE-LM
(5)	Inactivity Logout		·	·		STRIDE-LM
(6)	Dynamic Privilege Management					STRIDE-LM
(7)	Privileged User Accounts					STRIDE-LM
(8)	Dyna… …count Management					STRIDE-LM
(9)	Re… …Use of Shared and Gr…					…RIDE-LM
(11)	U… …s			·		…IDE-LM
(12)	…ng for Atypical U…			·		…DE-LM
(13)	…for High-risk Indi…			·		…IDE-LM



Search …

FRAMEWORKS AND CONTROLS

- NIST Cybersecurity Framework
  - CSF Version 1.1 [Summary]
- NIST Special Publication 800-53
  - NIST SP 800-53, Revision 4 [Summary]
  - NIST SP 800-53, Revision 5 [Summary]
- CSA Cloud Controls Matrix
  - Cloud Controls Matrix v3.0.1 [Summary]
- CIS Critical Security Controls
  - Critical Security Controls v7.1 [Summary]
- STRIDE-LM Threat Model

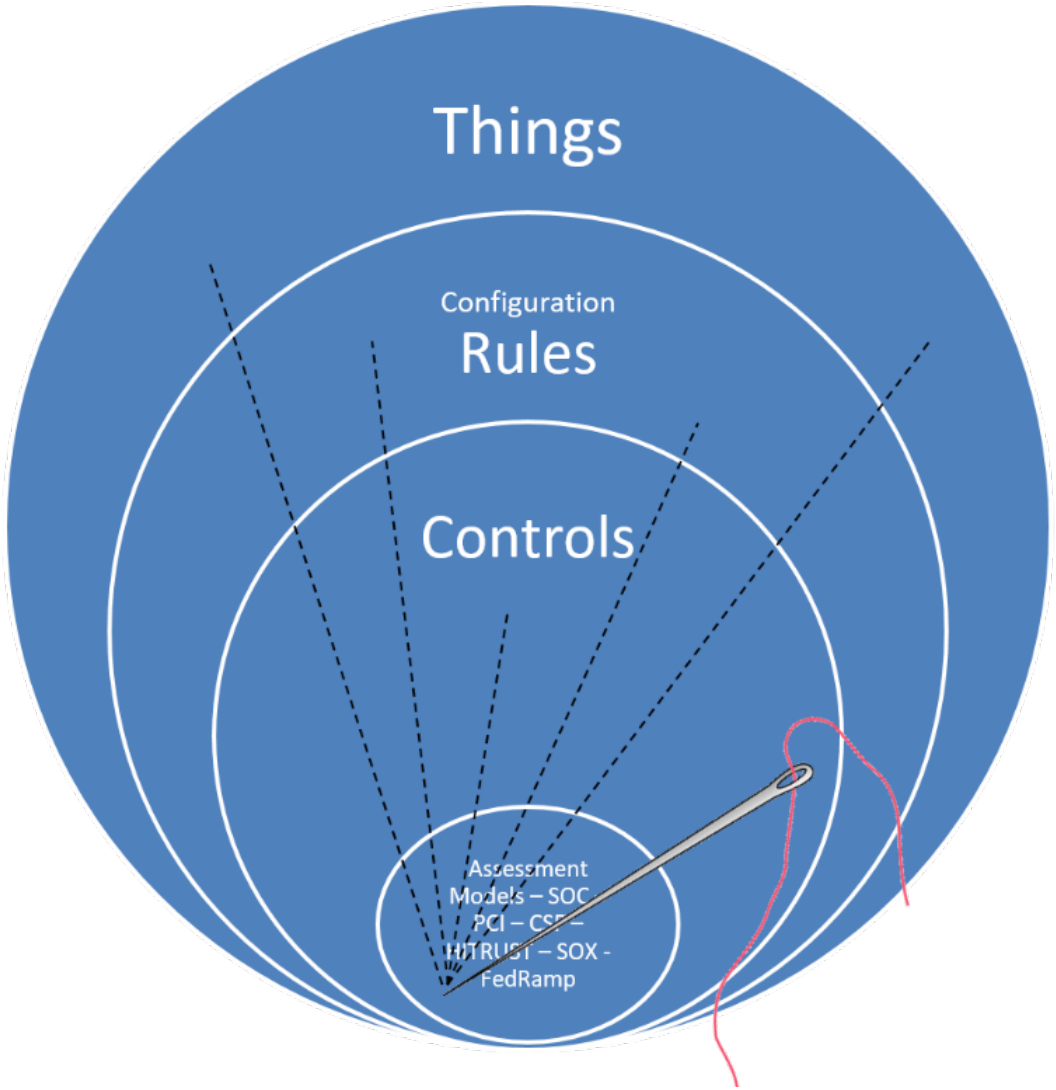
©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

What's so hard about mapping?

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

How to map

- Have a workplan
- Identify what sources and domains should map – line up the full schema
- Iterate
- Finalize
- Negative Map (what should have but didn't)
- Map the Missing
- QA
- Communicate back to content owners



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

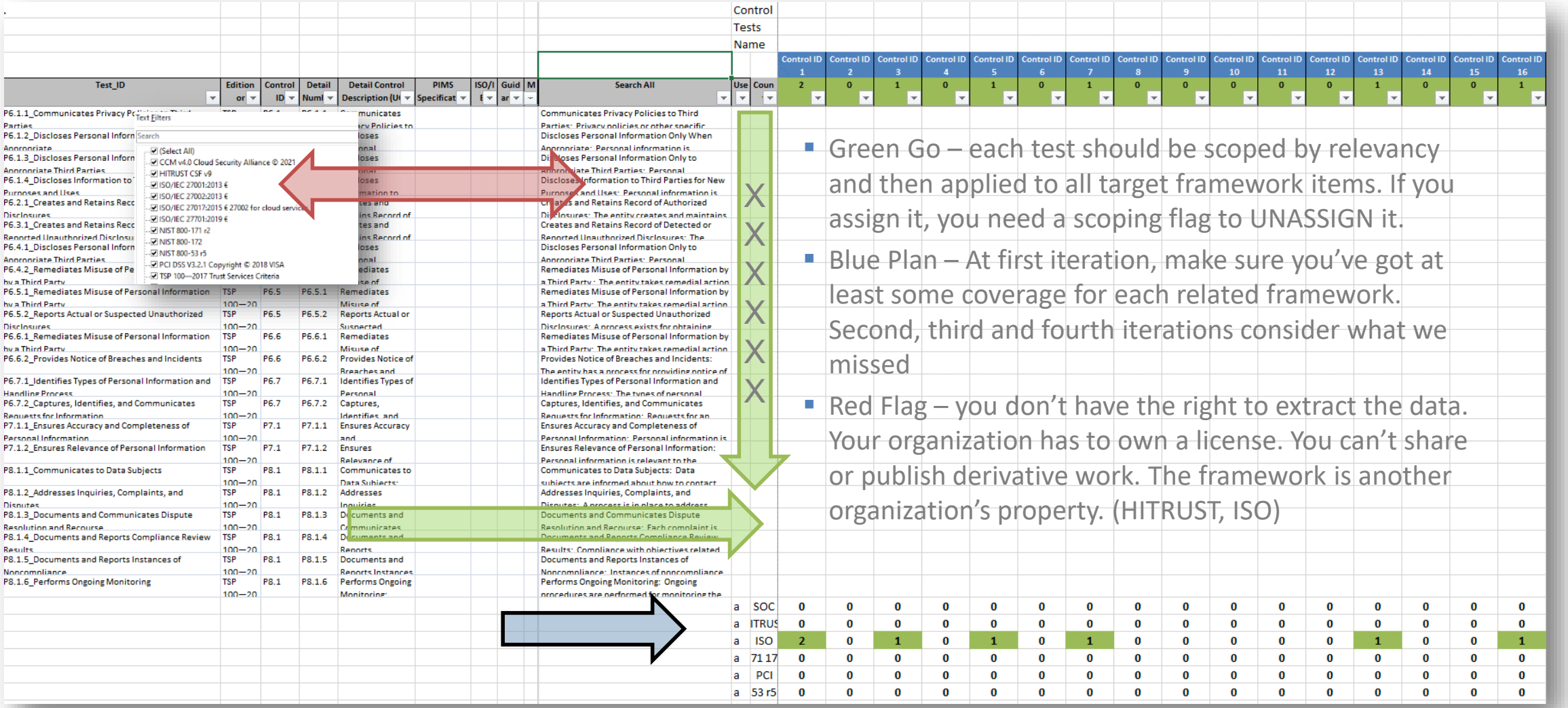
For Each Control Statement gather keywords, concepts and suitable common domains

- Search for list of testable items based on keywords and common terms, including global spelling. Consider more than “does it” by asking if the implied understanding of the control is that it “should”.
- Prepare a list of probable matches – likely 1-2% of total population.
- Consider overuse and reduce the number of times we use same items
- Consider that the client may use multiple controls to accomplish a same objective. This exercise may result in client customization to their written policies and program objectives.

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Mapping Plan –> Records need sufficient legal rights to put into a searchable system.

EnterpriseGRC Solutions, Inc.



- Green Go – each test should be scoped by relevancy and then applied to all target framework items. If you assign it, you need a scoping flag to UNASSIGN it.
- Blue Plan – At first iteration, make sure you've got at least some coverage for each related framework. Second, third and fourth iterations consider what we missed
- Red Flag – you don't have the right to extract the data. Your organization has to own a license. You can't share or publish derivative work. The framework is another organization's property. (HITRUST, ISO)

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

ISACA San Francisco Chapter · ISO Silicon Valley

Encryption – Let's discuss –Transition to CCM 4.2 ASAP

EnterpriseGRC Solutions, Inc.

