EnterpriseGRC Solutions, Inc.

"This associates to That – and That includes This"
The Pitfalls and Opportunities in upgrading to CCM 4.0

Robin Basham, CEO, EnterpriseGRC Solutions

Presentation to ISC2 East Bay, May 13th, 2021

Familiar Faces I've invited to join conversation – just a few. There are plenty more. If you want to chime in, let us know via chat.

EnterpriseGRC Solutions, Inc.

Robin Basham, ISC2 East Bay Chapter Pres. CEO, EnterpriseGRC Solutions, GRC Expert

Kumar Selvaraj

Zscaler

CCM company driver

CSTAR Customer

(ISACA / PCI / HITRUST)

Sean Cordero

Chair, Cloud Control Matrix Working Group

Cloud Security Alliance

ISC2 East Bay Past Conference Co-Chair

Dorian Cougias Lead Analyst at Unified Compliance Framework

ISC2 East Bay Sponsor, Speaker, Great Contact

Eric Heitzman, Software Security Expert, Security Compass – Great Contact

“We’d like to use CCM as our Master Control List”

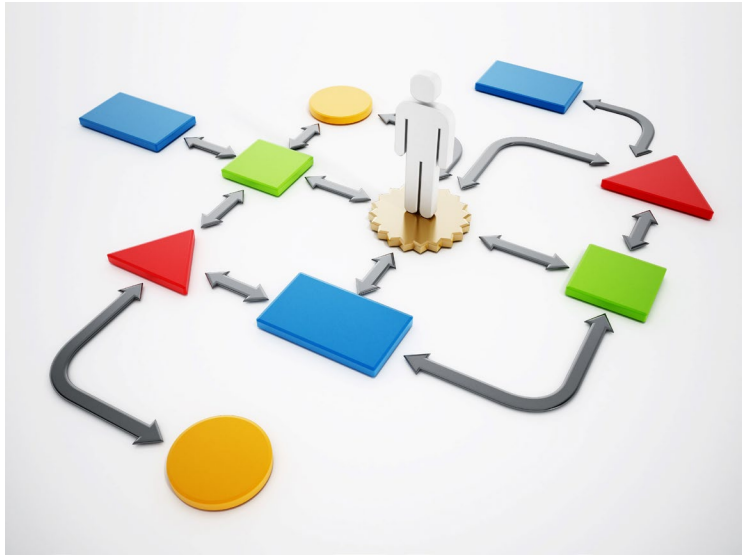
EnterpriseGRC Solutions, Inc.

1. Major Cloud Providers expect to use ©Cloud Security Alliance, CCM 4.0 as the backbone supporting their Security Programs Policies, Programs, Audits
2. Leveraging existing ©AICPA SOC 2, ©HITRUST, PCI, FedRamp, 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.*
3. 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. Volunteers generally can’t do it. Is increasingly necessary (CMMC)
4. The available mappings offered by AICPA, NIST, HITRUST, and CSA have proven un-useful. We’d like to help restore consumer confidence in using CCM 4.0 as a mapped framework. We also seek to support NIST expanded efforts for SP-800-53 r5, SP-800-53B, NIST SP-800-171r2, SP-800-172 Cybersecurity

*EnterpriseGRC Solutions wants to share work product delivered to a CSA partner and has approval to share their name during this conversation.

Management Strategy First + Why 4.0 Now

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



- Using CCM 4.0 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
- Use ISO/IEC 27001 with Cloud, Privacy and Processing as the Policy framework
- Use a RMF on top of your preferred framework (Could be SOC 2, CSTAR, ISO27, **HITRUST™, Should be NIST CSF).
- Establish Categories for the Corporate Common Controls. Push those categories into Policies, Controls, Programs.

*EnterpriseGRC Solutions wants to share work product delivered to a CSA partner and has approval to share their name during this conversation.

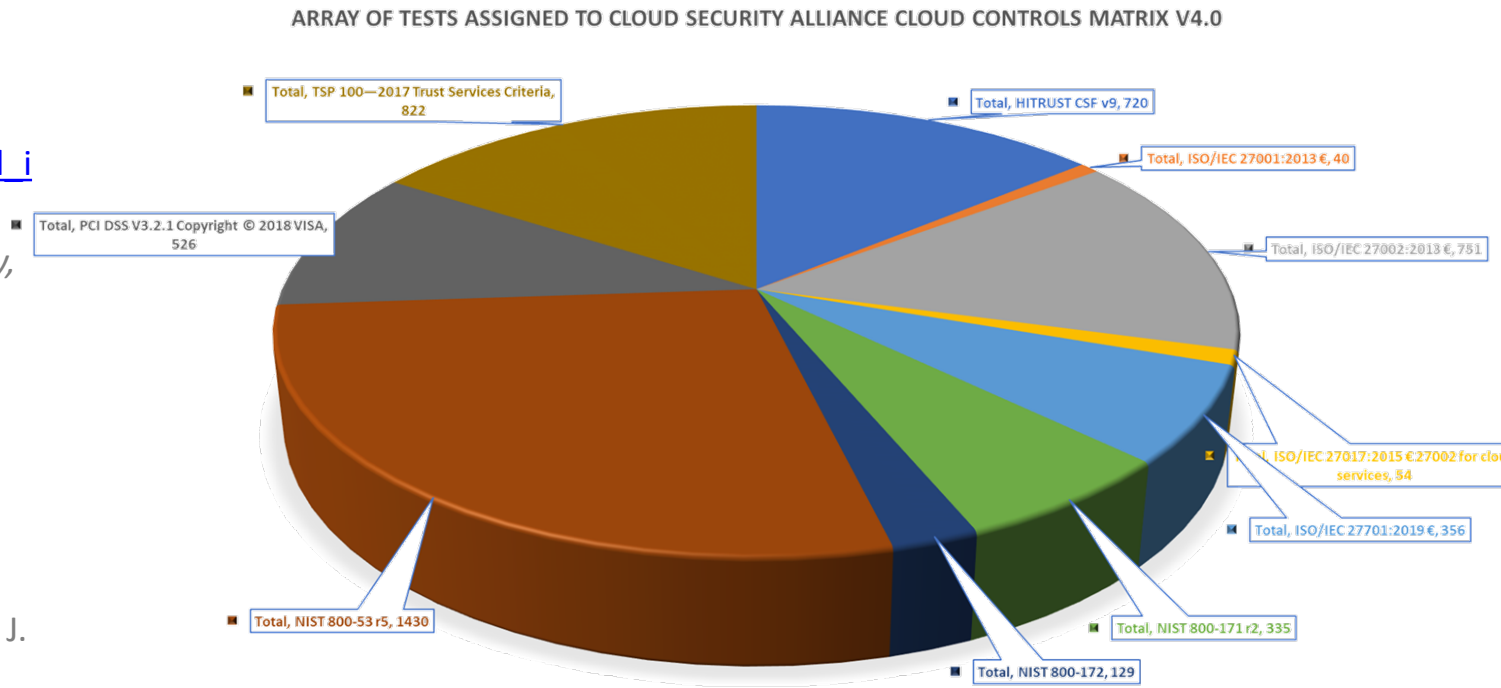
Cloud Control Matrix Domains and Controls – What's the rush?

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

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

EnterpriseGRC Solutions, Inc.

- California Consumer Privacy Act of 2018 – *Privacy + Cryptography lack implementation details, but customers hold providers accountable to the results* CCPA **SB-1121 California Consumer Privacy Act of 2018.** https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
- 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) new controls replace 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

Polling Question

*EnterpriseGRC Solutions verifies and purchases a copy of each framework each time we do a mapping exercise for our client. Clients are required to show their license to operate with CSA, CIS, HITRUST, GAMP, ISACA, AICPA etc. and the content of the mapping remains with that client for their operational application only. We do not provide framework content to the public. We do not work with unlicensed content. We give mapping to NIST, CIS, CSA, AICPA in good faith to support their working groups and advance our Professional Community.

CCM 3.0 to 4.0 Mapping and Transition Discussion

EnterpriseGRC Solutions, Inc.

- Delay in adapting CCM 3.x to 4.0 will contribute to failing new legal requirements - Laws for Privacy/IOT, CCPA, GDPR
- Compounding industry framework updates often publish or retain old and wrong mapping
  - Misuse of Tagging, incorrect data models; Confusing overlays, enhancements, guidance and criterion driven attributes with new and distinct controls
  - Not using a distinct set of control identifiers at the correct level of the framework – Domain, Parent/Family, Child/Test/Enhancement

Control Domain	Control Title	Control ID	ated Control Specifica	CCM v3.0.1			ISO/IEC 27001/02/17/18		
				Controls Mapping	ap Lev	Addenda	Controls Mapping	Gap Level	Addenda
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate audit and assurance policies, procedures and standards' Requirement of 'at least	27001: 9.2 Nope, that's the audit program. The audit policy would be part of Policies C.5.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least	AAC-02	No Gap	N/A	27001: A.18.2.1 27002: A.18.2.1	Partial Gap	Missing specification(s) in ISOs: Terms 'audit and assurance' and 'at
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	AAC-01 AAC-02	No Gap	N/A	27001: A.18.2.1 27002: 18.2.1 27018: 18.2.1 additional guidance	No Gap	N/A
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	GRM-01 GRM-03	No Gap	N/A	27001: A.18.2.2 27002: 18.2.2 27001: A.18.2.3 27002: 18.2.3	No Gap	N/A

- Framework Enhancements associate to expectations in the market. The next audit will presume the new framework has been in use for the preceding year.
- Customers expect the Cybersecurity, Privacy, Cloud, and Processing certifications as associated to their most common assessment events.
  - SOC2, ISO27001, FedRamp, DFARS CMMC, HITRUST, PCI, GDPR, CCPA/CCPRA etc.

What's so hard about mapping? The What->

EnterpriseGRC Solutions, Inc.

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 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 Management
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 Management
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 Management
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 Informatio...	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_...	ISO27		
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/N		
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(5)...	ISO/N		
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/N		
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); 1...	ISO/N		
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 completed 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); PS-...	ISO/N		
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/N		
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/N		
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 includes on-going information security requireme...	A.7.2.3; A.7.3.1; CLD.8.1.5; AC-2(12); AC-3(14); PS-4...	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 7.3 Termination ...	Access and Administra
A.8.1.1 Inventory of assets	ISO/IEC 27002:2013 €	A.8.1 Responsibility fo...	PIMS Applied 27701/27018	Policy: Each department shall identify assets relevant to the lifecycle of information and document their imp...	A.8.2.3; A.11.2.5; A.11.2.6; CLD.8.1.5; CM-8(7); CP-2...	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 8 Asset manag...	Asset Management SC
A.8.1.2 Ownership of assets	ISO/IEC 27002:2013 €	A.8.1 Responsibility fo...	PIMS Applied 27701/27018	Policy: Individuals as well as other entities having approved management responsibility for the asset lifecycl...	A.8.2.3; A.11.2.5; A.11.2.6; CLD.8.1.5; CM-8(7); CP-2...	ISO/NIST/LSHC up to date	ISO/IEC 27018:2019(E) 8 Asset manag...	Asset Management St.

ISO/IEC 27001/02/17/18

Controls Mapping	Gap Level	Addenda
27001: 9.2 Nope, that's the audit program. The audit policy would be part of Policies C.5.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.
27001: A.18.2.1 27002: A.18.2.1	Partial Gap	Missing specification(s) in ISOs: Terms 'audit and assurance' and 'at
27001: A.18.2.1 27002: 18.2.1 27018: 18.2.1 additional guidance	No Gap	N/A
27001: A.18.2.2 27002: 18.2.2 27001: A.18.2.3 27002: 18.2.3	No Gap	N/A

Data Architectures are distinct: Controls Overlay – Example: DSP-13 Sub-Processing

EnterpriseGRC Solutions, Inc.