Edition or Source	main ID	trol ID	Client ID	Control Objective	Control Objective Description	R u r p	List of pol icy	CSA Test language - pre adoption/ CSA edits open	Unified Testing Map	Unified Testing Map:Test_ID (to review the details of each mapped item see the All Mapping Tab)	ified Universe
CCM v4.0 Cloc	CCM_	CEK-	CEK-01 Encryption and Key Management Policy	Encryption and Key Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and			CCM_CEK-1.1 A re cryptography , encryption and key management	A.10.1.1, A.10.1.2, A.13.2.1, A.13.2.2, A.18.1.3, A.18.1.5,	C.5.2 Policy; C.8.3 Information security risk treatment; A.10.1 Cryptographic controls; A.13.2 Information transfer; A.18.1 Compliance with legal and contractual requirements; ISO27701_6.5 Asset	A.13.2; A.18.1; ISO27701_6.5;
CCM v4.0 Cloud	CCM_	CEK-	CEK-02 CEK Roles and Responsibilities	CEK Roles and Responsibilities	Define and implement cryptographic, encryption and key management roles			CCM_CEK-2.1 Are cryptography , encryption and key management roles	A.8.2.1, A.9.2.3, A.10.1.1, A.10.1.2, A.13.1.3, A.13.2.1, A.18.1.3,	A.8.2 Information classification; A.9.2 User access management; A.10.1 Cryptographic controls; A.13.1 Network security management; A.13.2 Information transfer; A.18.1 Compliance with legal and	A.13.1; A.13.2; A.18.1; CLD.6.3
CCM v4.0 Cloud	CCM_	CEK-	CEK-03 Data Encryption	Data Encryption	Provide cryptographic protection to data-at-rest and in-transit, using			CCM_CEK-3.1 Are data at-rest and in-transit cryptographically protected using	A.6.2.1, A.8.3.1, A.10.1.1, A.10.1.2, A.13.2.1, A.14.1.2, A.14.1.3,	A.6.2 Mobile devices and teleworking; A.8.3 Media handling; A.10.1 Cryptographic controls; A.13.2 Information transfer; A.14.1 Security requirements of information systems; A.18.1 Compliance with	A.13.2; A.14.1; A.18.1; AC-19;
CCM v4.0 Cloud	CCM_	CEK-	CEK-04 Encryption Algorithm	Encryption Algorithm	Use encryption algorithms that are appropriate for data protection,			CCM_CEK-4.1 Are appropriate encryption algorithms used for data protection,	A.8.2.1, A.8.3.3, A.10.1.1, A.10.1.2, A.14.1.2, A.14.1.3, A.18.1.3,	A.8.2 Information classification; A.8.3 Media handling; A.10.1 Cryptographic controls; A.14.1 Security requirements of information systems; A.18.1 Compliance with legal and contractual requirements; SA-	A.14.1; A.18.1; SC-12; SC-28;
CCM v4.0 Cloud	CCM_	CEK-	CEK-05 Encryption Change Management	Encryption Change Management	Establish a standard change management procedure, to			CCM_CEK-5.1 Are standard change management procedures established to	A.8.2.1, A.10.1.2, A.12.1.2, A.14.2.2, A.18.1.3, ISO27701_6.7.1,	A.8.2 Information classification; A.10.1 Cryptographic controls; A.12.1 Operational procedures and responsibilities; A.14.2 Security in development and support processes; A.18.1 Compliance with legal	A.14.2; A.18.1; ISO27701_6.11
CCM v4.0 Cloud	CCM_	CEK-	CEK-06 Encryption Change Cost Benefit Analysis	Encryption Change Cost Benefit Analysis	Manage and adopt changes to cryptography-, encryption-, and key			CCM_CEK-6.1 Are changes to cryptography-, encryption- and key management-	A.8.2.1, A.10.1.2, A.12.1.2, A.14.2.2, A.18.1.3, ISO27701_6.7.1,	C.6.1 Actions to address risks & opportunities; A.6.1 Internal organization; A.10.1 Cryptographic controls; A.12.1 Operational procedures and responsibilities; A.13.2 Information transfer; A.14.2	A.12.1; A.13.2; A.14.2; HT_09.
CCM v4.0 Cloud	CCM_	CEK-	CEK-07 Encryption Risk Management	Encryption Risk Management	Establish and maintain an encryption and key management risk program that			CCM_CEK-7.1 Is a cryptographic, encryption and key management risk	A.6.1.5, A.10.1.1, A.10.1.2, A.18.1.3, ISO27701_6.7.1, ISO27701_6.11.1,	A.6.1 Internal organization; A.10.1 Cryptographic controls; A.18.1 Compliance with legal and contractual requirements; ISO27701_6.7 Cryptography; CM-3 Configuration Change Control; SA-9	ISO27701_6.7; 3; SA-9; SC-8; S
CCM v4.0 Cloud	CCM_	CEK-	CEK-08 CSC Key Management Capability	CSC Key Management Capability	CSPs must provide the capability for CSCs to manage their own data			CCM_CEK-8.1 Are CSC's provided the capability to manage their own data	A.10.1.2, A.15.1.2, A.15.1.3, CLD.6.3.1, CLD.12.1.5, CA-6(2), CP-	A.10.1 Cryptographic controls; A.15.1 Information security in supplier relationships; CLD.6.3 Relationship between cloud service customer and cloud service provider; CLD.12.1 Operational	CLD.6.3; CLD.1 CCPA2018-T12-
CCM v4.0 Cloud	CCM_	CEK-	CEK-09 Encryption and Key Management Audit	Encryption and Key Management Audit	Audit encryption and key management systems, policies, and processes with a			CCM_CEK-9.1 Are encryption and key management systems, policies, and	CCPA12.1.4 1798.140(d), 2.3.0 BMSN, 3.6.5 PCD, 3.6.6 PCD,	A.10.1 Cryptographic controls; A.12.7 Information systems audit considerations; A.18.2 Information security reviews; C.9.2 Internal audit; ISO27701_6.7 Cryptography; N171_3.14 System and Information	A.18.2; C.9.2; ISO27701_6.7;
CCM v4.0 Cloud	CCM_	CEK-	CEK-10 Key Generation	Key Generation	Generate cryptographic keys using industry-accepted cryptographic			CCM_CEK-10.1 Are cryptographic keys being generated using industry	A.10.1.1, A.10.1.2, A.18.1.5, HT_6.d, 3.6.1 PCD, 3.6.6 PCD, N171_3.13.11,	A.10.1 Cryptographic controls; A.18.1 Compliance with legal and contractual requirements; SA-10 Developer Configuration Management; SC-12 Cryptographic Key Establishment and Management; SC-	10; SC-12; SC-2 7; N171_3.14;
CCM v4.0 Cloud	CCM_	CEK-	CEK-11 Key Purpose	Key Purpose	Manage cryptographic secret and private keys that are provisioned for a			CCM_CEK-11.1 Are cryptographic secret and private keys that are provisioned for	A.9.2.4, A.9.3.1, A.10.1.1, A.10.1.2, A.14.1.3, HT_10.g, 3.5.2 PCD, 3.6.7	A.9.2 User access management; A.10.1 Cryptographic controls; 10.03 Cryptographic Controls; 3_PCD Protect Stored Data; IA-5 Authenticator Management; SC-12 Cryptographic Key Establishment and	HT_10.03; 3_P 5; SC-12; CC6.1
CCM v4.0 Cloud	CCM_	CEK-	CEK-12 Key Rotation	Key Rotation	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which			CCM_CEK-12.1 Are cryptographic keys rotated based on a cryptoperiod	A.10.1.1, A.10.1.2, A.12.4.1, ISO27701_6.7.1, N172_3.5.2e,	A.10.1 Cryptographic controls; A.12.4 Logging and monitoring; ISO27701_6.7 Cryptography; N171_3.5 Identification and Authentication; 6_MVMP Develop and Maintain Secure Systems and Applications.;	ISO27701_6.7; N171_3.5; 6_M
CCM v4.0 Cloud	CCM_	CEK-	CEK-13 Key Revocation	Key Revocation	Define, implement and evaluate processes, procedures and technical			CCM_CEK-13.1 Are cryptographic keys revoked and removed prior to the end of	11.300(b), A.10.1.1, A.10.1.2, A.11.2.7, A.12.1.2, A.15.1.3,	Sec. 11.300 Controls for identification codes/passwords; A.10.1 Cryptographic controls; A.11.2 Equipment; A.12.1 Operational procedures and responsibilities; A.15.1 Information security in	A.10.1; A.11.2; A.12.1; A.15.1;
CCM v4.0 Cloud	CCM_	CEK-	CEK-14 Key Destruction	Key Destruction	Define, implement and evaluate processes, procedures, and technical			CCM_CEK-14.1 Are Processes, procedures and technical measures to destroy keys	A.8.1.2, A.10.1.2, A.11.2.7, A.18.1.3, CLD.12.1.5, HT_10.g, 3.6.5 PCD,	A.8.1 Responsibility for assets; A.10.1 Cryptographic controls; A.11.2 Equipment; A.18.1 Compliance with legal and contractual requirements; CLD.12.1 Operational procedures and responsibilities; 10.03	A.18.1; CLD.12. HT_10.03; 3_P
CCM v4.0 Cloud	CCM_	CEK-	CEK-15 Key Activation	Key Activation	Define, implement and evaluate processes, procedures, and technical			CCM_CEK-15.1 Are Processes, procedures and technical measures to create keys	A.10.1.2, A.14.1.2, A.18.1.5, CLD.12.1.5, AC-3(8), IA-5(2), SA-	A.10.1 Cryptographic controls; A.12.1 Operational procedures and responsibilities; A.14.1 Security requirements of information systems; A.18.1 Compliance with legal and contractual requirements;	A.14.1; A.18.1; CLD.12.1; HT_1
CCM v4.0 Cloud	CCM_	CEK-	CEK-16 Key Suspension	Key Suspension	Define, implement and evaluate processes, procedures, and technical			CCM_CEK-16.1 Are Processes, procedures and technical measures to monitor,	A.10.1.1, A.10.1.2, A.14.1.2, CM-3(6), MP-6(1), HT_6.d, HT_6.g,	A.10.1 Cryptographic controls; A.14.1 Security requirements of information systems; CM-3 Configuration Change Control; MP-6 Media Sanitization; 06.01 Compliance with Legal Requirements; 09.06 Network	MP-6; HT_06.0 HT_09.06;
CCM v4.0 Cloud	CCM_	CEK-	CEK-17 Key Deactivation	Key Deactivation	Define, implement and evaluate processes, procedures and technical			CCM_CEK-17.1 Are Processes, procedures and technical measures to deactivate	A.10.1.1, A.10.1.2, A.12.1.1, A.14.1.2, A.18.1.5, AC-3(8), IA-5(2),	A.10.1 Cryptographic controls; A.12.1 Operational procedures and responsibilities; A.14.1 Security requirements of information systems; A.18.1 Compliance with legal and contractual requirements;	A.14.1; A.18.1; HT_10.03; 3_P
CCM v4.0 Cloud	CCM_	CEK-	CEK-18 Key Archival	Key Archival	Define, implement and evaluate processes, procedures, and technical			CCM_CEK-18.1 Are Processes, procedures and technical measures to manage	A.10.1.2, A.13.2.2, A.14.2.7, A.18.1.3, SA-15(11), SC-12(1),	A.10.1 Cryptographic controls; A.13.2 Information transfer; A.14.2 Security in development and support processes; A.18.1 Compliance with legal and contractual requirements; SA-15 Development Process,	A.14.2; A.18.1; 15; SC-12; HT_
CCM v4.0 Cloud	CCM_	CEK-	CEK-19 Key Compromise	Key Compromise	Define, implement and evaluate processes, procedures, and technical			CCM_CEK-19.1 Are Processes, procedures and technical measures to encrypt	A.10.1.2, A.11.2.7, A.18.1.3, ISO27701_6.5.3, SC-12(1), HT_10.g,	A.8.3 Media handling; A.10.1 Cryptographic controls; A.11.2 Equipment; A.18.1 Compliance with legal and contractual requirements; ISO27701_6.5 Asset management; SC-12 Cryptographic Key	A.18.1; ISO27701_6.5;
CCM v4.0 Cloud	CCM_	CEK-	CEK-20 Key Recovery	Key Recovery	Define, implement and evaluate processes, procedures and technical			CCM_CEK-20.1 Are Processes, procedures and technical measures to assess the	A.10.1.2, A.18.1.3, SA-9(6), SC-12(1), SC-12(3), SC-28(1), SI-7(6), HT_6.d,	A.10.1 Cryptographic controls; A.18.1 Compliance with legal and contractual requirements; SA-9 External System Services; SC-12 Cryptographic Key Establishment and Management; SC-28 Protection of	SC-12; SC-28; S CCPA2018-T14-
CCM v4.0 Cloud	CCM_	CEK-	CEK-21 Key Inventory Management	Key Inventory Management	Define, implement and evaluate processes, procedures and technical			CCM_CEK-21.1 Are Processes, procedures and technical measures being defined,	A.10.1.2, A.18.1.3, SA-9(6), SC-12(1), SC-12(3), SC-23(5), SC-28(1), SI-	A.10.1 Cryptographic controls; A.18.1 Compliance with legal and contractual requirements; SA-9 External System Services; SC-12 Cryptographic Key Establishment and Management; SC-28 Protection of	SC-12; SC-28; S CCPA2018-T14-