Editi	Control ID	Detail Num	Test_ID	Detail Control Description (UCF)	PIMS Specification ISO/IEC 27701:2019 - ISO/IEC 27018:2019	ISO/IEC 27017:2015 (E) Supplemental Guidance	Guidance for clo	Mapped esting
ISO/IEC 27001:2013 €	C.6.1	ISO2701_C6.1.1	ISO2701_C6.1.1 General	**6.1.1 General** When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security and privacy management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects in the processing of PII; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and how to integrate and implement the actions into its information security and privacy management system processes; and evaluate the effectiveness of these actions. e) apply the information security and privacy risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability, within the scope of the PIMS. f) apply a privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.	**ISO/IEC 27701:2019(E) 5.4.1 Actions to address risks and opportunities** **5.4.1.1 General** The requirements stated in ISO/IEC 27001:2013, **6.1.1** along with the interpretation specified in 5.1, apply. **5.4.1.2 Information security risk assessment** The requirements stated in ISO/IEC 27001:2013, **6.1.2** apply with the following refinements: ISO/IEC 27001:2013, **6.1.2 c)** 1) is refined as follows: The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability, within the scope of the PIMS. The organization shall apply a privacy risk assessment process to identify risks related	<blank>	<blank>	A.12.6.1, A.18.2.1, A.12.7.1, A.16.1.4, CA-2(2), CA-9(1), CM-6(1), CM-7(1), CM-8(1), CM-8(4), CM-9(1), PM-5(1), IR-6(2), RA-5(3), RA-5(4), RA-5(10), SA-4(2), SA-4(5), SA-4(9), SA-9(1), SA-10(1), SA-11(2), SA-11(7), SA-15(7), GMP5_6.2.5.1.
ISO/IEC 27001:2013 €	C.6.1	ISO2701_C6.1.2	ISO2701_C6.1.2 Information security risk assessment	**6.1.2 Information security risk assessment** The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid, and comparable results; c) identifies the information security risks: *1. The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability, within the scope of the PIMS.*	**ISO/IEC 27701:2019(E) 5.4.1 Actions to address risks and opportunities** **5.4.1.1 General** The requirements stated in ISO/IEC 27001:2013, **6.1.1** along with the interpretation specified in 5.1, apply. **5.4.1.2 Information security risk assessment** The requirements stated in ISO/IEC 27001:2013, **6.1.2** apply with the following refinements: ISO/IEC 27001:2013, **6.1.2 c)** 1) is refined as follows: The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability, within the scope of the PIMS. The organization shall apply a privacy risk assessment process to identify risks related	<blank>	<blank>	A.12.6.1, A.18.2.1, A.12.7.1, A.16.1.4, CA-2(2), CA-9(1), CM-6(1), CM-7(1), CM-8(1), CM-8(4), CM-9(1), PM-5(1), IR-6(2), RA-5(3), RA-5(4), RA-5(10), SA-4(2), SA-4(5), SA-4(9), SA-9(1), SA-10(1), SA-11(2), SA-11(7), SA-15(7), GMP5_6.2.5.1.
ISO/IEC 27001:2013 €	C.6.1	ISO2701_C6.1.3	ISO2701_C6.1.3 Information security risk treatment	**6.1.3 Information security risk treatment** The organization shall define and apply information security *and privacy* risktreatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source. *b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted.* *When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives, and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.* c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to	**ISO/IEC 27701:2019(E) 5.4.1.3 Information security risk treatment** The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions: ISO/IEC 27001:2013, 6.1.3 c) is refined as follows: The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted. When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals. ISO/IEC 27001:2013, 6.1.3 d) is refined as follows: Produce a Statement of Applicability that contains:	<blank>	<blank>	A.12.6.1, A.18.2.1, A.12.7.1, A.16.1.4, CA-2(2), CA-9(1), CM-6(1), CM-7(1), CM-8(1), CM-8(4), CM-9(1), PM-5(1), IR-6(2), RA-5(3), RA-5(4), RA-5(10), SA-4(2), SA-4(5), SA-4(9), SA-9(1), SA-10(1), SA-11(2), SA-11(7), SA-15(7), GMP5_6.2.5.1.
ISO/IEC 27001:2013 €	C.7.5	ISO2701_C7.5.1	ISO2701_C7.5.1 General - Documented information	**7.5.1 General - Documented information** The organization's information security *and privacy* management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of theprivacy information management system (PIMS). NOTE The extent of documented information for aprivacy information management system (PIMS) can differ from one organization to another due to: 1) the size of the organization and its type of activities, processes, products, and services; 2) the complexity of processes and their interactions; and 3) the competence of persons	**ISO/IEC 27701:2019(E) 5.5.5.1 General** The requirements stated in **ISO/IEC 27001:2013, 7.5.1** along with the interpretation specified in 5.1, apply. ISO/IEC 27018:2019(E) 12.1 Operational procedures and responsibilities The objective specified in **ISO/IEC27002:2013, 12.1** applies. Pay special note to the required adjustments necessary to key operational procedures, namely: ISO/IEC 27018:2019(E) 12.3.1 Information backup ...	<blank>	<blank>	A.12.1.1, ISO13485_7.5.1, CM-3(1), CM-3(2), SA-8(29), SA-8(32), SA-15(11), 11.10(k), EU11_4.1_VAL, EU11_4.2_VAL, EU11_4.5_VAL, HT_4.a, GMP5_4.2.5.5, GMP5_4.4.3, GMP5_ADX_D5-4.2.1, P003 6
						<blank>		HT_6.b, HT_6.d, HT_6.e, HT_6.f, GMP5_ADX_O11-4.3.1, GMP5_ADX_O11-4.3.2, GMP5_ADX_O11-4.3.3, GMP5_ADX_O11-4.3.4, 11.10(j), 11.30, ISO27701_6.2.1
ISO/IEC 27002:2013 €	A.6.1	A.6.1.1	A.6.1.1 Information security roles and responsibilities	**Policy:** Allocation of information security *and privacy* responsibilities is done in accordance with the information security AND PRIVACY policies (see clause 5.1.1). Responsibilities for the protection of individual assets and for carrying out specific information security processes are managed through the Information Asset Owner Procedures as detailed in the Computer Operations Narrative and in all distribution and collection of end user computing assets related to standard operating procedures (SOP) within IT Support. End-user computing is further governed by the Acceptable Use Policy that is distributed as a part of the annual Security AND PRIVACY Awareness Training (SAT). All Assets are classified according to the type of Application, Infrastructure, Product/Service, or Networking Device, are rated for their Disclosure Impact or Data Sensitivity, and assigned Information Asset Owner (IAO) for Product, Administration, Delegation, Development, and Support. Responsibility for annual refresh and communication of IAO is determined by Enterprise Compliance (EC) as a function of the integrated audit. Business Units, or supervisory organization, are responsible for communication and management of assets. They are required, as part of the audit and annual Business Impact Analysis (BIA), to record the asset's purpose, intended use, and classification. Determination of responsibility for information security risk management activities and for acceptance of residual risks are part of the Enterprise Risk Management process and Security AND PRIVACY Risk Assessment Process. These responsibilities may be supplemented with more detailed guidance for specific sites and information processing facilities. End-user responsibilities for the protection of assets and for carrying out specific security processes are	**ISO/IEC 27018:2019(E) 6.1.1 Information security roles and responsibilities** Control 6.1.1 and the associated implementation guidance and other information specified in ISO/ IEC27002 apply. The following sector-specific guidance also applies. *Public cloud PII protection implementation guidance* *The public cloud PII processor should designate a point of contact for use by the cloud service customer regarding the processing of PII under the contract.* ---------- **ISO/IEC 27701:2019(E) 6.3.1.1 Information security roles and responsibilities**	**Other ISO/IEC 27017:2015 (E) information for cloud** Even when responsibilities are determined within a [illegible] the parties, the cloud customer is accountable for the decision to use [illegible] decision should be made according to the roles and responsibilities determined within the cloud service customer's organization. The cloud service provider is accountable for information security stated as part of the cloud service agreement. The information security implementation and provisioning should be made according to the roles and responsibilities determined within the cloud service provider's organization. Ambiguity in roles and in the definition and allocation of responsibilities related to issues such as data ownership, access control, and infrastructure maintenance, can give rise to business or legal disputes, especially when dealing with third parties. Data and files on the cloud service provider's systems that are created or modified during the use of the cloud service can be critical to the secure operation, recovery and continuity of the service.	The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.	HT_2.a, HT_2.d, HT_2.e, HT_2.f, GMP5_ADX_M-5.3.3, GMP5_ADX_M10-3.2.2, GMP5_ADX_O2-4.4.3, GMP5_6.1.2, GMP5_6.1.4, ISO27701_6.3.1

ata Security & Privacy Lifecycle Management	Personal Data Sub-processing	**DSP-13**	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	**No Mapping**	**Full Gap** The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.

Full Gap The full V4 control specification is missing from the ISOs and has to be used to close the gap.

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

Updates to NIST SP800-53 changed the schema in DECEMBER 2020

EnterpriseGRC Solutions, Inc.

NIST

Search CSRC | CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PUBLICATIONS SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

SP 800-53 Rev. 5

Security and Privacy Controls for Information Systems and Organizations

Date Published: September 2020 (Includes updates as of Dec. 10, 2020)

Supersedes: SP 800-53 Rev. 5 (09/23/2020)

Planning Note (1/22/2021):

See the Errata (beginning on p. xvii) for a list of updates to the original publication.

New supplemental materials are also available:

- **Control Catalog Spreadsheet** (NEW)
  The entire security and privacy control catalog in spreadsheet format. *Note: For a spreadsheet of control baselines, see the SP 800-53B details.*

- **Analysis of updates between 800-53 Rev. 5 and Rev. 4** (Updated 1/22/21)
  Describes the changes to each control and control enhancement, provides a brief summary of the changes, and includes an assessment of the significance of the changes. *Note that this comparison was authored by T… Corporation for the Director of National Intelligence (DNI) and is being shared with permission by DNI.*

- **Mapping of Appendix J Privacy Controls (Rev. 4) to Rev. 5**
  Supports organizations using the privacy controls in Appendix J of SP 800-53 Rev. 4 that are transitioning to the integrated control catalog in Rev. 5.

- **Mappings between 800-53 Rev. 5 and other frameworks and standards** (NIST Cybersecurity Framework and NIST Privacy Framework; ISO/IEC 27001 [updated 1/22/21])
  The mappings provide organizations a general indication of SP 800-53 control coverage with respect to other frameworks and standards. When leveraging the mappings, it is important to consider the intended scope of each publication and how each publication is used; organizations should not assume equivalency based solely on the mapping tables because mappings are not always one-to-one and there is a degree of subjectivity in the mapping analysis.

Also available:

- **Security and Privacy Control Collaboration Index Template** (Excel & Word)
  The collaboration index template supports information security and privacy program collaboration to help ensure that the objectives of both disciplines are met and that risks are appropriately managed. It is an optional tool for information security and privacy programs to identify the degree of collaboration needed between security and privacy programs

DOCUMENTATION

Publication:
SP 800-53 Rev. 5 (DOI)
Local Download

Supplemental Material:
Control Catalog (spreadsheet) (xls)
Analysis of updates between 800-53 Rev. 5 and … by MITRE Corp. for ODNI (xls)
Mapping: Appendix J Privacy Controls (Rev. 4) to Rev. 5 (xls)
Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5 (xls)
Mapping: Rev. 5 to ISO/IEC 27001 (word)
OSCAL Version of Rev. 5 controls (web)
Control Collaboration Index Template (xls)
Control Collaboration Index Template (word)
Blog post (web)

Other Parts of this Publication:
SP 800-53B

Document History:
12/10/20: SP 800-53 Rev. 5 (Final)

TOPICS

Security and Privacy
privacy controls; security controls; security programs & operations

Laws and Regulations
E-Government Act; Federal Information Security Modernization Act; Homeland Security Presidential

B1176 | Provenance | Supply Chain Integrity — Pedigree

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
SR-4	Provenance				Y	New base control	Document, monitor, and maintain valid provenance … systems, system components, and associated data and associated data
SR-4(1)	Provenance | Identity				Y	New control enhancement	Establish and maintain unique identification of spec… chain elements, processes, and personnel associate… identified system and critical system components Incorporates withdrawn control SA-12(14)
SR-4(2)	Provenance | Track and Trace				Y	New control enhancement	Establish and maintain unique identification of spec… and critical system components for tracking throug… chain Incorporates withdrawn control SA-12(14)
SR-4(3)	Provenance | Validate As Genuine and Not Altered				Y	New control enhancement	Employ specified controls to validate that the syste… component received is genuine and has not been alt… Incorporates withdrawn control SA-12(10)
SR-4(4)	Provenance | Supply Chain Integrity — Pedigree				Y	New control enhancement	Employ specified controls and conduct specified a… ensure the integrity of the system and system comp… validating the internal composition and provenance… mission-essential technologies, products, and servi…
SR-5	Acquisition Strategies, Tools, and Methods	X	X	X	Y	New base control Adds to L, M, and H Security Control Baselines (SP 800-53B)	Employ specified acquisition strategies, contract t… procurement methods to protect against, identify, … supply chain risks Incorporates withdrawn control SA-12(1)
SR-5(1)	Acquisition Strategies, Tools, and Methods | Adequate Supply				Y	New control enhancement	Employ specified controls to ensure an adequate su… critical system components Incorporates withdrawn control SA-12(6)
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 compone… system services prior to selection, acceptance, mod… update. Incorporates withdrawn control SA-12(7)
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 as… suppliers or contractors and the system, system co… system service they provide Incorporates withdrawn control SA-12(2)
SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis				Y	New control enhancement	Employ specified analysis or testing of specified su… elements, processes, and actors associated with th… system component, or system service Incorporates withdrawn control SA-12(11)
SR-7	Supply Chain Operations Security				Y	New base control	Employ specified OPSEC controls to protect supp… related information Incorporates withdrawn control SA-12(3)
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 i… supply chain Incorporates withdrawn control SA-12(12)
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 protecti… Incorporates withdrawn control SA-18
SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development Life			X	Y	New control enhancement Adds to H Security Control Baseline (SP 800-53B)	Employ anti-tamper technologies, tools, and techni… throughout the system development life cycle Incorporates withdrawn control SA-18(1)
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… tampering Incorporates withdrawn control SA-18(2)
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-… policy and procedures, to include reporting counte… components Incorporates withdrawn control SA-19
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 counte… components Incorporates withdrawn control SA-19(1)
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 syste… components awaiting service or repair and serviced… components awaiting return to service Incorporates withdrawn control SA-19(2)
SR-11(3)	Component Authenticity | Anti-				Y	New control enhancement	Periodically scan for counterfeit system component

Introduction | Legend | Rev4 Rev5 Compared

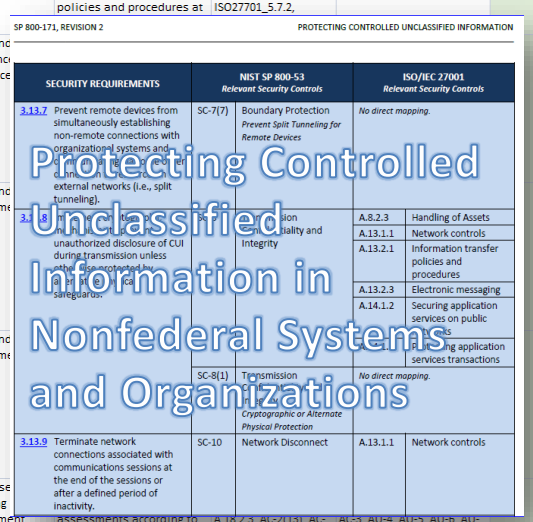
		MP-3	_To be deleted
		IR-4	_To be deleted
		SR3-5-6	_To be deleted
		SR-9-11	_To be deleted
		SR-12-11	_To be deleted
		withdrawn	_To be deleted
		PT-2	_To be deleted
		PT-3	_To be deleted
		T-2	_To be deleted
		T-1	_To be deleted
		T-4->PT-6	_To be deleted
		T-5	_To be deleted
		T-7	_To be deleted
	->IP-6 Individual Access	IP-6->PT-6	_To be deleted
	->PA-1 Privacy Authorization Policy and Procedures	PA-1->PT-1	_To be deleted
○	->PA-4 Information Sharing with External Parties	PA-4->PT-4	_To be deleted

NIST 171 r2 and NIST 172 use NIST 800-53 v5 as Parent/Family

EnterpriseGRC Solutions, Inc.

Assessment Universe.Domain ID	Assessment Universe.Edition or Source	Assessment Universe.Control ID	Assessment Universe.Test ID	Assessment Universe.Control Objective	Assessment Universe.Control Objective Description	Assessment Universe.Unified Testing Map	Assessment Universe.Unified Universe Mapping	Assessment Universe.Unified Universe Mapping.Value	Assessment Universe_1.Edition or Source	Assessment Universe_1.Control Objective
CCM_A&A	CCM v4.0 Cloud Security Alliance © 2021	A&A-01	A&A-01.1, A&A-01.2	Audit and Assurance Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at	ISO2701_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(6), SA-11(7), HT_6.g, HT_6.i, HT_13.s, 11.6.0 RMTN, ISO27701_5.2.3, ISO27701_5.7.2,	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, HT_13.07, ISO27701_5.2, ISO27701_5.7, CC1.1, CC1.2, CC1.3, 11_RMTN, CC3.1, SA-11	SA-4	NIST 800-53 r5	SA-4 Acquisition Process
CCM_A&A	CCM v4.0 Cloud Security Alliance © 2021	A&A-01	A&A-01.1, A&A-01.2	Audit and Assurance and Proce					NIST 800-53 r5	SA-11 Developer Security Testing and Evaluation
CCM_A&A	CCM v4.0 Cloud Security Alliance © 2021	A&A-02	A&A-02.1	Independ Assessme					NIST 800-53 r5	CA-2 Assessments
CCM_A&A	CCM v4.0 Cloud Security Alliance © 2021	A&A-02	A&A-02.1	Independ Assessme					NIST 800-53 r5	CA-7 Continuous Monitoring
CCM_A&A	CCM v4.0 Cloud Security Alliance © 2021	A&A-03	A&A-03.1	Risk Base Planning Assessment	assessments 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-	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-12, AU-13, AU-14, AU-16, CA-7, HT_06.03, HT_09.10 N171_3.1, N171_3.3, ISO27701_5.7, ISO27701_6.15, CC1.1, CC1.2,		NIST 800-53 r5	AC-2 Account Management
CCM_A&A	CCM v4.0 Cloud Security Alliance © 2021	A&A-03	A&A-03.1	Risk Based Planning Assessment	Perform independent audit and assurance assessments 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-	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-12, AU-13, AU-14, AU-16, CA-7, HT_06.03, HT_09.10 N171_3.1, N171_3.3, ISO27701_5.7, ISO27701_6.15, CC1.1, CC1.2,	AC-3	NIST 800-53 r5	AC-3 Access Enforcement

Control ID	Domain ID	Control Objective	Edition or Source	Control Objecti...	PROTECT...	Test ID	External Resource	Unified Universe Mapping
N171_3.1	AC 800-53-R5	N171_3.1 Access Control	NIST 800-171 r2	3.1 ACCESS CONTROL		N171_3.1.1; N17...	NIST SP 800-171 rev 2	AC-2; AC-3; AC-4; AC-5; AC-6; AC-7; AC-8; AC-11; AC-12; AC-17; AC-18; AC-19; AC-20
N171_3.2	AT 800-53-R5	N171_3.2 Awareness and Training	NIST 800-171 r2	3.2 AWARENESS AN...		N171_3.2.1; N17...	NIST SP 800-171 rev 2	AT-2; AT-3; A.7.2; A.12.2
N171_3.3	AU 800-53-R5	N171_3.3 Audit and Accountability	NIST 800-171 r2	3.3 AUDIT AND ACC...		N171_3.3.1; N17...	NIST SP 800-171 rev 2	AU-2; AU-3; AU-5; AU-6; AU-7; AU-8; AU-9; A.12.4; A.16.1; A.18.1; A.12.7
N171_3.4	CM 800-53-R5	N171_3.4 Configuration Manage...	NIST 800-171 r2	3.4 CONFIGURATION...		N171_3.4.1; N17...	NIST SP 800-171 rev 2	CM-2; CM-3; CM-4; CM-5; CM-6; CM-7; CM-8; CP-11; A.8.1; A.9.2; A.9.4; A.12.1; A.12.5
N171_3.5	IA 800-53-R5	N171_3.5 Identification and Auth...	NIST 800-171 r2	3.5 IDENTIFICATION ...		N171_3.5.1; N17...	NIST SP 800-171 rev 2	IA-2; IA-4; IA-5; IA-6; A.9.2; A.9.3; A.9.4
N171_3.6	IR 800-53-R5	N171_3.6 Incident Response	NIST 800-171 r2	3.6 INCIDENT RESPO...		N171_3.6.1; N17...	NIST SP 800-171 rev 2	IR-2; IR-3; IR-4; IR-5; IR-6; IR-7; A.6.1; A.7.2; A.16.1
N171_3.7	MA 800-53-R5	N171_3.7 Maintenance	NIST 800-171 r2	3.7 MAINTENANCE		N171_3.7.1; N17...	NIST SP 800-171 rev 2	MA-2; MA-3; MA-4; MA-5; A.11.2
N171_3.8	MP 800-53-R5	N171_3.8 Media Protection	NIST 800-171 r2	3.8 MEDIA PROTECTI...		N171_3.8.1; N17...	NIST SP 800-171 rev 2	CP-9; MP-2; MP-3; MP-4; MP-5; MP-6; MP-7
N171_3.9	PS 800-53-R5	N171_3.9 Personnel Security	NIST 800-171 r2	3.9 PERSONNEL SEC...		N171_3.9.1; N17...	NIST SP 800-171 rev 2	PS-3; PS-4; PS-5; A.10.1; A.7.1; A.7.3; A.8.1
N171_3.10	PE 800-53-R5	N171_3.10 Physical Protection	NIST 800-171 r2	3.10 PHYSICAL PROT...		N171_3.10.1; N1...	NIST SP 800-171 rev 2	PE-2; PE-3; PE-5; PE-6; PE-17; A.6.2; A.11.1; A.11.2; A.13.2
N171_3.11	RA 800-53-R5	N171_3.11 Risk Assessment	NIST 800-171 r2	3.11 RISK ASSESSMENT		N171_3.11.1; N1...	NIST SP 800-171 rev 2	RA-3; RA-5; A.12.6
N171_3.12	CA 800-53-R5	N171_3.12 Security Assessment	NIST 800-171 r2	3.12 SECURITY ASSES...		N171_3.12.1; N1...	NIST SP 800-171 rev 2	CA-2; CA-5; CA-7; A.14.2; A.18.2
N171_3.13	SC 800-53-R5	N171_3.13 System and Communi...	NIST 800-171 r2	3.13 SYSTEM AND C...		N171_3.13.1; N1...	NIST SP 800-171 rev 2	SA-8; SC-2; SC-4; SC-7; SC-8; SC-10; SC-12; SC-13; SC-15; SC-18; SC-23; SC-28
N171_3.14	SI 800-53-R5	N171_3.14 System and Informati...	NIST 800-171 r2	3.14 SYSTEM AND IN...		N171_3.14.1; N1...	NIST SP 800-171 rev 2	SI-2; SI-3; SI-4; SI-5; A.6.1; A.12.2; A.12.6; A.14.2; A.16.1


SP 800-171, REVISION 2 — PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

SECURITY REQUIREMENTS	NIST SP 800-53 Relevant Security Controls		ISO/IEC 27001 Relevant Security Controls	
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and [illegible] external networks (i.e., split tunneling).	SC-7(7)	Boundary Protection *Prevent Split Tunneling for Remote Devices*	*No direct mapping.*	
3.13.8 [illegible] unauthorized disclosure of CUI during transmission unless otherwise protected by [illegible] safeguards.	SC-8	Transmission Confidentiality and Integrity	A.8.2.3	Handling of Assets
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.13.2.3	Electronic messaging
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
	SC-8(1)	Transmission Confidentiality and Integrity *Cryptographic or Alternate Physical Protection*	*No direct mapping.*	
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SC-10	Network Disconnect	A.13.1.1	Network controls

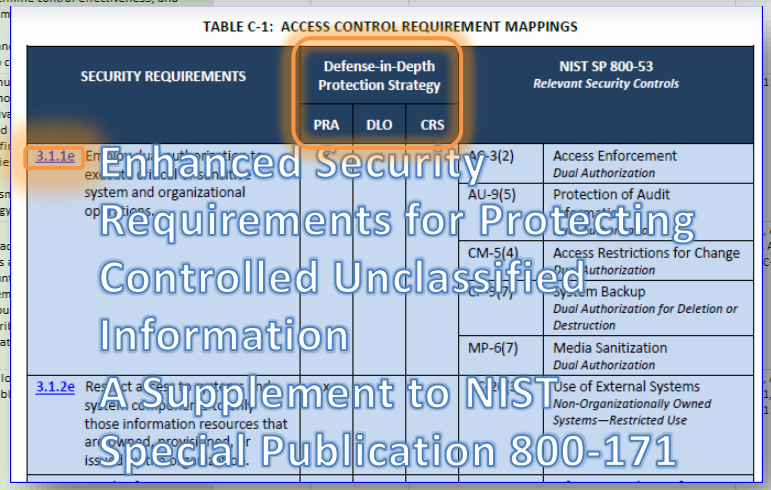


TABLE C-1: ACCESS CONTROL REQUIREMENT MAPPINGS

SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy PRA	DLO	CRS	NIST SP 800-53 Relevant Security Controls	
3.1.1e [illegible] system and organizational [illegible]				AC-3(2)	Access Enforcement *Dual Authorization*
				AU-9(5)	Protection of Audit [illegible] *Dual Authorization*
				CM-5(4)	Access Restrictions for Change *Dual Authorization*
				CP-9(7)	System Backup *Dual Authorization for Deletion or Destruction*
				MP-6(7)	Media Sanitization *Dual Authorization*
3.1.2e [illegible] those information resources that [illegible]				SA-9(5)	Use of External Systems *Non-Organizationally Owned Systems—Restricted Use*

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Enhanced Security Requirements for Protecting Controlled Unclassified Information

A Supplement to NIST Special Publication 800-171

https://doi.org/10.6028/NIST.SP.800-172 https://doi.org/10.6028/NIST.SP.800-171r2

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; MONITOR 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; TR
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; PERMISSIONS; 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 a...	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
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) 800-53 rev 5 - ...		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 cryptog...	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.13.2; CA-3; SC-7 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
N171_3.1.15 Authorize remo...	N171_3.1	NIST 800-171 r2	NIST800-53...	Add A.13.2.1;		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.13.1		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 connect ...	N171_3.1	NIST 800-171 r2	NIST800-53...	FIX THIS - includes the ...		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 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 AGREEMENTS; PROCESSING AGREEMENTS; MOU; SECURITY ASSESSMENT; EXTERNAL S
N171_3.1.21 Limit use of org...	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 of ...	SOCIAL MEDIA; 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 DU...	PHISHING; MALICIOUS; PRACTICAL EXERCISES; PRIVACY; INSIDER THREAT; INDICATORS; INAPP

Polling Question

Identify "Why" something maps and expose sufficient scoping attributes to determine *if* that control is relevant to a business domain or product.

EnterpriseGRC Solutions, Inc.