Robin Basham (robin@enterprisegrc.com) is signed

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

ISACA San Francisco Chapter | ISC² Silicon Valley | ISC² Chapter

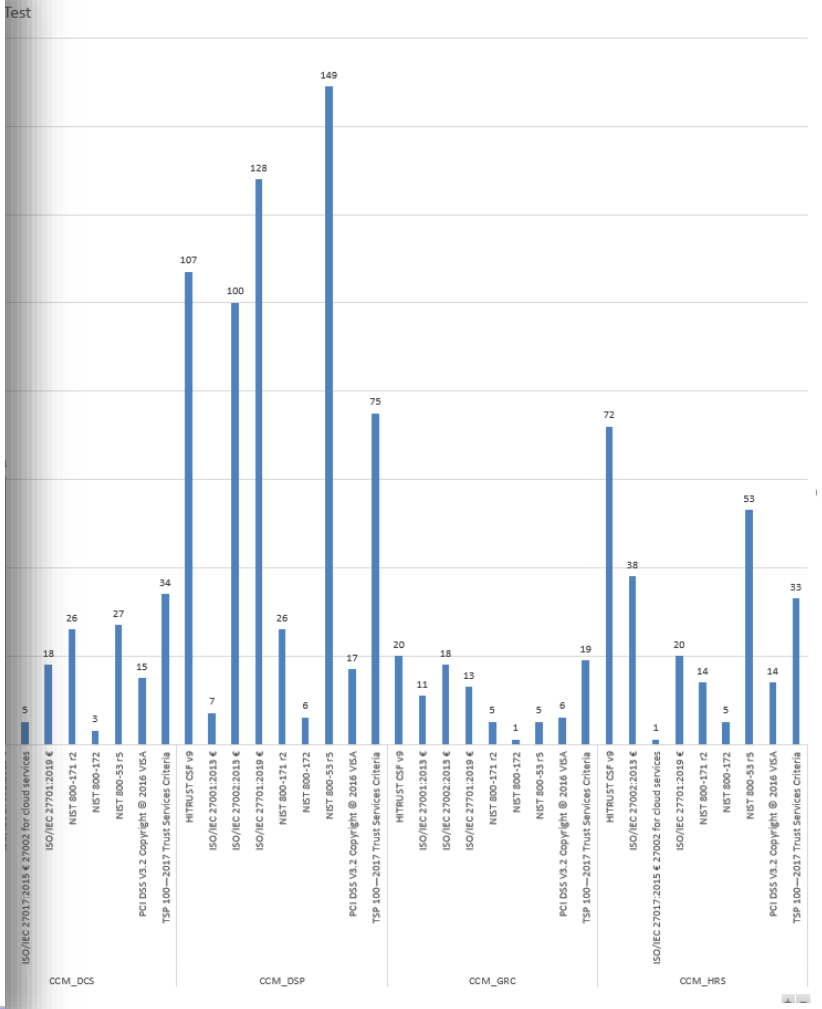
Correctly Formatted Mappings Accessible/ Usable

EnterpriseGRC Solutions, Inc.

Row Labels	Count of Detail Number
CCM_A&A	174
HITRUST CSF v9	
ISO/IEC 27001:2013 €	
ISO/IEC 27002:2013 €	
ISO/IEC 27701:2019 €	
NIST 800-171 r2	
NIST 800-53 r5	
PCI DSS V3.2 Copyright © 2016 VISA	
TSP 100—2017 Trust Services Criteria	
CCM_AIS	
HITRUST CSF v9	
ISO/IEC 27001:2013 €	
ISO/IEC 27002:2013 €	
ISO/IEC 27017:2015 € 27002 for cloud services	
ISO/IEC 27701:2019 €	
NIST 800-171 r2	
NIST 800-172	
NIST 800-53 r5	
PCI DSS V3.2 Copyright © 2016 VISA	
TSP 100—2017 Trust Services Criteria	
CCM_BCR	
HITRUST CSF v9	
ISO/IEC 27001:2013 €	
ISO/IEC 27002:2013 €	
ISO/IEC 27017:2015 € 27002 for cloud services	
ISO/IEC 27701:2019 €	
NIST 800-171 r2	
NIST 800-172	
NIST 800-53 r5	
PCI DSS V3.2 Copyright © 2016 VISA	
TSP 100—2017 Trust Services Criteria	
CCM_CCC	
HITRUST CSF v9	
ISO/IEC 27001:2013 €	
ISO/IEC 27002:2013 €	
ISO/IEC 27701:2019 €	
NIST 800-171 r2	
NIST 800-172	
NIST 800-53 r5	
PCI DSS V3.2 Copyright © 2016 VISA	
TSP 100—2017 Trust Services Criteria	
CCM_CEK	
California Consumer Privacy Act of 2018	
HIPAA - HITECH Title 45 C.F.R. § 164	
HITRUST CSF v9	
ISO/IEC 27002:2013 €	
ISO/IEC 27017:2015 € 27002 for cloud services	
ISO/IEC 27701:2019 €	
NIST 800-171 r2	
NIST 800-172	
NIST 800-53 r5	
PCI DSS V3.2 Copyright © 2016 VISA	
Title 21 CFR Part 11	
TSP 100—2017 Trust Services Criteria	

Row Labels	Count of Detail Number
CCM_CEK	
California Consumer Privacy Act of 2018	
HIPAA - HITECH Title 45 C.F.R. § 164	
HITRUST CSF v9	
ISO/IEC 27002:2013 €	
CEK-01	
CEK-02	
CEK-03	
Data Encryption	
A.10.1.1 Policy on the use of cryptographic controls	
A.10.1.2 Key management	
A.13.2.1 Information transfer policies and procedures	
A.14.1.2 Securing application services on public networks	
A.14.1.3 Protecting application services transactions	
A.18.1.1 Identification of applicable legislation and contractual requirements	
A.18.1.2 Intellectual property rights	
A.18.1.3 Protection of records	
A.18.1.4 Privacy and protection of personally identifiable information	
A.18.1.5 Regulation of cryptographic controls	
A.6.2.1 Mobile device policy	
A.8.3.1 Management of removable media	
CEK-04	
CEK-05	
CEK-06	
CEK-07	
CEK-08	
CEK-09	
Encryption and Key Management Audit	
A.10.1.2 Key management	
A.12.7.1 Information systems audit controls	
A.18.2.1 Independent review of information security	
A.18.2.2 Compliance with security policies and standards	
CEK-10	
CEK-11	
CEK-12	
CEK-13	
Key Revocation	
A.10.1.1 Policy on the use of cryptographic controls	
A.10.1.2 Key management	
A.11.2.7 Secure disposal or re-use of equipment	
A.12.1.2 Change management	
A.15.1.3 Information and communication technology supply chain	
CEK-14	
CEK-15	
CEK-16	
Key Suspension	
A.10.1.1 Policy on the use of cryptographic controls	
A.10.1.2 Key management	
A.14.1.2 Securing application services on public networks	
CEK-17	
CEK-18	
CEK-19	
CEK-20	
CEK-21	
ISO/IEC 27017:2015 € 27002 for cloud services	
ISO/IEC 27701:2019 €	
NIST 800-171 r2	
NIST 800-172	
NIST 800-53 r5	
PCI DSS V3.2 Copyright © 2016 VISA	
Title 21 CFR Part 11	
TSP 100—2017 Trust Services Criteria	44
Grand Total	326

- Data Encryption
  - HIPAA - HITECH Title 45 C.F.R. § 164
    - **Access Control: § 164.312(a)(2)(iv)**
  - HITRUST CSF v9
    - **06.01 Compliance with Legal Requirements**
    - **09.08 Exchange of Information**
    - **09.09 Electronic Commerce Services**
  - ISO/IEC 27002:2013 €
    - **A.10.1 Cryptographic controls**
    - **A.13.2 Information transfer**
    - **A.14.1 Security requirements of information systems**
    - **A.18.1 Compliance with legal and contractual requirements**
    - **A.6.2 Mobile devices and teleworking**
    - **A.8.3 Media handling**
  - ISO/IEC 27018:2019 €
    - **ISO/IEC 27018:2019(E) A.11.13 Access to data on pre-used data storage space**
  - ISO/IEC 27701:2019 €
    - **ISO27701_6.5 Asset management**
    - **ISO27701_6.7 Cryptography**
  - NIST 800-171 r2
    - **N171_3.13 System and Communications Protection**
  - NIST 800-53 r5
    - **AC-19 Access Control for Mobile Devices**
    - **SC-12 Cryptographic Key Establishment and Management**
    - **SC-28 Protection of Information at Rest**
    - **SI-4 System Monitoring**
    - **SI-7 Software, Firmware, and Information Integrity**
  - TSP 100—2017 Trust Services Criteria
    - **CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal ar**
- Encryption Algorithm
  - California Consumer Privacy Act of 2018
    - **14.01 1798.150 (a) Content**
  - HITRUST CSF v9
    - **06.01 Compliance with Legal Requirements**
    - **10.02 Correct Processing in Applications**
    - **10.03 Cryptographic Controls**
  - ISO/IEC 27002:2013 €
    - **A.10.1 Cryptographic controls**
    - **A.14.1 Security requirements of information systems**
    - **A.18.1 Compliance with legal and contractual requirements**
    - **A.8.2 Information classification**
    - **A.8.3 Media handling**
  - ISO/IEC 27701:2019 €
    - **ISO27701_6.5 Asset management**
    - **ISO27701_6.7 Cryptography**
  - NIST 800-171 r2
    - **N171_3.14 System and Information Integrity**
  - NIST 800-53 r5



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

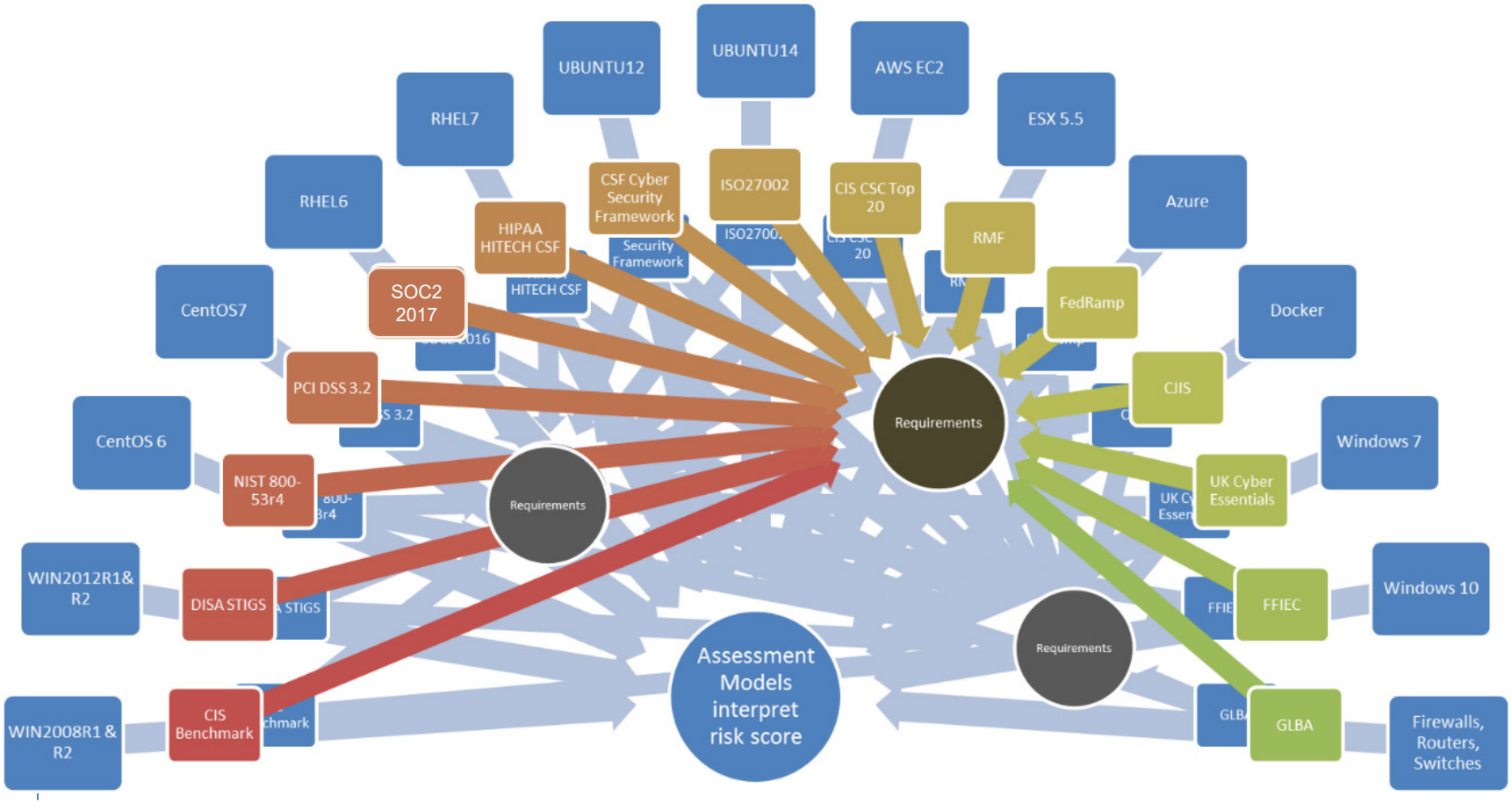
ISACA San Francisco Chapter · Silicon Valley

Are Risks Top Down or Bottom Up?

- CIS Benchmark, OWASP, MITRE ATT&CK® controls mapped according to the distinct environments used to deliver a service: should map to NIST 800-53r5 and ISO27002 which are then associated to your Cloud Environment.
- NIST 800-53r5 and ISO27002 should be tagged to each continuously monitored configuration.
- Control mapping involves how the requirement is implemented in policy, practice, contract, ***configuration or architecture***. The map may point to a policy, for example, where this detail needs explicit statement. This could map to a CIS, OWASP benchmark that is specific to an OS or PaaS/IaaS.

EnterpriseGRC Solutions, Inc.

Rules run on Environments –> are tagged to controls –> are interpreted by assessment models