DSP-13	No Mapping	CCM v4.0 ...	Personal Data Sub-processing	ISO27001/27002/...	Full CCMv4 ISO Gap	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	DSP-13.1	CCM_DSP-13.1 Are processes, procedures and technical measures defined, implemented and evaluated, for the transfer and sub-processing of personal data within the service supply chain, and according to any applicable laws and regulations?	A.15.1.2; A.18.1.4; CP-4(2); IR-4(10); IR-6(3); PT-3(1); PT-6(2); SA-9(1); SA-9(3); SI-12(1); SR-4(1); HT_5.k; HT_9.s; HT_13.a; HT_13.b; HT_13.n; ISO27701_6.12.1; ISO27701_7.3.2; ISO27701_7.3.7; ISO27701_7.3.8; ISO27701_7.4.2; ISO27701_7.4.4; ISO27701_8.2.1; ISO27701_8.5.3; ISO27701_8.5.5; ISO27701_8.5.6; CC7.4.11; CC7.4.13; CC8.1.15; P1.1.1; P2.1.1	A.15.1.2 Addressing security within supplier agreements; A.18.1.4 Privacy and protection of personally identifiable information; CP-4.2 Alternate Processing Site; IR-4.10 Supply Chain Coordination; IR-6.3 Supply Chain Coordination; PT-3.1 Data Tagging; PT-6.2 Exemption Rules; SA-9.1 Risk Assessments and Organizational Approvals; SA-9.3 Establish and Maintain Trust Relationship with Providers; SI-12.1 Limit Personally Identifiable Information Elements; SR-4.1 Identity; 05.k Addressing Security in Third Party Agreements; 09.s Information Exchange Policies and Procedures; 13.a Privacy Notice; 13.b Openness and Transparency; 13.n Participation and Redress; ISO27701_6.12.1 Information security in supplier relationships; ISO27701_7.3.2 Determining information for PII principals; ISO27701_7.3.7 PII controllers' obligations to inform third parties; ISO27701_7.3.8 Providing copy of PII processed; ISO27701_7.4.2 Limit processing; ISO27701_7.4.4 PII minimization objectives; ISO27701_8.2.1 Customer agreement; ISO27701_8.5.3 Records of PII disclosure to third parties; ISO27701_8.5.5 Legally binding PII disclosures; ISO27701_8.5.6 Disclosure of subcontractors used to process PII; CC7.4.11_Periodically Evaluates Incidents; CC7.4.13_Application of Sanctions; CC8.1.15_Protects Personal Information; P1.1.1_Communicates to Data Subjects; P2.1.1_Communicates to Data Subjects	A.15.1; A.18.1; CP-4; IR-4; IR-6; PT-3; PT-6; SA-9; SI-12; SR-4; HT_05.02; HT_09.08; HT_13.01; HT_13.05; ISO27701_6.12; ISO27701_7.3; ISO27701_7.4; ISO27701_8.2; ISO27701_8.5; CC7.4; CC8.1; P1.1; P2.1	A.15.1 Information security in supp Contingency Plan Testing; IR-4 Inci Processing Purposes; PT-6 System Retention; SR-4 Provenance; 05.02 Limitation; ISO27701_6.12 Supplier design and privacy by default; ISO and disclosure; CC7.4 The entity re program to understand, contain, re authorizes, designs, develops or ac infrastructure, data, software, and p about its privacy; P2.1 The entity c disposal of personal information to collection, use, retention
DSP-14	No Mapping	CCM v4.0 ...	Disclosure of Data Sub-processors	ISO27001/27					A.13.2.4; A.15.1.1; A.18.1.4; CP-4(2); IR-6(3); PT-6(2); SA-	A.13.2.4 Confidentiality or non-disclosure agreements; A.15.1.1 Information security policy for supplier relationships;		ISO/IEC 27018:2019(E) A.6.2 Record in supplier relationships; A.18.1 Co Incident Reporting; PT-6 System of Retention; SR-4 Provenance; 05.02 Individual Participation; 13.05 Use principals; ISO27701_7.4 Privacy by ISO27701_8.5 PII sharing, transfer, documents, tests, approves, and in objectives.; P1.1 The entity provide available regarding the collection, and the consequences, if any, of ea personal information to third parti disclosure to meet the entity's obje timely record of authorized disclos The entity creates and retains a cor (including breaches) of personal in implements a process for receiving and disputes from data subjects an
DSP-15	DSI-05	CCM v4.0 ...	Limitation of Production Data Use	ISO27001/27002/...	Partial CCMv4 ISO Gap	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	DSP-15.1	CCM_DSP-15.1 Is authorization obtained from data owners, and the associated risk managed , before replicating or using production data in non-production environments? Is the production data cleansed or reduced where possible to limit risk?	A.6.1.1; A.9.2.2; A.12.1.4; A.14.2.6; A.14.3.1; A.18.1.4; PT-4(1); PT-4(2); PT-5(1); PT-6(1); SA-3(2); HT_10.c; HT_13.a; HT_13.b; HT_13.c; HT_13.g; HT_13.h; HT_13.i; HT_13.k; HT_13.q; ISO27701_6.11.2; ISO27701_6.11.3; ISO27701_7.3.8; ISO27701_7.4.1; ISO27701_7.4.2; ISO27701_8.2.1; ISO27701_8.5.7; CC7.3.5; CC7.4.13; P1.1.1; P2.1.1; P3.2.2; P6.1.2; P6.7.1	A.6.1.1 Information security roles and responsibilities; A.9.2.2 User access provisioning; A.12.1.4 Separation of development, testing and operational environments; A.14.2.6 Secure development environment; A.14.3.1 Protection of test data; A.18.1.4 Privacy and protection of personally identifiable information; PT-4.1 Tailored Consent; PT-4.2 Just-in-time Consent; PT-5.1 Just-in-time Notice; PT-6.1 Routine Uses; SA-3.2 Use of Live or Operational Data; 10.c Control of Internal Processing; 13.a Privacy Notice; 13.b Openness and Transparency; 13.c Accounting of Disclosures; 13.g Purpose Legitimacy; 13.h Purpose Specification; 13.i Collection Limitation; 13.k Use and Disclosure; 13.q Privacy and Impact Assessment; ISO27701_6.11.2 Security in development and support processes; ISO27701_6.11.3 Test data; ISO27701_7.3.8 Providing copy of PII processed; ISO27701_7.4.1 Limit collection; ISO27701_7.4.2 Limit processing; ISO27701_8.2.1 Customer agreement; ISO27701_8.5.7 Engagement of a subcontractor to process PII; CC7.3.5_Determines Personal Information Used or Disclosed; CC7.4.13_Application of Sanctions; P1.1.1_Communicates to Data Subjects; P2.1.1_Communicates to Data Subjects; P3.2.2_Documents Explicit Consent to Retain Information–Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.; P6.1.2_Discloses Personal Information Only When Appropriate; P6.7.1_Identifies Types of Personal Information and Handling Process	A.6.1; A.9.2; A.12.1; A.14.2; A.14.3; A.18.1; PT-4; PT-5; PT-6; SA-3; HT_10.02; HT_13.01; HT_13.03; HT_13.04; HT_13.05; HT_13.07; ISO27701_6.11; ISO27701_7.3; ISO27701_7.4; ISO27701_8.2; ISO27701_8.5; ISO27018_A.3.1; CC7.3; CC7.4; P1.1; P2.1; P3.2; P6.1; P6.7	A.6.1 Internal organization; A.9.2 U Security in development and suppo requirements; PT-4 Consent; PT-5 10.02 Correct Processing in Applica Use Limitation; 13.07 Accountabilit ISO27701_7.3 Obligations to PII pri Conditions for collection and proce Public cloud PII processor's purpos resulted in a failure of the entity to such failures.; CC7.4 The entity resp program to understand, contain, re provides notice to data subjects ab collection, use, retention, disclosur any, of each choice. Explicit consen entity communicates the need for explicit consent of data subjects, a to privacy.; P6.7 The entity provide the data subjects' personal informa privacy.

Data Security & Privacy Lifecycle Management | Personal Data Sub processing | **DSP-13** | Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations. | **No Mapping** | **Full Gap** | The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.

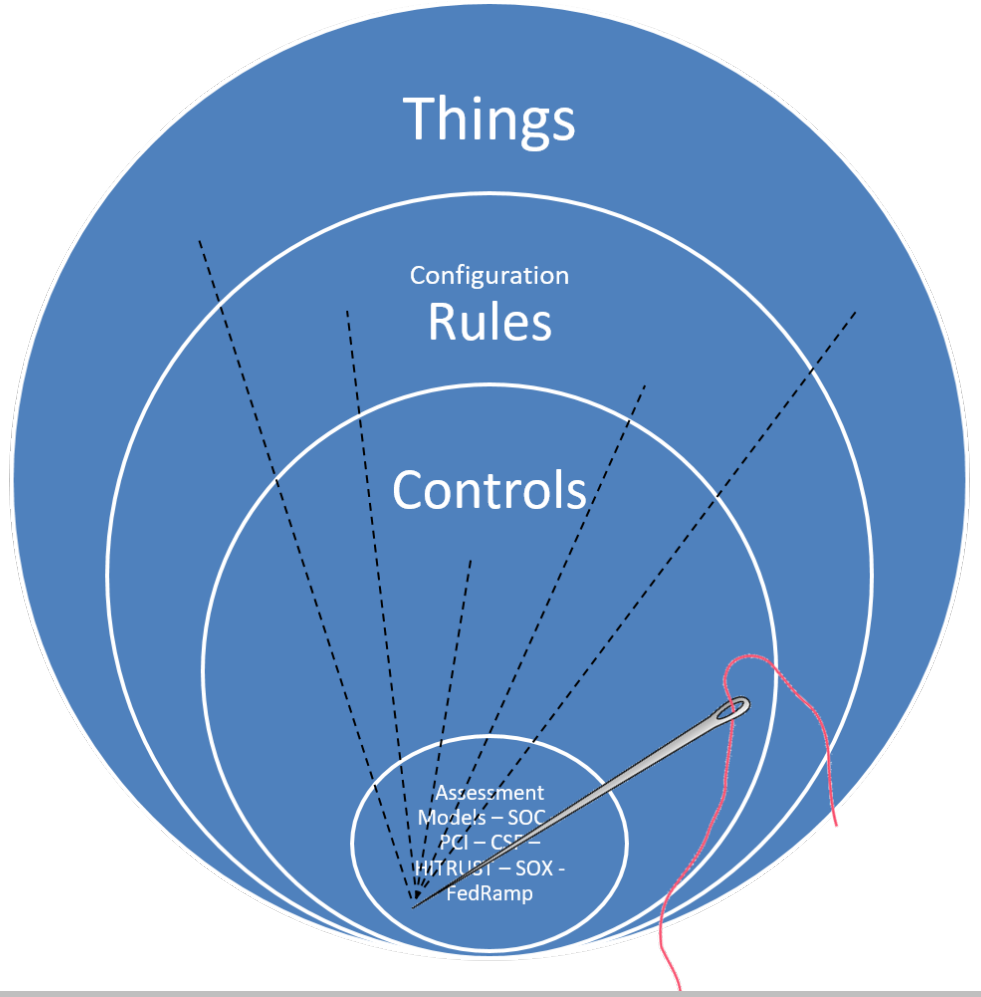
Example: DSP-13 Output should include supporting content

EnterpriseGRC Solutions, Inc.

CCM_DSP	CCM v4.0 Cloud Security Alliance © 2021	DSP-13	DSP-13.1	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable	PT-3(1), PT-6(2), SA-9(1), SA-9(3), SI-12(1), SR-4(1), HT_5.k, HT_9.s, HT_13.a, HT_13.b, HT_13.n.	ISO/IEC 27701:2019 €	ISO/IEC 27701:2019(E) 7.4.4 PII minimization objectives Control The organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives. Implementation guidance	Full CCMv4 ISO Gap	ISO27701_7.4.4
CCM_DSP	CCM v4.0 Cloud Security Alliance © 2021	DSP-13	DSP-13.1	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable	PT-3(1), PT-6(2), SA-9(1), SA-9(3), SI-12(1), SR-4(1), HT_5.k, HT_9.s, HT_13.a, HT_13.b, HT_13.n.	TSP 100—2017 Trust Services Criteria	Communicates to Data Subjects: Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.	Full CCMv4 ISO Gap	P2.1.1
CCM_DSP	CCM v4.0 Cloud Security Alliance © 2021	DSP-13	DSP-13.1	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable	PT-3(1), PT-6(2), SA-9(1), SA-9(3), SI-12(1), SR-4(1), HT_5.k, HT_9.s, HT_13.a, HT_13.b, HT_13.n.	TSP 100—2017 Trust Services Criteria	Protects Personal Information: The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.	Full CCMv4 ISO Gap	CC8.1.15
CCM_DSP	CCM v4.0 Cloud Security Alliance © 2021	DSP-13	DSP-13.1	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable	PT-3(1), PT-6(2), SA-9(1), SA-9(3), SI-12(1), SR-4(1),	ISO/IEC 27701:2019 €	ISO/IEC 27701:2019(E) 7.3.7 PII controllers' obligations to inform third parties Control The organization should inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to	Full CCMv4 ISO Gap	ISO27701_7.3.7
Data Security & Privacy Lifecycle Management		Personal Data Sub-processing	**DSP-13**	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	**No Mapping**	**Full Gap**	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	**No Mapping**	**Full Gap**	The full V4 control specification is missing from the ISOs and has to be used to close the gap.	
	Security Alliance © 2021				technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable	12(1), SR-4(1), HT_5.k, HT_9.s, HT_13.a, HT_13.b, HT_13.n.		*Required for HITRUST Certification CSF v9.3 The organization ensures that communications protection requirements, including the security of exchanges of information, is the subject of policy development (see also 04.a and 04.b) and compliance audits (see 06.g) consistent with relevant legislation. When using electronic communication applications or systems for information exchange, the following items are addressed:		
CCM_DSP	CCM v4.0 Cloud Security Alliance © 2021	DSP-13	DSP-13.1	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable	PT-3(1), PT-6(2), SA-9(1), SA-9(3), SI-12(1), SR-4(1), HT_5.k, HT_9.s, HT_13.a, HT_13.b, HT_13.n.	TSP 100—2017 Trust Services Criteria	Communicates to Data Subjects: Notice is provided to data subjects regarding the following: — Purpose for collecting personal information — Choice and consent — Types of personal information collected — Methods of collection (for example, use of cookies or other tracking techniques) — Use, retention, and disposal	Full CCMv4 ISO Gap	P1.1.1

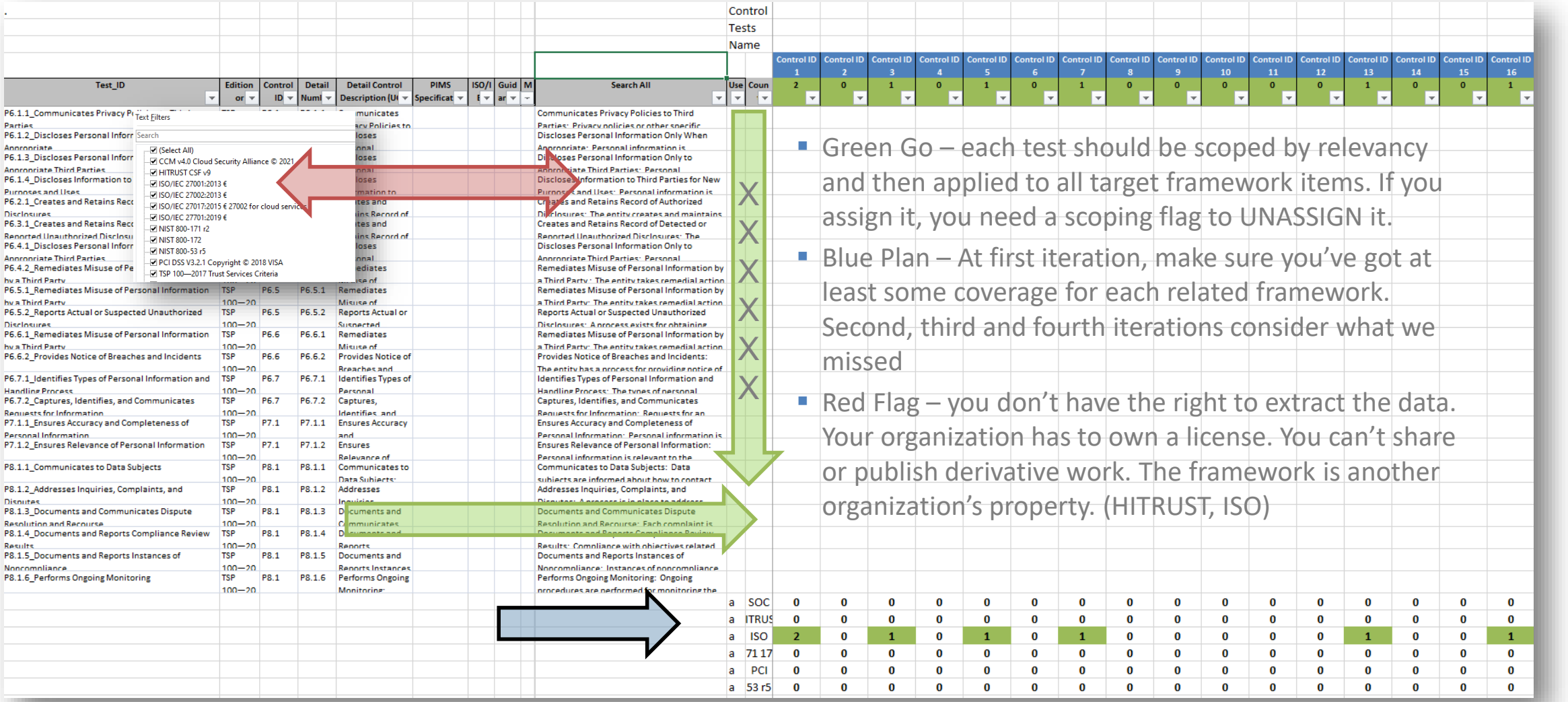
How to map

- Have a workplan
- Identify what domains should map
- Iterate
- Finalize
- Negative Map (what should have but didn't)
- Map the Missing
- QA
- Communicate