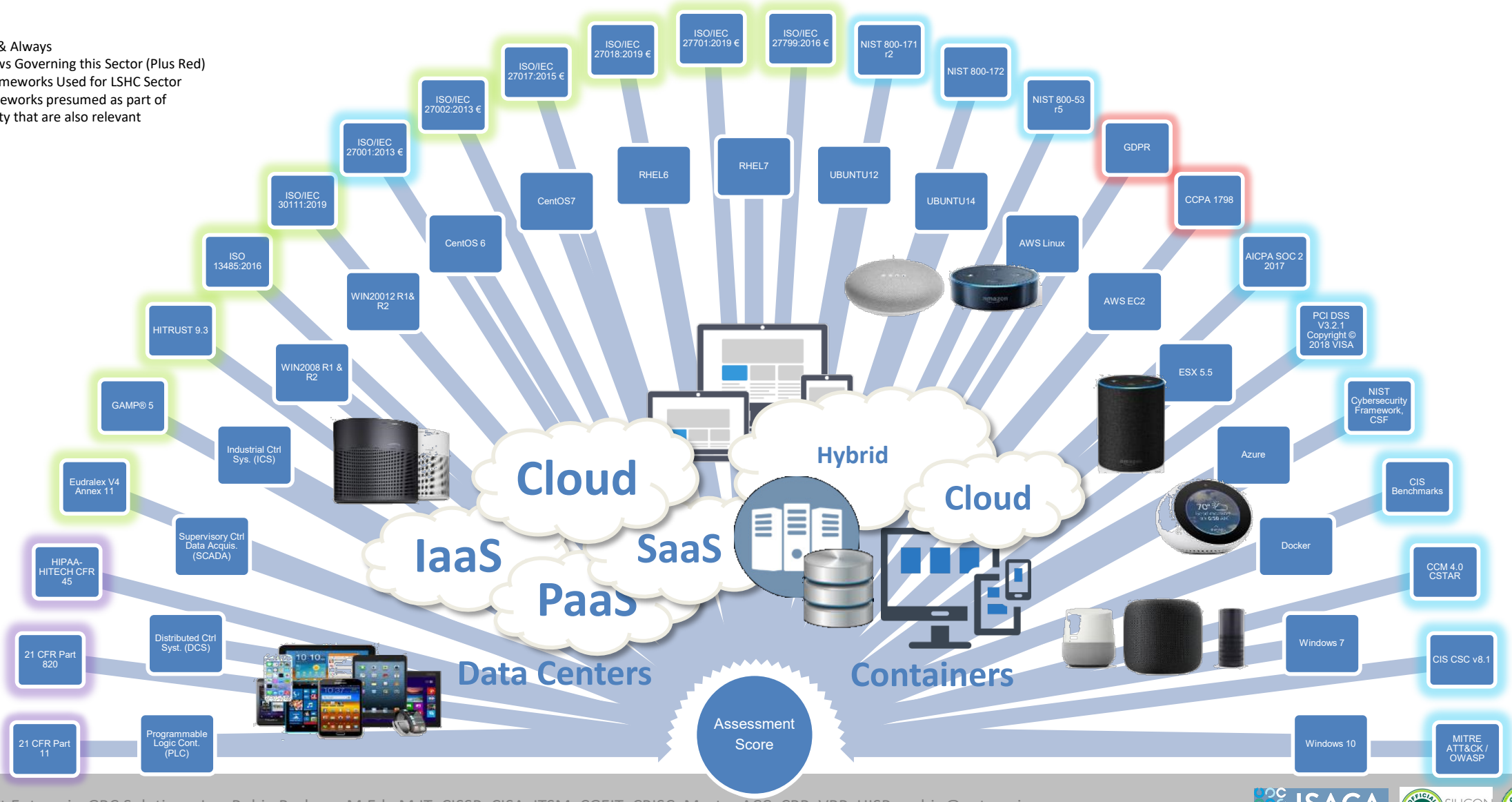


©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Imagine Regulating Federal E-Commerce Cloud Based Medical Service

EnterpriseGRC Solutions, Inc.

Red = Now & Always
Purple = Laws Governing this Sector (Plus Red)
Green = Frameworks Used for LSHC Sector
Blue = Frameworks presumed as part of Cybersecurity that are also relevant



©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

ISACA San Francisco Chapter | Silicon Valley

Mappers benefit by mapping technical controls to frameworks, frameworks to client domains, configurations to policy

EnterpriseGRC Solutions, Inc.

ment Testing ☆ > Cryptography

Test_ID	Mapped testi...	Mapped testing or practices:Test_ID	Mapped testing or practices:Problem Metadata	Risk Drivers	Detail Control Description (UCF)	Proble...	Mapped Proce...	Mapped Process
T1468_Encrypt sensitive data at rest in the browser	A.18.1.3; AC-16(5); AC-19(4); AU-13(3); SA-4(5); SA-8(20); SA-9(6); SC-12(3); SC-28(1); SC-28(2); SC-28(3); SI-12(2); SA-15(12); SI-19(3)	A.18.1.3 Protection of records; AC-16.5 Attribute Displays on Objects to Be Output; AC-19.4 Restrictions for Classified Information; AU-13.3 Unauthorized Replication of Information; SA-4.5 System, Component, and Service Configurations; SA-8.20 Secure Metadata Management; SA-9.6 Organization-controlled Cryptographic Keys; SC-12.3 Asymmetric Keys; SC-28.1 Cryptographic Protection; SC-28.2 Offline Storage; SC-28.3 Cryptographic Keys; SI-12.2 Minimize Personally Identifiable Information in Testing, Training, and Research; SA-15.12 Minimize Personally Identifiable Information; SI-19.3 Release	SECURITY ATTRIBUTE OUTPUT; OUTPUT DEVICES; PRIVACY ATTRIBUTE OUTPUT; UNCLASSIFIED MOBILE DEVICES; CLASSIFIED INFORMATION; INFORMATION REVIEW; INFORMATION INSPECTION; TRUSTED DISTRIBUTION; MASTER COPY; SECURITY CONFIGURATIONS; U.S. GOVERNMENT CONFIGURATION BASELINE; USGCB; FUNCTIONS; PORTS; PROTOCOLS; SERVICES; SECURITY CHARACTERISTICS; DEVELOPER PROVIDED; DEVELOPER; Security and Privacy Engineering Principles | Secure Metadata Management; CRYPTOGRAPHIC KEYS; EXCLUSIVE CONTROL; ASYMMETRIC KEYS; NSA-APPROVED; KEY MANAGEMENT TECHNOLOGY AND PROCESSES; PUBLIC KEY INFRASTRUCTURE; PKI; CLASS 3; CLASS 4; PRIVATE KEY; PUBLIC KEY; CRYPTOGRAPHIC PROTECTION; INFORMATION AT REST; OFF-LINE STORAGE; Protection of Information at Rest | Cryptographic Keys; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII; DATA MINIMIZATION; Development Process, Standards, and Tools | Minimize Personally Identifiable Information; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII	Storing plaintext sensitive data in client side local storage makes the data easily accessible by anyone who gains privileged access to the client system. This bypasses user authentication enforced by the application. In addition to data leakage in shared client environments, such as a public computer's browser, a cross-site scripting (XSS) flaw allows attackers to easily access sensitive data.	The mechanism for encrypting data in the browser is driven by the requirement to gain access to the data while the application is offline (i.e., a Progressive Web App). __When offline access is not a requirement__ follow these steps: *** Authenticate the user against the backend system** * Request a salt from the client (see notes below) * Use the salt to generate a symmetric encryption key * Send the key to the client (see notes below) * Use the client key to encrypt and decrypt data at rest. * To regain access to encrypted data, follow these steps again using the existing salt. __*Note:*__ More detail is available in HOWTO section (Encrypt using a key obtained from the server) of this task. __When offline access is a requirement__ follow these steps: * Generate or retrieve a salt on the client (see notes below) * Prompt the user for a passphrase to initialize the encryption/decryption key * Use the user's passphrase and salt to generate a symmetric encryption key * Passphrases can be turned into cryptographic keys using a Password-Based Key Derivation Function (PBKDF) * PBKDF2 is a widely supported function that achieves this. * Use the key to encrypt and decrypt data at rest. * To regain access to encrypted data, follow these steps again using the existing salt. __*Note:*__ More detail is available in HOWTO (Encrypt using a key generated from a user passphrase) section of this task. __*Note:*__ The steps here only concern access to encrypted data. User authentication against backend systems is a crucial part of a PWA running in online mode. __*Additional Notes*__ * The key is derived using a per-client salt * Use unique keys per client. An example of a client instance is a specific browser. * Key uniqueness is guaranteed by using a per-client salt. * Randomly generate the salt by the client and store it in the browser. When an existing salt is available, it should be reused. * The salt can be stored in Local Storage in plain text * The key is used in the browser to encrypt and decrypt locally stored data * Keep the key in memory on the client. Do not store the key in the browser. * When the client's browsing context is closed, the key will be dismissed. * The implementation of the encryption/decryption logic must be centralized * In an Angular application, these features are typically implemented using an application-wide service. Only this service handles the keys.	Cryptography	A.10.1; A.8.2; A.9.4; A.11.1; A.12.4; A.6.2; A.14.2	A.10.1 Cryptographic classification; A.9.4 Sy control; A.11.1 Secure monitoring; A.6.2 Mo teleworking; A.14.2 Sc support processes
T1880_Encrypt data at rest for Lambda functions (AWS)	A.18.1.3; AC-16(5); AU-13(3); SA-4(5); SA-8(20); SC-12(3); SC-28(1); SC-28(2); SC-28(3); SI-12(2); SA-15(12); SI-19(3)	A.18.1.3 Protection of records; AC-16.5 Attribute Displays on Objects to Be Output; AU-13.3 Unauthorized Replication of Information; SA-4.5 System, Component, and Service Configurations; SA-8.20 Secure Metadata Management; SC-12.3 Asymmetric Keys; SC-28.1 Cryptographic Protection; SC-28.2 Offline Storage; SC-28.3 Cryptographic Keys; SI-12.2 Minimize Personally Identifiable Information in Testing, Training, and Research; SA-15.12 Minimize Personally Identifiable Information; SI-19.3 Release	SECURITY ATTRIBUTE OUTPUT; OUTPUT DEVICES; PRIVACY ATTRIBUTE OUTPUT; TRUSTED DISTRIBUTION; MASTER COPY; SECURITY CONFIGURATIONS; U.S. GOVERNMENT CONFIGURATION BASELINE; USGCB; FUNCTIONS; PORTS; PROTOCOLS; SERVICES; SECURITY CHARACTERISTICS; DEVELOPER PROVIDED; DEVELOPER; Security and Privacy Engineering Principles | Secure Metadata Management; ASYMMETRIC KEYS; NSA-APPROVED; KEY MANAGEMENT TECHNOLOGY AND PROCESSES; PUBLIC KEY INFRASTRUCTURE; PKI; CLASS 3; CLASS 4; PRIVATE KEY; PUBLIC KEY; CRYPTOGRAPHIC PROTECTION; INFORMATION AT REST; OFF-LINE STORAGE; Protection of Information at Rest | Cryptographic Keys; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII; DATA MINIMIZATION; Development Process, Standards, and Tools | Minimize Personally Identifiable Information; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII	Storage devices, such as memory cards, disks, and USB devices are normally accessible by other users and processes. For example, Android external storage could be available to all the running apps. If any sensitive data is stored in clear text on these devices, attackers could potentially read the data, if proper access control mechanisms are not implemented.	Apply appropriate protections to ensure the data is encrypted at rest, if a Lambda function is responsible for storing sensitive data such as PII in cloud storage utilities. ## Lambda `/tmp` Directory While it is possible to store data in the `/tmp` directory of a Lambda function. This is generally considered a poor location to store persistent data, especially sensitive PII. A resource [limit of 512 MB](https://docs.aws.amazon.com/lambda/latest/dg/limits.html) is also applied to the `/tmp` directory. ## Environment Variable Encryption Environment variables used in Lambda functions are encrypted by default using AWS Key Management Service. When the function is invoked, the values are decrypted and made available to the Lambda code. Unless specified, the environment variable is encrypted using a default service key that AWS creates. If more control is needed over the encryption key it is possible to create a customer-managed key. Compliance requirements such as PCI DSS or SOC2 may require keys to be managed internally. It is best practice to enable helpers for encryption in transit for environment variables used by Lambda functions. This masks the value you entered and results in a call to AWS KMS to encrypt the value and return it as Ciphertext. ## AWS S3 Data Encryption Data protection in AWS S3 can be accomplished by using either Server-Side Encryption (where the object is encrypted before it is saved to disk and decrypted when the object is downloaded), or Client-Side Encryption (where data is encrypted before it is uploaded to S3). ## RDS Data Encryption If your Lambda function is responsible for storing data in a managed database such as RDS, encryption at rest can be enabled by simply choosing "Enable Encryption" in the RDS console. Keys can either be managed by AWS or by using customer-managed keys. The AES-256 encryption algorithm is used to store the underlying storage for DB instances as well as automated backups and snapshots.	Cryptography	A.10.1; A.8.2; A.9.4; A.11.1; A.12.4; A.6.2; A.14.2; A.18.1	A.10.1 Cryptographic classification; A.9.4 Sy control; A.11.1 Secure monitoring; A.6.2 Mo teleworking; A.14.2 Sc support processes; A. and contractual requi

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

If ANY of these practices are not achieved, they NEED TO FACTOR into the RMF

EnterpriseGRC Solutions, Inc.

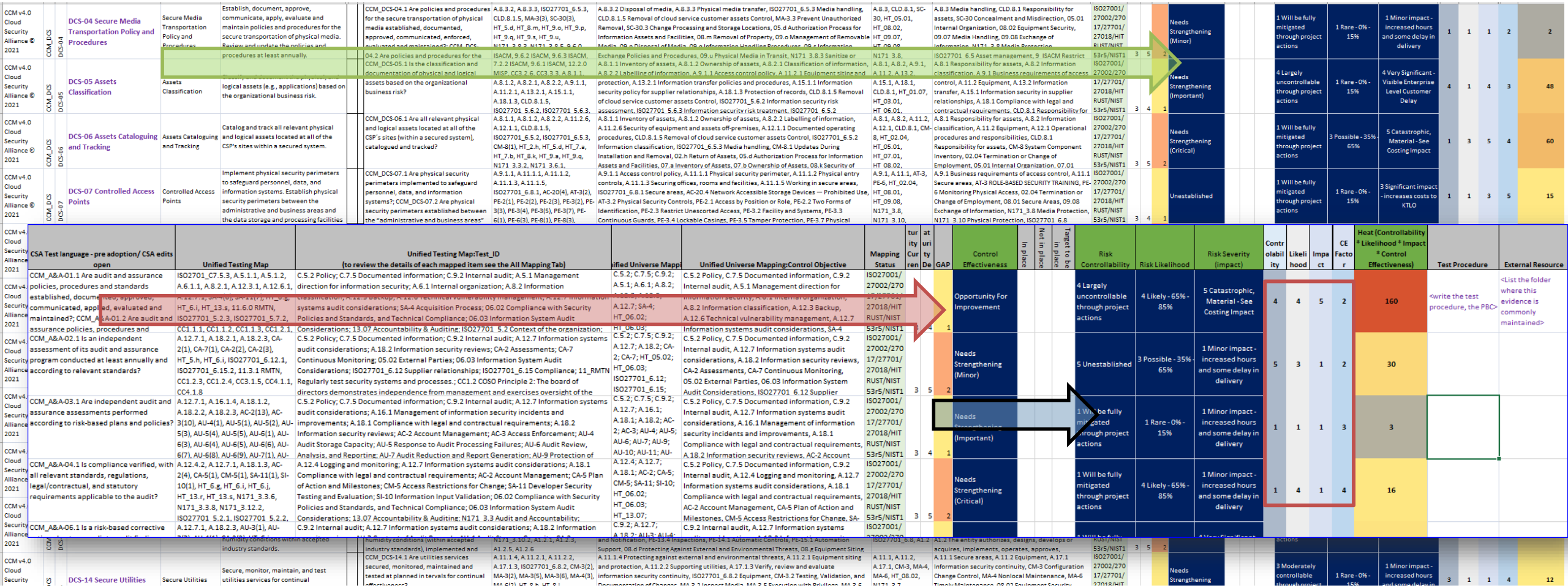
Assessment Testing ☆ > Cryptography

Test_ID	Mapped testi...	Mapped testing or practices:Test_ID	Mapped testing or practices:Problem Metadata	Risk Drivers	Detail Control Description (UCF)	Proble...	Mapped Proce...	Mapped Processes:
parameter store for sensitive data storage (Amazon ECS)	8(20); SC-12(3); SC-28(1); SC-28(2); SC-28(3); SI-12(2); SA-15(12); SI-19(3)	Cryptographic Protection; SC-28.2 Offline Storage; SC-28.3 Cryptographic Keys; SI-12.2 Minimize Personally Identifiable Information in Testing, Training, and Research; SA-15.12 Minimize Personally Identifiable Information; SI-19.3 Release	Principles | Secure Metadata Management; ASYMMETRIC KEYS; NSA-APPROVED; KEY MANAGEMENT TECHNOLOGY AND PROCESSES; PUBLIC KEY INFRASTRUCTURE; PKI; CLASS 3; CLASS 4; PRIVATE KEY; PUBLIC KEY; CRYPTOGRAPHIC PROTECTION; INFORMATION AT REST; OFF-LINE STORAGE; Protection of Information at Rest | Cryptographic Keys; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII; DATA MINIMIZATION; Development Process, Standards, and Tools | Minimize Personally Identifiable Information; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII	format can cause sensitive information leakage and the misuse of data.	Protect sensitive data as containers are deployed to ECS clusters. AWS offers solutions out of the box to handle the injection of sensitive data into containers using either AWS Secrets Manager or AWS Systems Manager Parameter Store. These features allow containers to retrieve the sensitive data from a secure location and inject the plaintext secret value as the container is initially started.	Cryptography	A.10.1; A.8.2; A.9.4; A.11.1; A.12.4; A.6.2; A.14.2; A.18.1	control; A.11.1 Secure a monitoring; A.6.2 Mobil teleworking; A.14.2 Secu support processes; A.18 and contractual require
T2046_Encrypt data stored in DynamoDB at rest (Amazon DynamoDB)	A.18.1.3; AC-16(5); AC-19(4); AU-13(3); SA-4(5); SA-8(20); SA-9(6); SC-12(3); SC-28(1); SC-28(2); SC-28(3); SI-12(2); SA-15(12); SI-19(3)	A.18.1.3 Protection of records; AC-16.5 Attribute Displays on Objects to Be Output; AC-19.4 Restrictions for Classified Information; AU-13.3 Unauthorized Replication of Information; SA-4.5 System, Component, and Service Configurations; SA-8.20 Secure Metadata Management; SA-9.6 Organization-controlled Cryptographic Keys; SC-12.3 Asymmetric Keys; SC-28.1 Cryptographic Protection; SC-28.2 Offline Storage; SC-28.3 Cryptographic Keys; SI-12.2 Minimize Personally Identifiable Information in Testing, Training, and Research; SA-15.12 Minimize Personally Identifiable Information; SI-19.3 Release	SECURITY ATTRIBUTE OUTPUT; OUTPUT DEVICES; PRIVACY ATTRIBUTE OUTPUT; UNCLASSIFIED MOBILE DEVICES; CLASSIFIED INFORMATION; INFORMATION REVIEW; INFORMATION INSPECTION; TRUSTED DISTRIBUTION; MASTER COPY; SECURITY CONFIGURATIONS; U.S. GOVERNMENT CONFIGURATION BASELINE; USGCB; FUNCTIONS; PORTS; PROTOCOLS; SERVICES; SECURITY CHARACTERISTICS; DEVELOPER PROVIDED; DEVELOPER; Security and Privacy Engineering Principles | Secure Metadata Management; CRYPTOGRAPHIC KEYS; EXCLUSIVE CONTROL; ASYMMETRIC KEYS; NSA-APPROVED; KEY MANAGEMENT TECHNOLOGY AND PROCESSES; PUBLIC KEY INFRASTRUCTURE; PKI; CLASS 3; CLASS 4; PRIVATE KEY; PUBLIC KEY; CRYPTOGRAPHIC PROTECTION; INFORMATION AT REST; OFF-LINE STORAGE; Protection of Information at Rest | Cryptographic Keys; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII; DATA MINIMIZATION; Development Process, Standards, and Tools | Minimize Personally Identifiable Information; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII	Data stored unencrypted on disks in DynamoDB can be stolen and misused. It is necessary to keep sensitive data protection as close to its origin as possible to prevent theft by malicious third-party software or web attacks.	DynamoDB **encrypts all data stored in tables at rest** by default but leaves the encryption key up to the administrator. DynamoDB supports either AWS managed keys or customer-managed keys (CMK). Utilize CMKs to give you full control over who can use the keys to access the encrypted data on DynamoDB tables.	Cryptography	A.8.2; A.10.1; A.11.2; A.14.1; A.18.1	A.8.2 Information classif Cryptographic controls; Security requirements o A.18.1 Compliance with requirements
T2048_Utilize client-side encryption for DynamoDB (Amazon DynamoDB)	A.10.1.1; A.10.1.2; A.13.1.2; A.14.1.2; A.14.1.3; A.18.1.3; AC-17(2); AU-9(3); SA-4(2); SI-7(6); SI-7(15); SI-10(5)	A.10.1.1 Policy on the use of cryptographic controls; A.10.1.2 Key management; A.13.1.2 Security of network services; A.14.1.2 Securing application services on public networks; A.14.1.3 Protecting application services transactions; A.18.1.3 Protection of records; AC-17.2 PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION; AU-9.3 CRYPTOGRAPHIC PROTECTION; SA-4.2 Design and Implementation Information for Controls; SI-7.6 Cryptographic Protection; SI-7.15 Code Authentication; SI-10.5 Restrict Inputs to Trusted Sources and Approved Formats	ENCRYPTION; SESSION CONFIDENTIALITY; SESSION INTEGRITY; SECURITY CATEGORIZATION; CRYPTOGRAPHIC PROTECTION; CRYPTOGRAPHIC MECHANISMS; INTEGRITY; IMPLEMENTATION INFORMATION; SECURITY- RELEVANT EXTERNAL SYSTEM INTERFACE; HIGH- LEVEL DESIGN; LOW-LEVEL DESIGN; SOURCE CODE; HARDWARE SCHEMATICS; DEVELOPER PROVIDED; DEVELOPER; RESILIENCE RESILIENCY; CRYPTOGRAPHIC PROTECTION MECHANISMS; RESILIENCY; RESILIENCE CRYPTOGRAPHY; CRYPTOGRAPHIC MECHANISMS; CRYPTOGRAPHIC AUTHENTICATION; DIGITAL SIGNATURES; RESTRICT INPUTS; WHITELISTING; TRUSTED SOURCES; ACCEPTABLE FORMATS; RESILIENCY; RESILIENCE	Data stored unencrypted on disk in DynamoDB can be stolen and misused. It is necessary to keep sensitive data protection as close to its origin as possible to prevent theft by malicious third-party software or web attacks.	DynamoDB gives you the ability to utilize client-side encryption to help ensure the **plaintext data is protected at origin as well as over the network.** **Utilize client-side encryption** in DynamoDB, by **including a software library** with your application that can handle **encryption**, the signing of attribute values, and key management.	Cryptography	A.9.1; A.10.1; A.12.5; A.13.1; A.14.1; A.18.1	A.9.1 Business requirem A.10.1 Cryptographic co operational software; A. management; A.14.1 Se information systems; A. legal and contractual re