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)

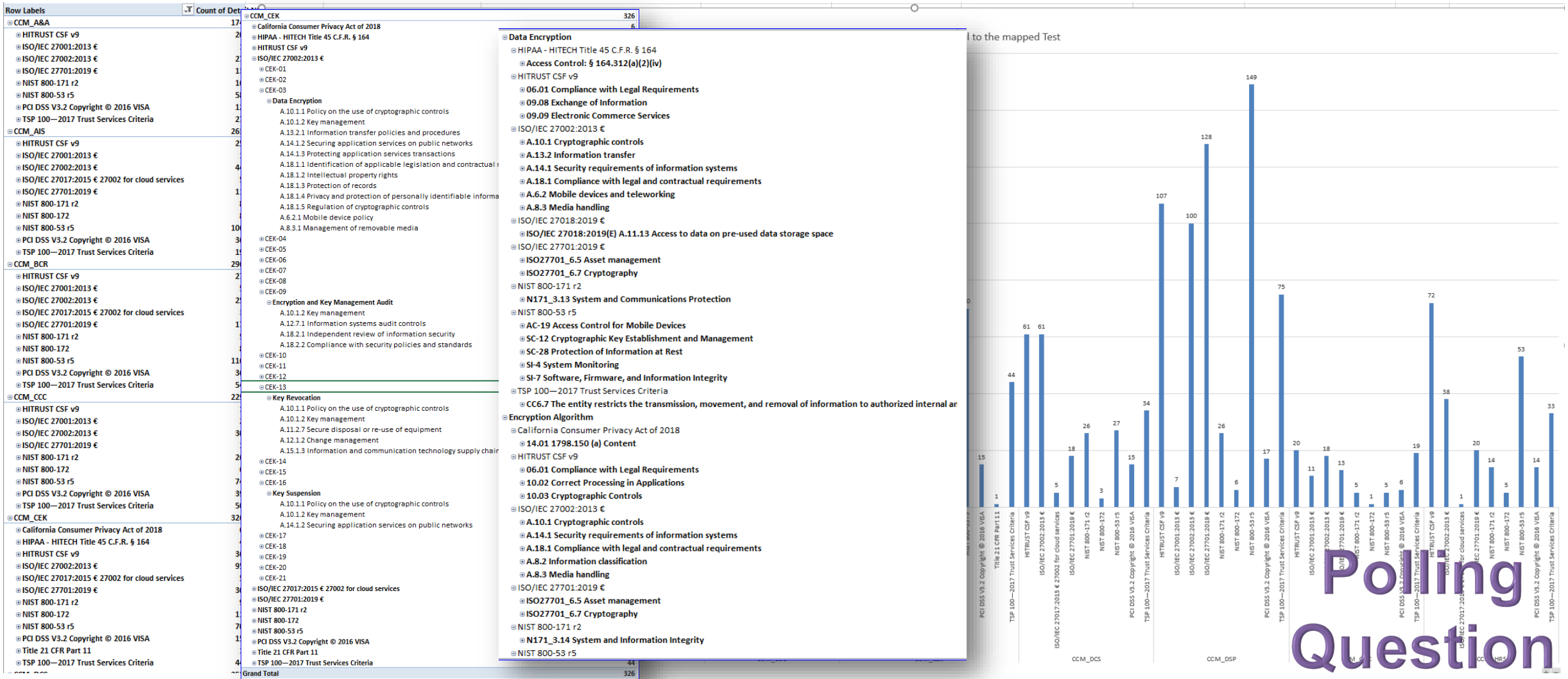
Encryption – Let's discuss

EnterpriseGRC Solutions, Inc.

Edition or Source	main ID	ntrol ID	Client ID	Control Objective	Control Objective Description	Fur p	List of policy	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 Cloud	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 [illegible] 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-

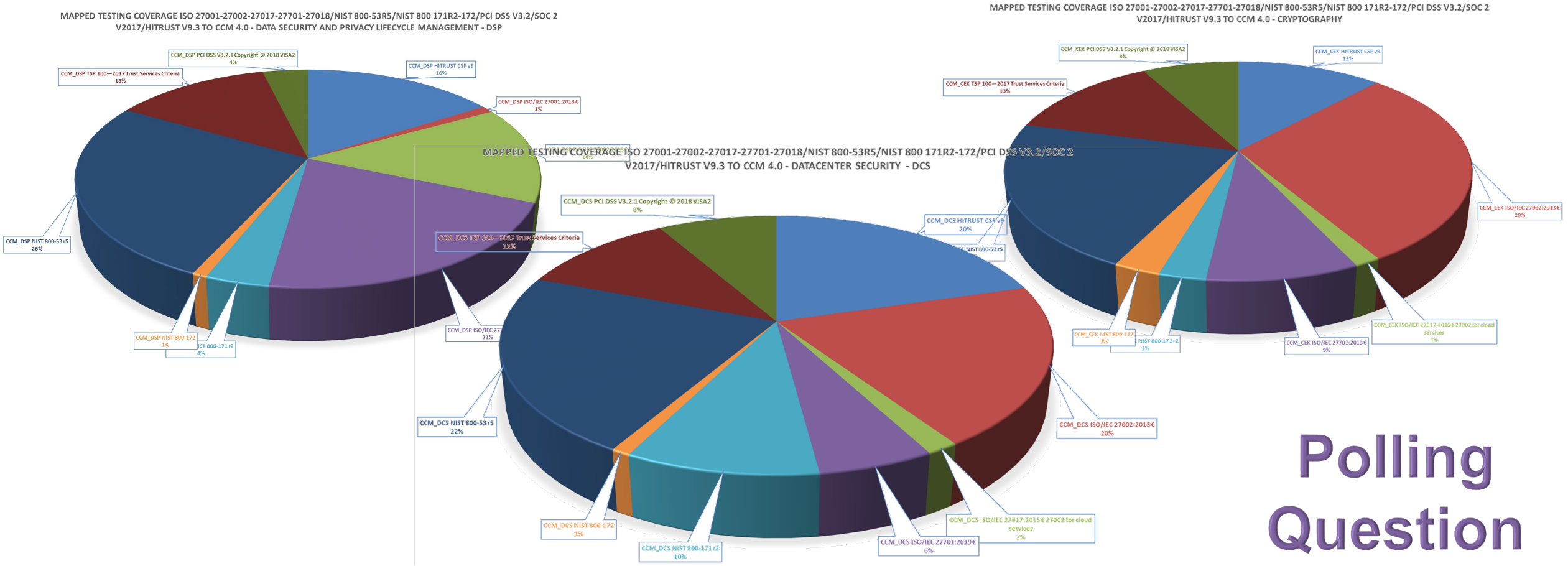
Correctly Formatted Mappings Accessible/ Usable

EnterpriseGRC Solutions, Inc.



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

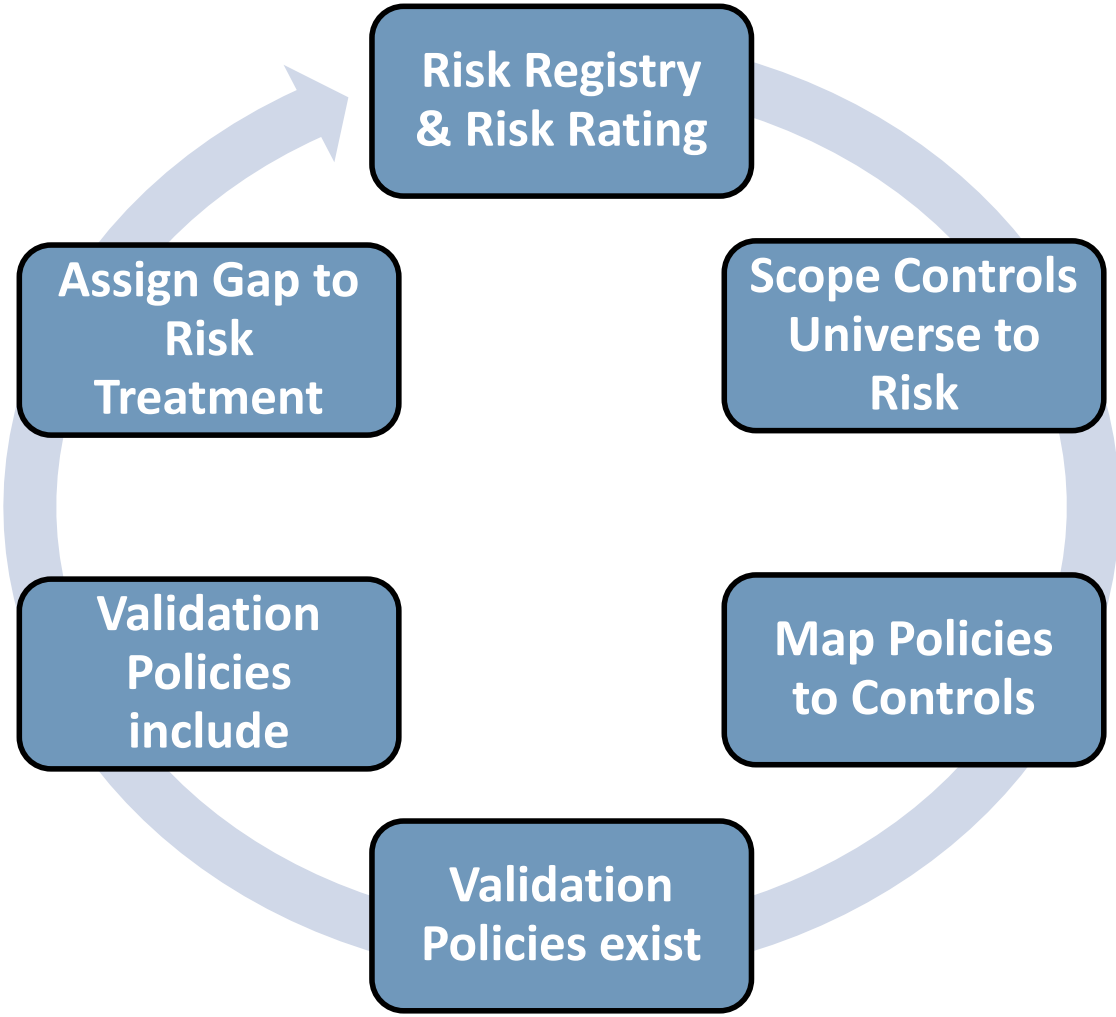
EnterpriseGRC Solutions, Inc.



Polling Question

Iterative steps Client Common Controls

- Controls map to Risks
- Control Selection affects designated coverage
- Aggregate mappings influence policy requirements
- Adding mapped controls requires policy validation, that they exist and that they include minimum expected statements
- New policy requires new risk cycle -> takes 1-2 years to fully implement

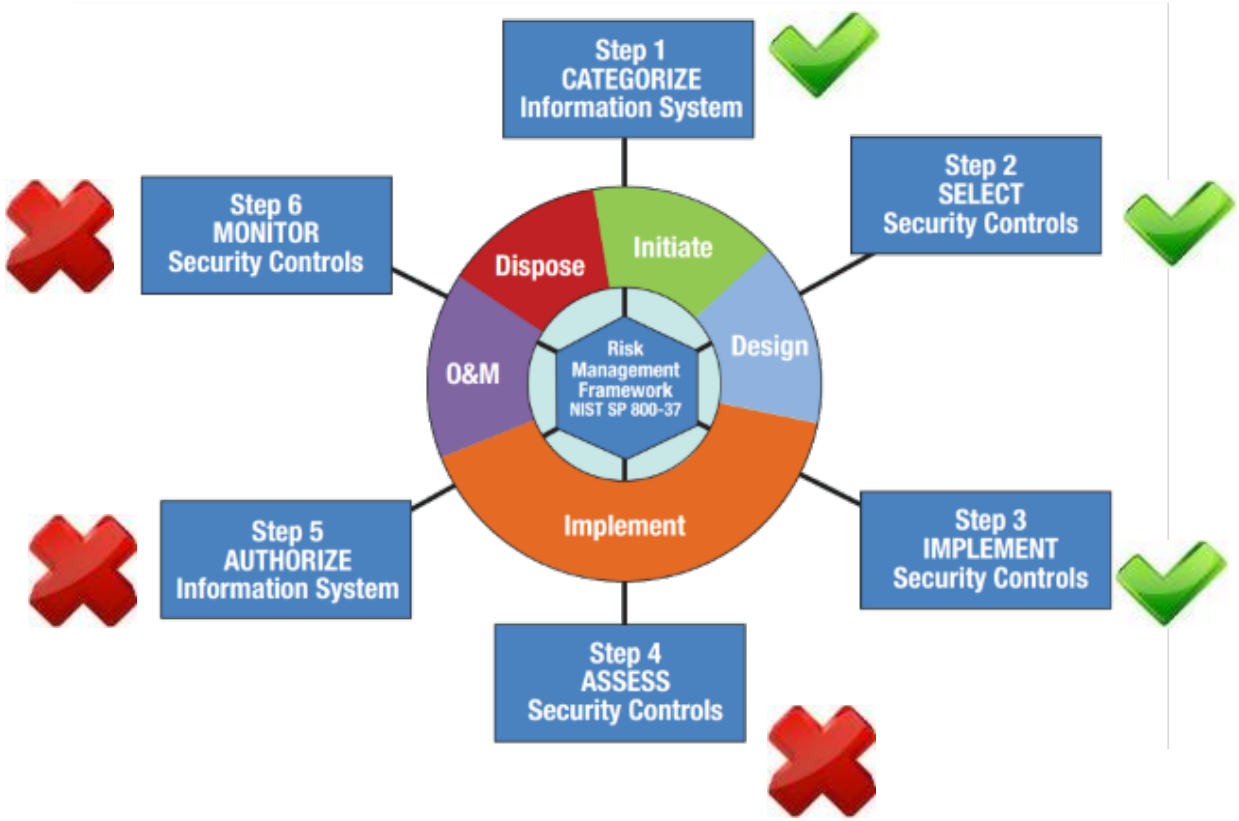


Cybersecurity Risk Management – Tie *Categories* to Risks

EnterpriseGRC Solutions, Inc.