T2056_Encrypt data stored at rest (Amazon Aurora)	A.18.1.3; AC-16(5); AC-19(4); AU-13(3); SA-4(5); SA-8(20); SA-9(6); SC-12(3); SC-28(1); SC-28(2); SC-28(3); SI-12(2); SA-15(12); SI-19(3)	A.18.1.3 Protection of records; AC-16.5 Attribute Displays on Objects to Be Output; AC-19.4 Restrictions for Classified Information; AU-13.3 Unauthorized Replication of Information; SA-4.5 System, Component, and Service Configurations; SA-8.20 Secure Metadata Management; SA-9.6 Organization-controlled Cryptographic Keys; SC-12.3 Asymmetric Keys; SC-28.1 Cryptographic Protection; SC-28.2 Offline Storage; SC-28.3 Cryptographic Keys; SI-12.2 Minimize Personally Identifiable Information in Testing, Training, and Research; SA-15.12 Minimize Personally Identifiable Information; SI-19.3 Release	SECURITY ATTRIBUTE OUTPUT; OUTPUT DEVICES; PRIVACY ATTRIBUTE OUTPUT; UNCLASSIFIED MOBILE DEVICES; CLASSIFIED INFORMATION; INFORMATION REVIEW; INFORMATION INSPECTION; TRUSTED DISTRIBUTION; MASTER COPY; SECURITY CONFIGURATIONS; U.S. GOVERNMENT CONFIGURATION BASELINE; USGCB; FUNCTIONS; PORTS; PROTOCOLS; SERVICES; SECURITY CHARACTERISTICS; DEVELOPER PROVIDED; DEVELOPER; Security and Privacy Engineering Principles | Secure Metadata Management; CRYPTOGRAPHIC KEYS; EXCLUSIVE CONTROL; ASYMMETRIC KEYS; NSA-APPROVED; KEY MANAGEMENT TECHNOLOGY AND PROCESSES; PUBLIC KEY INFRASTRUCTURE; PKI; CLASS 3; CLASS 4; PRIVATE KEY; PUBLIC KEY; CRYPTOGRAPHIC PROTECTION; INFORMATION AT REST; OFF-LINE STORAGE; Protection of Information at Rest | Cryptographic Keys; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII; DATA MINIMIZATION; Development Process, Standards, and Tools | Minimize Personally Identifiable Information; PRIVACY; PERSONALLY IDENTIFIABLE INFORMATION; PII	Unencrypted data stored on disks in cloud environments may be stolen and misused.	Always utilize strong encryption mechanisms on Aurora instances that handle data that is sensitive in nature. Aurora encryption is easy to enable within the AWS console and offers the ability to encrypt the data stored on the Aurora instance's underlying storage filesystem, automated backups, and snapshots. Aurora encryption is performed using AES-256 and is protected by the AWS Key Management System (KMS). Utilize KMS Customer-Managed Keys when possible to give you full control over who can use the keys to access the encrypted data on KMS instances.	Cryptography	A.10.1; A.8.2; A.9.4; A.11.1; A.12.4; A.6.2; A.14.2	A.10.1 Cryptographic co classification; A.9.4 Syste control; A.11.1 Secure a monitoring; A.6.2 Mobil teleworking; A.14.2 Secu support processes
T2065_Configure TLS for secure connections to App Service (Microsoft Azure)	A.13.2.1; AC-4(4); AC-17(2); AC-18(1); IA-3(1); SC-5(1); SC-7(10); SC-7(17); SC-8(1); SC-23(5); SI-4(2)	A.13.2.1 Information transfer policies and procedures; AC-4.4 Flow Control of Encrypted Information; AC-17.2 PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION; AC-18.1 Authentication and Encryption; IA-3.1 Cryptographic Bidirectional Authentication; SC-5.1 Restrict Ability to Attack Other Systems; SC-7.10 Prevent Exfiltration; SC-7.17 Automated Enforcement of Protocol Formats; SC-8.1 Cryptographic Protection; SC-23.5 Allowed Certificate Authorities; SI-4.2 Automated Tools and Mechanisms for Real-time Analysis	CHECKING ENCRYPTED INFORMATION CONTENT; DECRYPT INFORMATION; BLOCK FLOW OF ENCRYPTED INFORMATION; ENCRYPTION; SESSION CONFIDENTIALITY; SESSION INTEGRITY; SECURITY CATEGORIZATION; WIRELESS AUTHENTICATION; ENCRYPTION; CRYPTOGRAPHIC; BIDIRECTIONAL AUTHENTICATION; REMOTE CONNECTIONS; RESTRICTION; INTERNAL USERS; SYSTEM ACCESS; EXFILTRATION; MANAGED INTERFACES; RESILIENCY; RESILIENCE ENFORCE PROTOCOL FORMATS; AUTOMATED; CRYPTOGRAPHIC MECHANISMS; ENCRYPTING; ALTERNATIVE PHYSICAL SAFEGUARDS; PREVENT UNAUTHORIZED DISCLOSURE OF INFORMATION; DETECT CHANGES TO INFORMATION; CERTIFICATE AUTHORITIES; CA; CERTIFICATES; SECURE SOCKET LAYER; SSL; TRANSPORT LAYER SECURITY; TLS; REAL-TIME ANALYSIS; AUTOMATED TOOLS; HOST- BASED; NETWORK-BASED; TRANSPORT-BASED; STORAGE-BASED; SECURITY INFORMATION AND EVENT MANAGEMENT; ALERTS; NOTIFICATIONS; RESILIENCY; RESILIENCE	Azure Web Apps allows sites to run under both HTTP and HTTPS by default and Web apps can be accessed by anyone using non-secure HTTP URLs.	Perform the following: - Redirect all HTTP traffic to HTTPS in Azure App Service: Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic. HTTPS uses the SSL/TLS protocol to provide a secure connection, which is both encrypted and authenticated. So it is important to support HTTPS for the security benefits. - Use the latest version of TLS encryption: App service currently allows the web app to set TLS versions 1.0, 1.1 and 1.2. It is highly recommended to use the latest TLS 1.2 version, which is the recommended TLS level by industry standards, such as PCI DSS, for web app secure connections. - Set 'Client Certificates (incoming client certificates)' to 'On': The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client who has valid certificates can access the app.	Cryptography	A.10.1; A.13.2; A.14.1; A.14.2	A.10.1 Cryptographic co transfer; A.14.1 Security information systems; A. development and suppo

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

The Product of Mapping is Security & Risk Program Management

EnterpriseGRC Solutions, Inc.