1. Categorizing systems allows us to associate what they do to the controls they support. Categorizing Regulatory Requirements permits us to gather all necessary statements for policy.
2. Establishing a single framework and mapping policies to a common control, sets direction for what we aggregate to its policy.
3. Implementing the controls through policy institutes the low watermark for all stakeholder.
4. Assessing through policy provides same documents to different audits.

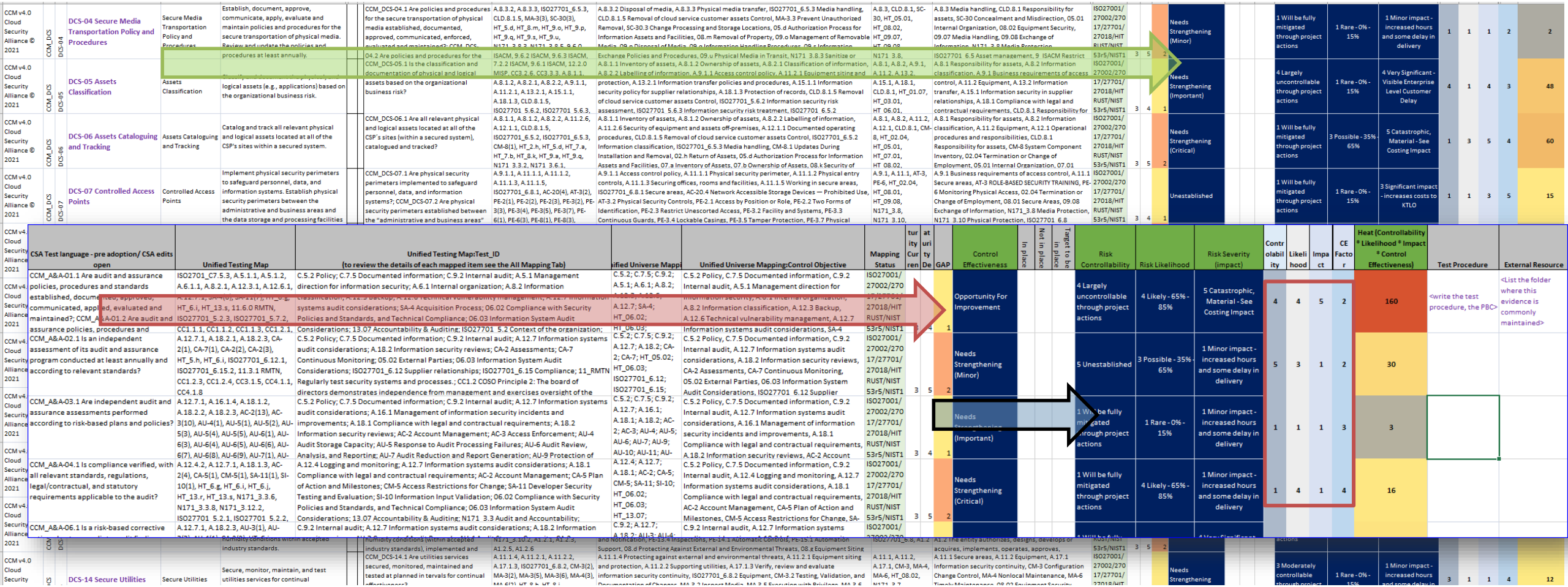
   Authorizing by context – by audit & policy
5. Monitoring provides risk feedback which allow us to add or modify to our RMF design.



RISK MANAGEMENT FRAMEWORK
NIST SP800-37

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	atu rity De	GAP	Control Effectiveness	In place	Not in place	Target to be in place	Risk Controllability	Risk Likelihood	Risk Severity (impact)	Contr olabil ity	Likeli hood	Impa ct	CE Facto r	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	ISO27001_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, A.14.2.3, 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;	A.12.4; A.12.7; A.18.1; 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; 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.

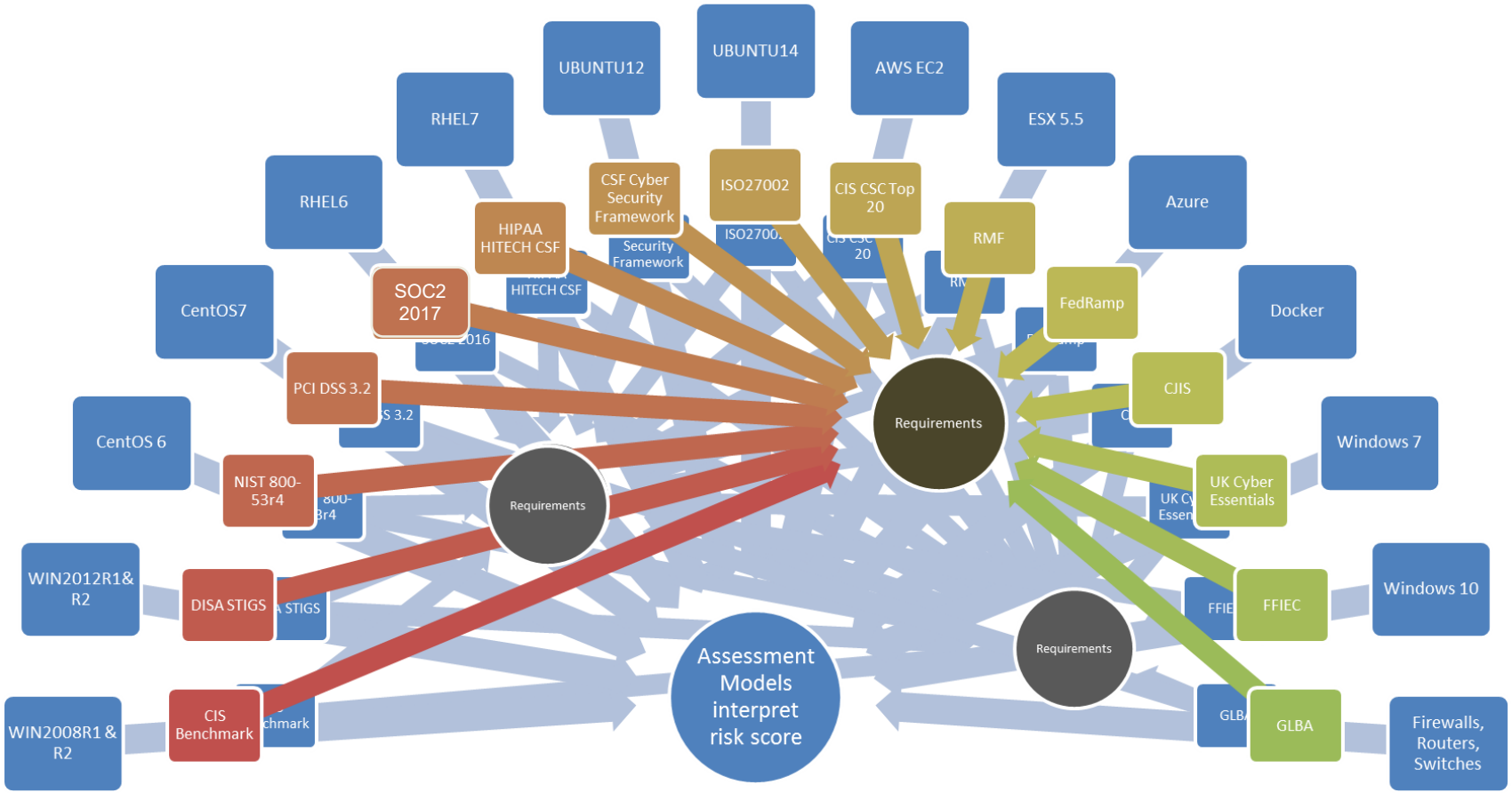
Risk Management needs to Only Handle It Once – OHIO, but capture all the inputs, players, timing, and necessary resources for improvement

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.

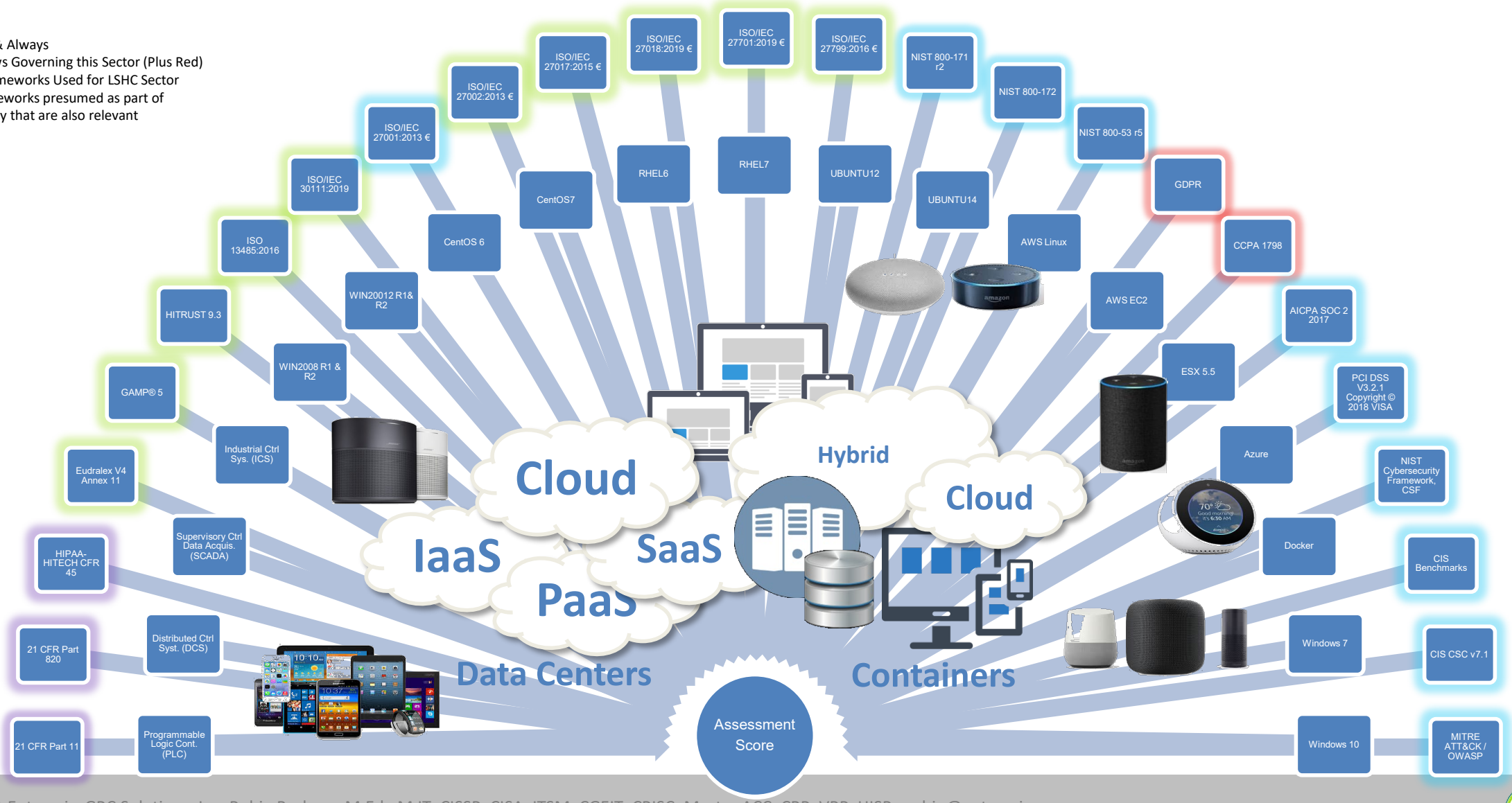
Rules run on Environments –> are tagged to controls –> are interpreted by assessment models



Imagine Regulating Federal E-Commerce Cloud Based Medical Services

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



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

EnterpriseGRC Solutions, Inc.

Assessment Testing ☆ > Cryptography

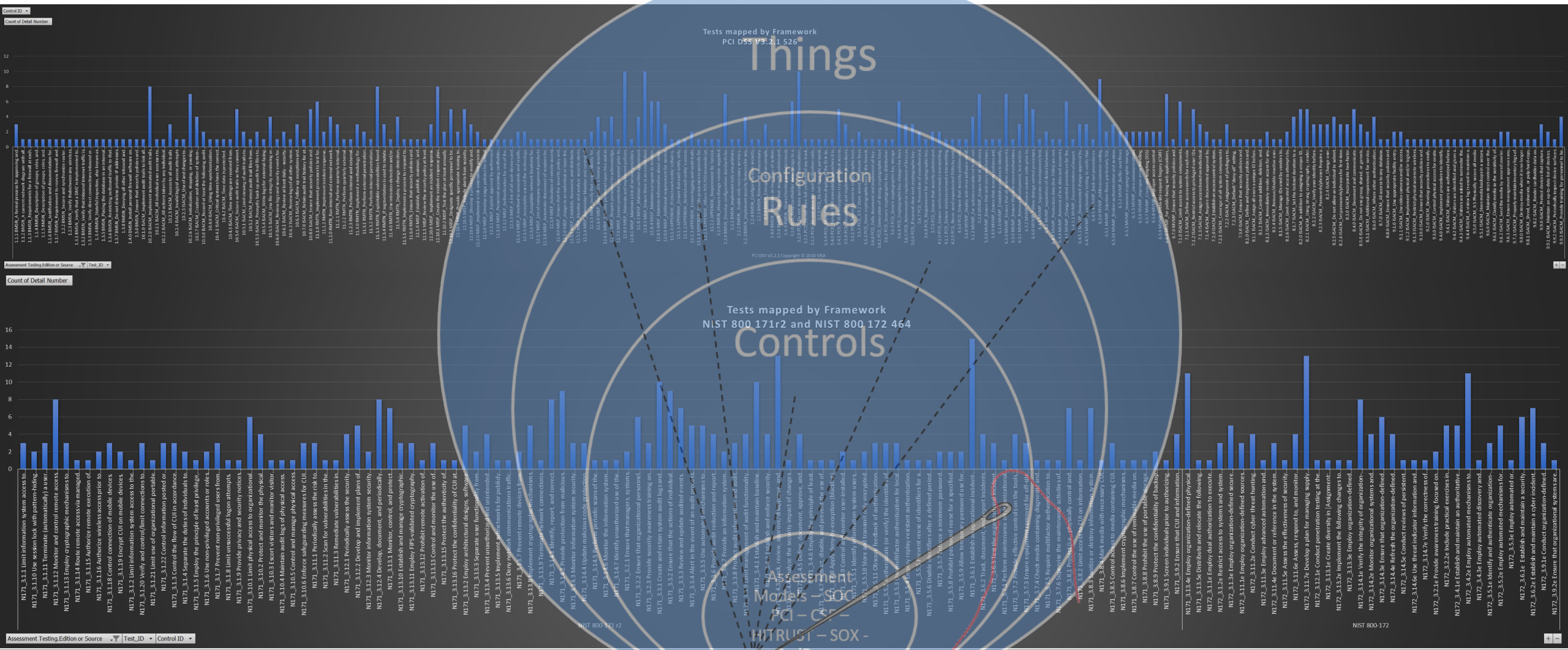
Test_ID	Mapped testi...	Mapped testing or practices:Test_ID	Mapped testing or practices:Problem Metadata	Risk Drivers	Detail Control Description (UCF)	Proble...	Mapped Proce...	Mapped Processes:
parameter store for sensitive data storage (Amazon ECS)	8(20); SC-12(3); SC-28(1); SC-28(2); SC-28(3); SI-12(2); SA-15(12); SI-19(3)	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	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 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 **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_Config ure 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 links.	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

SecurityCompass

This is an example of following this guidance.

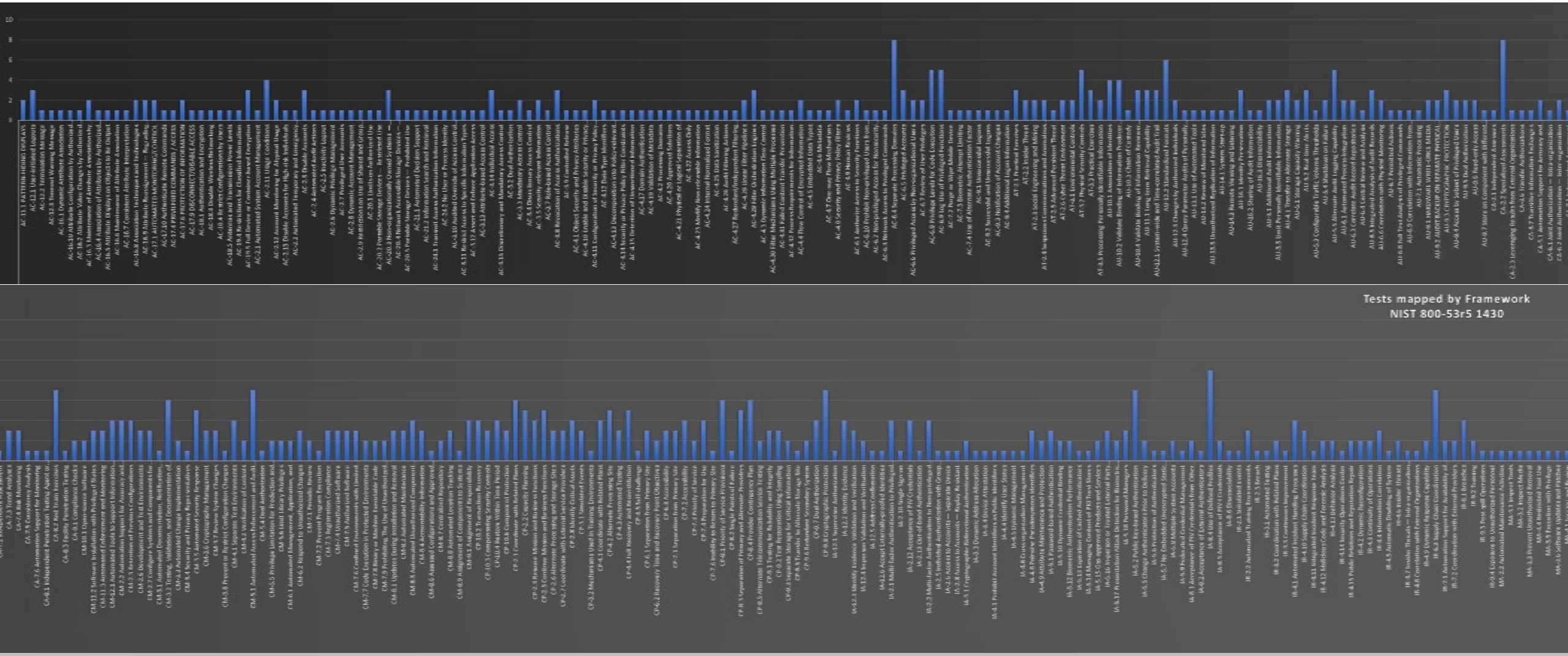
Content worthy of Data Visualization and AI – PCI, NIST-800 171+172

EnterpriseGRC Solutions, Inc.



Data Visualization and AI – NIST SP800-53r5 is a BEAST

EnterpriseGRC Solutions, Inc.



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.

Polling Question

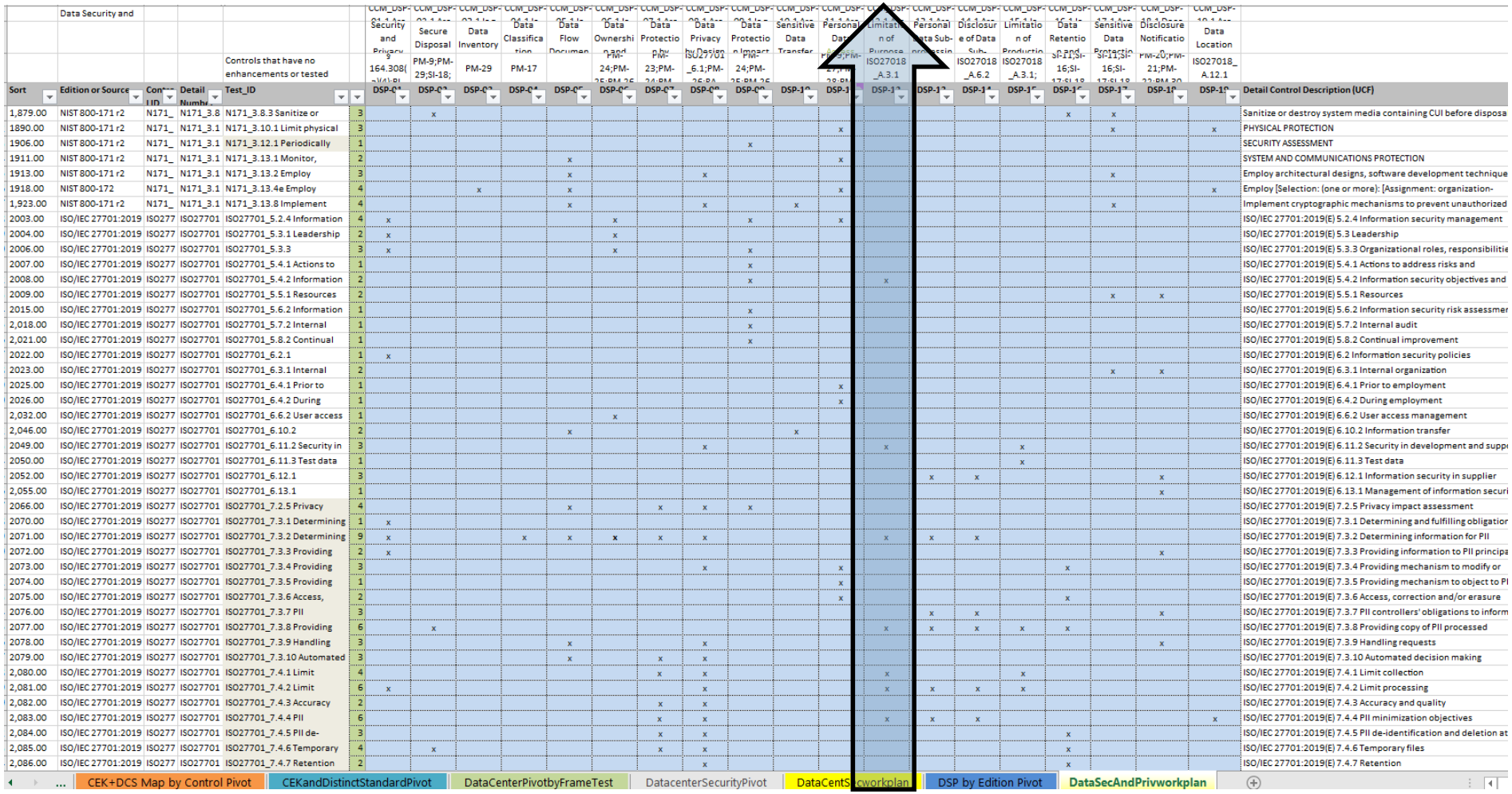

THANK YOU

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

EnterpriseGRC Solutions, Inc.

- 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.
- In some cases, meeting the goal of a control requires use of methods from other areas of a framework. In this situation, there should be a way to tag some mapping as contributing to or partially required in order to meet the objective. To use an ITIL term, they are underpinning. Control language should be refined to clarify this to reduce auditor confusion.

Mapping considers what should be covered based upon the intended outcomes for each cybersecurity framework's domain



Sort	Edition or Source	Control ID	Detail Number	Test_ID		Security and Privacy	Secure Disposal	Data Inventory	Data Classification	Data Flow Documen	Data Ownership and	Data Protection by	Data Privacy by Design	Data Protection Impact	Sensitive Data Transfer	Personal Data	Limitation of Purpose	Personal Data Sub-assessin	Disclosure of Data Sub-	Limitation of Productio	Data Retentio	Sensitive Data Protectio	Disclosure Notificatio	Data Location	Detail Control Description (UCF)
				Controls that have no enhancements or tested		164.308(	PM-9;PM-29;SI-18;	PM-29	PM-17		PM-24;PM-25;PM-26	PM-23;PM-24;PM-	ISO27701_6.1;PM-25;PM-	PM-24;PM-25;PM-26		PM-28;PM-	ISO27018_A.3.1		ISO27018_A.6.2	ISO27018_A.3.1;	SI-12;SI-16;SI-17;SI-18	SI-12;SI-16;SI-17;SI-18	PM-20;PM-21;PM-22;PM-30	ISO27018_A.12.1	
1,879.00	NIST 800-171 r2	N171_	N171_3.8	N171_3.8.3 Sanitize or	3		x														x	x			Sanitize or destroy system media containing CUI before disposa
1890.00	NIST 800-171 r2	N171_	N171_3.1	N171_3.10.1 Limit physical	3											x						x		x	PHYSICAL PROTECTION
1906.00	NIST 800-171 r2	N171_	N171_3.1	N171_3.12.1 Periodically	1									x											SECURITY ASSESSMENT
1911.00	NIST 800-171 r2	N171_	N171_3.1	N171_3.13.1 Monitor,	2					x						x									SYSTEM AND COMMUNICATIONS PROTECTION
1913.00	NIST 800-171 r2	N171_	N171_3.1	N171_3.13.2 Employ	3					x			x									x			Employ architectural designs, software development technique
1918.00	NIST 800-172	N171_	N171_3.1	N171_3.13.4e Employ	4			x		x						x								x	Employ [Selection: (one or more): [Assignment: organization-
1,923.00	NIST 800-171 r2	N171_	N171_3.1	N171_3.13.8 Implement	4					x			x		x							x			Implement cryptographic mechanisms to prevent unauthorized
2003.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.2.4 Information	4	x					x			x		x									ISO/IEC 27701:2019(E) 5.2.4 Information security management
2004.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.3.1 Leadership	2	x					x														ISO/IEC 27701:2019(E) 5.3 Leadership
2006.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.3.3	3	x					x			x											ISO/IEC 27701:2019(E) 5.3.3 Organizational roles, responsibilitie
2007.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.4.1 Actions to	1									x											ISO/IEC 27701:2019(E) 5.4.1 Actions to address risks and
2008.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.4.2 Information	2									x			x								ISO/IEC 27701:2019(E) 5.4.2 Information security objectives and
2009.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.5.1 Resources	2																	x	x		ISO/IEC 27701:2019(E) 5.5.1 Resources
2015.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.6.2 Information	1									x											ISO/IEC 27701:2019(E) 5.6.2 Information security risk assessmer
2,018.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.7.2 Internal	1									x											ISO/IEC 27701:2019(E) 5.7.2 Internal audit
2,021.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_5.8.2 Continual	1									x											ISO/IEC 27701:2019(E) 5.8.2 Continual improvement
2022.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.2.1	1	x																			ISO/IEC 27701:2019(E) 6.2 Information security policies
2023.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.3.1 Internal	2																	x	x		ISO/IEC 27701:2019(E) 6.3.1 Internal organization
2025.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.4.1 Prior to	1											x									ISO/IEC 27701:2019(E) 6.4.1 Prior to employment
2026.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.4.2 During	1											x									ISO/IEC 27701:2019(E) 6.4.2 During employment
2,032.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.6.2 User access	1						x														ISO/IEC 27701:2019(E) 6.6.2 User access management
2,046.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.10.2	2					x					x										ISO/IEC 27701:2019(E) 6.10.2 Information transfer
2049.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.11.2 Security in	3								x				x			x					ISO/IEC 27701:2019(E) 6.11.2 Security in development and suppo
2050.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.11.3 Test data	1															x					ISO/IEC 27701:2019(E) 6.11.3 Test data
2052.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.12.1	3													x	x				x		ISO/IEC 27701:2019(E) 6.12.1 Information security in supplier
2,055.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_6.13.1	1																		x		ISO/IEC 27701:2019(E) 6.13.1 Management of information securi
2066.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.2.5 Privacy	4					x		x	x	x											ISO/IEC 27701:2019(E) 7.2.5 Privacy impact assessment
2070.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.1 Determining	1	x																			ISO/IEC 27701:2019(E) 7.3.1 Determining and fulfilling obligatior
2071.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.2 Determining	9	x			x	x	x	x	x				x	x	x						ISO/IEC 27701:2019(E) 7.3.2 Determining information for PII
2072.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.3 Providing	2	x																	x		ISO/IEC 27701:2019(E) 7.3.3 Providing information to PII principa
2073.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.4 Providing	3								x			x					x				ISO/IEC 27701:2019(E) 7.3.4 Providing mechanism to modify or
2074.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.5 Providing	1											x									ISO/IEC 27701:2019(E) 7.3.5 Providing mechanism to object to PI
2075.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.6 Access,	2											x					x				ISO/IEC 27701:2019(E) 7.3.6 Access, correction and/or erasure
2076.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.7 PII	3													x	x				x		ISO/IEC 27701:2019(E) 7.3.7 PII controllers' obligations to inform
2077.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.8 Providing	6		x										x	x	x	x	x				ISO/IEC 27701:2019(E) 7.3.8 Providing copy of PII processed
2078.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.9 Handling	3					x			x										x		ISO/IEC 27701:2019(E) 7.3.9 Handling requests
2079.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.3.10 Automated	3					x		x	x												ISO/IEC 27701:2019(E) 7.3.10 Automated decision making
2,080.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.1 Limit	4							x	x				x			x					ISO/IEC 27701:2019(E) 7.4.1 Limit collection
2,081.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.2 Limit	6	x							x				x	x	x	x					ISO/IEC 27701:2019(E) 7.4.2 Limit processing
2,082.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.3 Accuracy	2							x	x												ISO/IEC 27701:2019(E) 7.4.3 Accuracy and quality
2,083.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.4 PII	6							x	x				x	x	x					x	ISO/IEC 27701:2019(E) 7.4.4 PII minimization objectives
2,084.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.5 PII de-	3							x	x								x				ISO/IEC 27701:2019(E) 7.4.5 PII de-identification and deletion at
2,085.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.6 Temporary	4		x					x	x								x				ISO/IEC 27701:2019(E) 7.4.6 Temporary files
2,086.00	ISO/IEC 27701:2019	ISO277	ISO27701	ISO27701_7.4.7 Retention	2								x								x				ISO/IEC 27701:2019(E) 7.4.7 Retention

... | CEK+DCS Map by Control Pivot | CEKandDistinctStandardPivot | DataCenterPivotbyFrameTest | DatacenterSecurityPivot | DataCentSecworkplan | DSP by Edition Pivot | DataSecAndPrivworkplan

EnterpriseGRC Solutions, Inc.