CSA Test language - pre adoption/ CSA edits open	Unified Testing Map	Unified Testing Map:Test_ID (to review the details of each mapped item see the All Mapping Tab)	ified Universe Mappi	Unified Universe Mapping:Control Objective	Mapping Status	turity Curren	at urity De	GAP	Control Effectiveness	In place	Not in place	Target to be in place	Risk Controllability	Risk Likelihood	Risk Severity (impact)	Contrlability	Likelihood	Impact	CE Factor	Heat (Controllability * Likelihood * Impact * Control Effectiveness)	Test Procedure	External Resource
CCM_A&A-01.1 Are audit and assurance policies, procedures and standards established, documented, approved, communicated, applied, evaluated and maintained?; CCM_A&A-01.2 Are audit and assurance policies, procedures and	ISO27701_C7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.8.2.1, A.12.3.1, A.12.6.1, A.12.7.1, SA-4(5), SA-11(1), HT_6.g, HT_6.i, HT_13.s, 11.6.0 RMTN, ISO27701_5.2.3, ISO27701_5.7.2, CC1.1.1, CC1.1.2, CC1.1.3, CC1.2.1,	C.5.2 Policy; C.7.5 Documented information; C.9.2 Internal audit; A.5.1 Management direction for information security; A.6.1 Internal organization; A.8.2 Information classification, A.12.3 Backup, A.12.6 Technical vulnerability management, A.12.7 Information systems audit considerations; SA-4 Acquisition Process; 06.02 Compliance with Security Policies and Standards, and Technical Compliance; 06.03 Information System Audit Considerations; 13.07 Accountability & Auditing; ISO27701_5.2 Context of the organization;	C.5.2; C.7.5; C.9.2; A.5.1; A.6.1; A.8.2; A.12.3; A.12.6; A.12.7; SA-4; HT_06.02; HT_06.03;	C.5.2 Policy, C.7.5 Documented information, C.9.2 Internal audit, A.5.1 Management direction for information security, A.6.1 Internal organization, A.8.2 Information classification, A.12.3 Backup, A.12.6 Technical vulnerability management, A.12.7 Information systems audit considerations, SA-4	ISO27001/ 27002/270 17/27701/ 27018/HIT RUST/NIST 53r5/NIST1	4	1		Opportunity For Improvement				4 Largely uncontrollable through project actions	4 Likely - 65% - 85%	5 Catastrophic, Material - See Costing Impact	4	4	5	2	160	<write the test procedure, the PBC>	<List the folder where this evidence is commonly maintained>
CCM_A&A-02.1 Is an independent assessment of its audit and assurance program conducted at least annually and according to relevant standards?	A.12.7.1, A.18.2.1, A.18.2.3, CA-2(1), CA-7(1), CA-2(2), CA-2(3), HT_5.h, HT_6.i, ISO27701_6.12.1, ISO27701_6.15.2, 11.3.1 RMTN, CC1.2.3, CC1.2.4, CC3.1.5, CC4.1.1, CC4.1.8	C.5.2 Policy; C.7.5 Documented information; C.9.2 Internal audit; A.12.7 Information systems audit considerations; A.18.2 Information security reviews; CA-2 Assessments; CA-7 Continuous Monitoring; 05.02 External Parties; 06.03 Information System Audit Considerations; ISO27701_6.12 Supplier relationships; ISO27701_6.15 Compliance; 11_RMTN Regularly test security systems and processes.; CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the	C.5.2; C.7.5; C.9.2; A.12.7; A.18.2; CA-2; CA-7; HT_05.02; HT_06.03; ISO27701_6.12; ISO27701_6.15;	C.5.2 Policy, C.7.5 Documented information, C.9.2 Internal audit, A.12.7 Information systems audit considerations, A.18.2 Information security reviews, CA-2 Assessments, CA-7 Continuous Monitoring, 05.02 External Parties, 06.03 Information System Audit Considerations, ISO27701_6.12 Supplier	ISO27001/ 27002/270 17/27701/ 27018/HIT RUST/NIST 53r5/NIST1	3	5	2	Needs Strengthening (Minor)				5 Unestablished	3 Possible - 35% - 65%	1 Minor impact - increased hours and some delay in delivery	5	3	1	2	30		
CCM_A&A-03.1 Are independent audit and assurance assessments performed according to risk-based plans and policies?	A.12.7.1, A.16.1.4, A.18.1.2, A.18.2.2, A.18.2.3, AC-2(13), AC-3(10), AU-4(1), AU-5(1), AU-5(2), AU-5(3), AU-5(4), AU-5(5), AU-6(1), AU-6(3), AU-6(4), AU-6(5), AU-6(6), AU-6(7), AU-6(8), AU-6(9), AU-7(1), AU-	C.5.2 Policy; C.7.5 Documented information; C.9.2 Internal audit; A.12.7 Information systems audit considerations; A.16.1 Management of information security incidents and improvements; A.18.1 Compliance with legal and contractual requirements; A.18.2 Information security reviews; AC-2 Account Management; AC-3 Access Enforcement; AU-4 Audit Storage Capacity; AU-5 Response to Audit Processing Failures; AU-6 Audit Review, Analysis, and Reporting; AU-7 Audit Reduction and Report Generation; AU-9 Protection of	C.5.2; C.7.5; C.9.2; A.12.7; A.16.1; A.18.1; A.18.2; AC-2; AC-3; AU-4; AU-5; AU-6; AU-7; AU-9; AU-10; AU-11; AU-	C.5.2 Policy, C.7.5 Documented information, C.9.2 Internal audit, A.12.7 Information systems audit considerations, A.16.1 Management of information security incidents and improvements, A.18.1 Compliance with legal and contractual requirements, A.18.2 Information security reviews, AC-2 Account	ISO27001/ 27002/270 17/27701/ 27018/HIT RUST/NIST 53r5/NIST1	3	4	1	Needs Strengthening (Important)				1 Will be fully mitigated through project actions	1 Rare - 0% - 15%	1 Minor impact - increased hours and some delay in delivery	1	1	1	3	3		
CCM_A&A-04.1 Is compliance verified, with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	A.12.4.2, A.12.7.1, A.18.1.3, AC-2(4), CA-5(1), CM-5(1), SA-11(1), SI-10(1), HT_6.g, HT_6.i, HT_6.j, HT_13.r, HT_13.s, N171_3.3.6, N171_3.3.8, N171_3.12.2, ISO27701 5.2.1, ISO27701 5.2.2,	A.12.4 Logging and monitoring; A.12.7 Information systems audit considerations; A.18.1 Compliance with legal and contractual requirements; AC-2 Account Management; CA-5 Plan of Action and Milestones; CM-5 Access Restrictions for Change; SA-11 Developer Security Testing and Evaluation; SI-10 Information Input Validation; 06.02 Compliance with Security Policies and Standards, and Technical Compliance; 06.03 Information System Audit Considerations; 13.07 Accountability & Auditing; N171_3.3 Audit and Accountability;	C.5.2; C.7.5; C.9.2; A.12.7; A.16.1; A.18.1; A.18.2; AC-2; CA-5; CM-5; SA-11; SI-10; HT_06.02; HT_06.03; HT_13.07;	C.5.2 Policy, C.7.5 Documented information, C.9.2 Internal audit, A.12.4 Logging and monitoring, A.12.7 Information systems audit considerations, A.18.1 Compliance with legal and contractual requirements, AC-2 Account Management, CA-5 Plan of Action and Milestones, CM-5 Access Restrictions for Change, SA-	ISO27001/ 27002/270 17/27701/ 27018/HIT RUST/NIST 53r5/NIST1	3	5	2	Needs Strengthening (Critical)				1 Will be fully mitigated through project actions	4 Likely - 65% - 85%	1 Minor impact - increased hours and some delay in delivery	1	4	1	4	16		
CCM_A&A-06.1 Is a risk-based corrective	A.12.7.1, A.18.2.3, AU-3(1), AU-	C.9.2 Internal audit; A.12.7 Information systems audit considerations; A.18.2 Information	C.9.2; A.12.7;	C.9.2 Internal audit, A.12.7 Information systems	ISO27001/																	

A Control area could have a minor finding – however the overall risk raised by that finding could be negligible

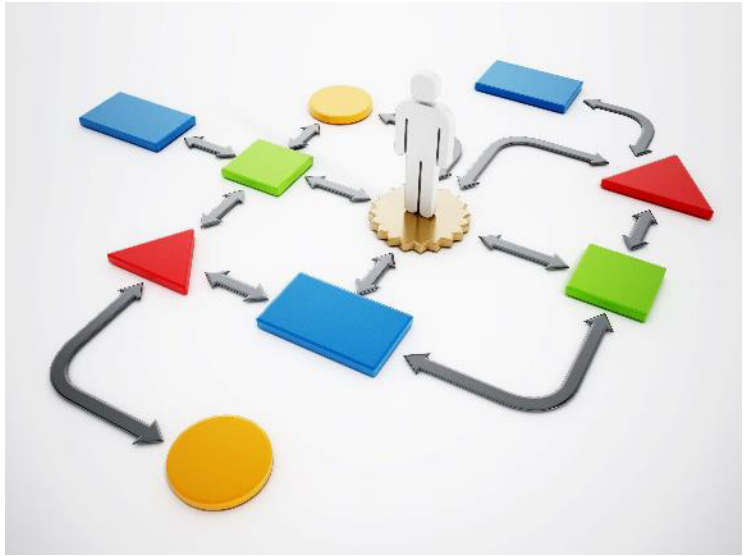
Other OFI could reveal a situation that is unmanaged, will occur again in multiple audits, and has potential for customer facing disruptions and loss of revenue.

Risk Management needs to Only Handle It Once – OHIO, but capture all the inputs, players, timing, and necessary resources for improvement

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Recap: Management Strategy First + Why r5 CCM 4 Now

- GRC Mapping strategy: **Order-of-Operations**
- Risk-> Goals-> Policies->Controls)



- Using NIST SP 800-53 r5 as the underpinning backbone assumes mapping to other major frameworks so the business “Only Handles Policy Once”. OHIO
- Use NIST 800-53 r5 as the mediating framework connecting architecture CMDB to CIS/DISA STIGs/OWASP/MITRE ATT&CK
- Use ISO/IEC 27001 with Cloud, Privacy and Processing as the Policy framework – commonly mapped to NIST SP 800-53 r4/r5 as part of NIST Appendix
- Use a RMF on top of your preferred framework (Could be SOC 2, CSTAR, ISO27, **HITRUST™, IMO use NIST CSF).
- Establish Categories for the Corporate Common Controls. Push those categories into Policies, Controls, Programs.

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com

Summarizing and Take-Aways

EnterpriseGRC Solutions, Inc.

1. Mapping accounts for the Risks & associated RACI of a program – so groupings should align with the common job assignments that would implement them.
2. Client based mapping begins with understanding the business programs and should account for domains (LOB) with isolated scope, such as Consumer, Cloud, Fed, Health & Human Service, Financial, Global, etc.
3. Language matching alone, rather than mapping to the recommended implementation guidance, results in guidance that's unusable.
4. Mapping accomplishes an aggregate Policy requirement that will and will always continue to be measured by product and by assessment event and will move at the pace of your slowest audit.

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com


THANK YOU