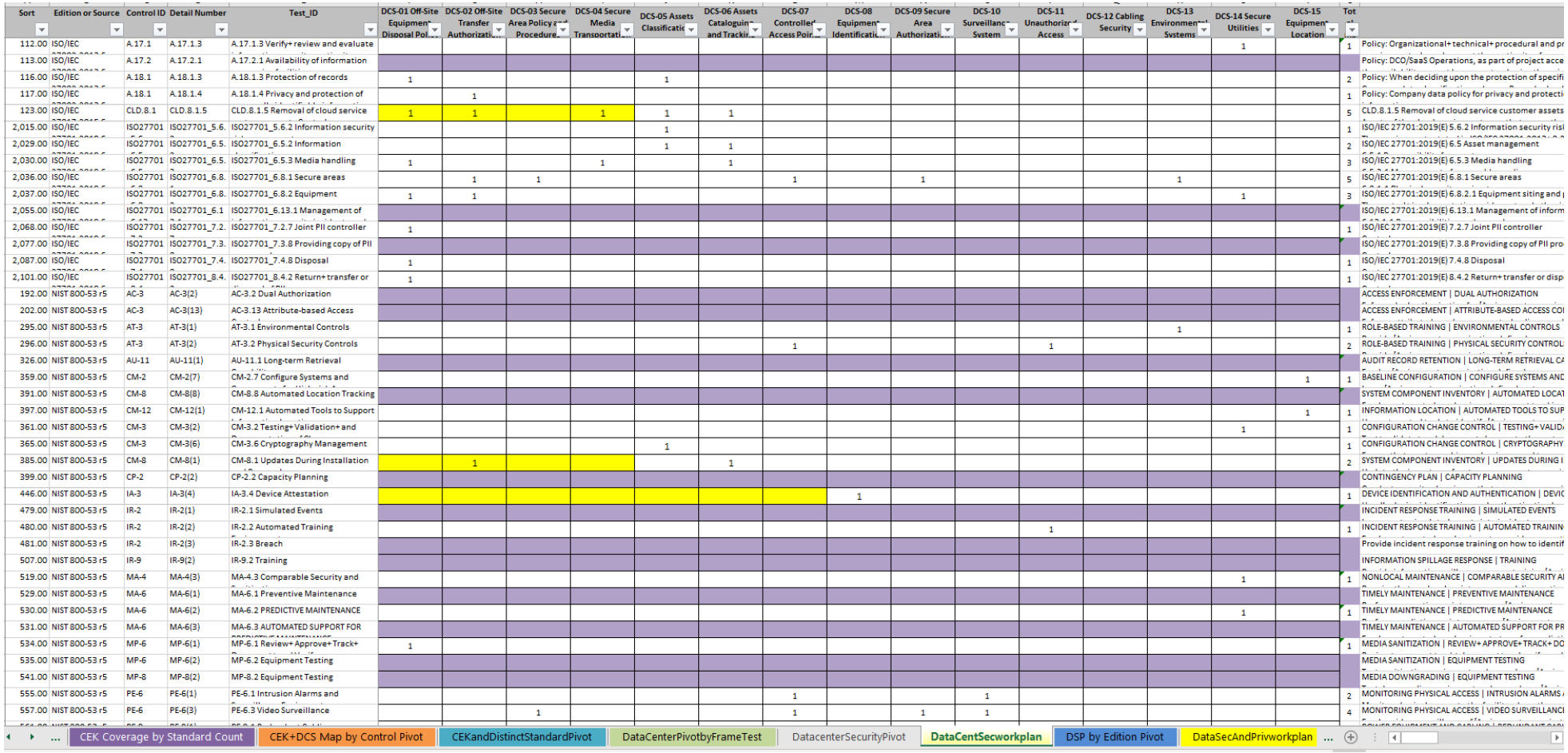
Mapping:

- Aligns common intent and objectives
- Doesn't raise low or high watermark.
- Lowers total work while assuring quality of controls
- Enables singular RMF

Systems Enable People. Mapping Efforts Require Detail Work Plans. People need skills to execute that plan.

EnterpriseGRC Solutions, Inc.

- Mapping domains, controls and tests requires planning and oversight.
- Optimization steps track how many times controls are both used and unused.



Sort	Edition or Source	Control ID	Detail Number	Test_ID	DCS-01 Off-Site Equipment Disposal Pol…	DCS-02 Off-Site Transfer Authorizati…	DCS-03 Secure Area Policy a… Procedure…	DCS-04 Secure Media Transportati…	DCS-05 Assets Classificatio	DCS-06 Assets Cataloguin… and Trackir…	DCS-07 Controlled Access Poin…	DCS-08 Equipment Identificatio…	DCS-09 Secure Area Authorizati…	DCS-10 Surveillanc… System	DCS-11 Unauthorize… Access	DCS-12 Cabling Security	DCS-13 Environmen… Systems	DCS-14 Secure Utilities	DCS-15 Equipmen… Location	Tot…	
112.00	ISO/IEC	A.17.1	A.17.1.3	A.17.1.3 Verify+ review and evaluate														1		1	Policy: Organizational+ technical+ procedural and pr
113.00	ISO/IEC	A.17.2	A.17.2.1	A.17.2.1 Availability of information																	Policy: DCO/SaaS Operations, as part of project acce
116.00	ISO/IEC	A.18.1	A.18.1.3	A.18.1.3 Protection of records	1				1											2	Policy: When deciding upon the protection of specifi
117.00	ISO/IEC	A.18.1	A.18.1.4	A.18.1.4 Privacy and protection of		1														1	Policy: Company data policy for privacy and protecti
123.00	ISO/IEC	CLD.8.1	CLD.8.1.5	CLD.8.1.5 Removal of cloud service	1	1		1	1	1										5	CLD.8.1.5 Removal of cloud service customer assets
2,015.00	ISO/IEC	ISO27701	ISO27701_5.6.	ISO27701_5.6.2 Information security					1											1	ISO/IEC 27701:2019(E) 5.6.2 Information security risl
2,029.00	ISO/IEC	ISO27701	ISO27701_6.5.	ISO27701_6.5.2 Information					1	1										2	ISO/IEC 27701:2019(E) 6.5 Asset management
2,030.00	ISO/IEC	ISO27701	ISO27701_6.5.	ISO27701_6.5.3 Media handling	1			1		1										3	ISO/IEC 27701:2019(E) 6.5.3 Media handling
2,036.00	ISO/IEC	ISO27701	ISO27701_6.8.	ISO27701_6.8.1 Secure areas		1	1				1		1				1			5	ISO/IEC 27701:2019(E) 6.8.1 Secure areas
2,037.00	ISO/IEC	ISO27701	ISO27701_6.8.	ISO27701_6.8.2 Equipment	1	1												1		3	ISO/IEC 27701:2019(E) 6.8.2.1 Equipment siting and
2,055.00	ISO/IEC	ISO27701	ISO27701_6.1	ISO27701_6.13.1 Management of																	ISO/IEC 27701:2019(E) 6.13.1 Management of inform
2,068.00	ISO/IEC	ISO27701	ISO27701_7.2.	ISO27701_7.2.7 Joint PII controller	1															1	ISO/IEC 27701:2019(E) 7.2.7 Joint PII controller
2,077.00	ISO/IEC	ISO27701	ISO27701_7.3.	ISO27701_7.3.8 Providing copy of PII																	ISO/IEC 27701:2019(E) 7.3.8 Providing copy of PII pro
2,087.00	ISO/IEC	ISO27701	ISO27701_7.4.	ISO27701_7.4.8 Disposal	1															1	ISO/IEC 27701:2019(E) 7.4.8 Disposal
2,101.00	ISO/IEC	ISO27701	ISO27701_8.4.	ISO27701_8.4.2 Return+ transfer or	1															1	ISO/IEC 27701:2019(E) 8.4.2 Return+ transfer or disp
192.00	NIST 800-53 r5	AC-3	AC-3(2)	AC-3.2 Dual Authorization																	ACCESS ENFORCEMENT | DUAL AUTHORIZATION
202.00	NIST 800-53 r5	AC-3	AC-3(13)	AC-3.13 Attribute-based Access																	ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CO
295.00	NIST 800-53 r5	AT-3	AT-3(1)	AT-3.1 Environmental Controls													1			1	ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS
296.00	NIST 800-53 r5	AT-3	AT-3(2)	AT-3.2 Physical Security Controls							1				1					2	ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROL
326.00	NIST 800-53 r5	AU-11	AU-11(1)	AU-11.1 Long-term Retrieval																	AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CA
359.00	NIST 800-53 r5	CM-2	CM-2(7)	CM-2.7 Configure Systems and															1	1	BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND
391.00	NIST 800-53 r5	CM-8	CM-8(8)	CM-8.8 Automated Location Tracking																	SYSTEM COMPONENT INVENTORY | AUTOMATED LOCAT
397.00	NIST 800-53 r5	CM-12	CM-12(1)	CM-12.1 Automated Tools to Support															1	1	INFORMATION LOCATION | AUTOMATED TOOLS TO SUP
361.00	NIST 800-53 r5	CM-3	CM-3(2)	CM-3.2 Testing+ Validation+ and														1		1	CONFIGURATION CHANGE CONTROL | TESTING+ VALID
365.00	NIST 800-53 r5	CM-3	CM-3(6)	CM-3.6 Cryptography Management					1											1	CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY
385.00	NIST 800-53 r5	CM-8	CM-8(1)	CM-8.1 Updates During Installation		1				1										2	SYSTEM COMPONENT INVENTORY | UPDATES DURING I
399.00	NIST 800-53 r5	CP-2	CP-2(2)	CP-2.2 Capacity Planning																	CONTINGENCY PLAN | CAPACITY PLANNING
446.00	NIST 800-53 r5	IA-3	IA-3(4)	IA-3.4 Device Attestation								1								1	DEVICE IDENTIFICATION AND AUTHENTICATION | DEVIC
479.00	NIST 800-53 r5	IR-2	IR-2(1)	IR-2.1 Simulated Events																	INCIDENT RESPONSE TRAINING | SIMULATED EVENTS
480.00	NIST 800-53 r5	IR-2	IR-2(2)	IR-2.2 Automated Training											1					1	INCIDENT RESPONSE TRAINING | AUTOMATED TRAININ
481.00	NIST 800-53 r5	IR-2	IR-2(3)	IR-2.3 Breach																	Provide incident response training on how to identif
507.00	NIST 800-53 r5	IR-9	IR-9(2)	IR-9.2 Training																	INFORMATION SPILLAGE RESPONSE | TRAINING
519.00	NIST 800-53 r5	MA-4	MA-4(3)	MA-4.3 Comparable Security and														1		1	NONLOCAL MAINTENANCE | COMPARABLE SECURITY A
529.00	NIST 800-53 r5	MA-6	MA-6(1)	MA-6.1 Preventive Maintenance																	TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE
530.00	NIST 800-53 r5	MA-6	MA-6(2)	MA-6.2 PREDICTIVE MAINTENANCE														1		1	TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE
531.00	NIST 800-53 r5	MA-6	MA-6(3)	MA-6.3 AUTOMATED SUPPORT FOR																	TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PR
534.00	NIST 800-53 r5	MP-6	MP-6(1)	MP-6.1 Review+ Approve+ Track+	1															1	MEDIA SANITIZATION | REVIEW+ APPROVE+ TRACK+ DO
535.00	NIST 800-53 r5	MP-6	MP-6(2)	MP-6.2 Equipment Testing																	MEDIA SANITIZATION | EQUIPMENT TESTING
541.00	NIST 800-53 r5	MP-8	MP-8(2)	MP-8.2 Equipment Testing																	MEDIA DOWNGRADING | EQUIPMENT TESTING
555.00	NIST 800-53 r5	PE-6	PE-6(1)	PE-6.1 Intrusion Alarms and							1			1						2	MONITORING PHYSICAL ACCESS | INTRUSION ALARMS
557.00	NIST 800-53 r5	PE-6	PE-6(3)	PE-6.3 Video Surveillance			1				1		1	1						4	MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE

CEK Coverage by Standard Count | CEK+DCS Map by Control Pivot | CEKandDistinctStandardPivot | DataCenterPivotbyFrameTest | DatacenterSecurityPivot | DataCentSecworkplan | DSP by Edition Pivot | DataSecAndPrivworkplan

Mappers benefit by mapping technical control to frameworks, frameworks to client domains

EnterpriseGRC Solutions, Inc.

ıment 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 * 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 S 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 S support processes; A and contractual requ