Presentation prepared for Cloud Security Alliance, CSA CCM 4.1 to NIST SP 800-53 rev 5 Working Group,
By Robin Basham, CEO EnterpriseGRC Solution, CISSP, CISA, CGEIT, CRISC, CRP, VRP, and President, ISC² East Bay Chapter
With collaboration from 20 CCM WG team members
November 24th, 2021
How it started: “We’d like to use Cloud Control Matrix & NIST SP 800-53 r5 Mapping as our Master Control List”

**RESOURCES / REASONS:** Companies using NIST SP 800-53 r4, must update to Rev 5.1. Cloud Controls Matrix has recently updated to CCM 4.1 – **We need them both, now.**

**Problem:** NIST SP 800-53 as a **mediating** framework is incompletely or inaccurately mapped in products; It requires updates for CIS CSC 7.1->8.1, CCM 3.1->4.0, NIST SP 800-171 r2 & NIST SP 800-172 (Cybersecurity Enhancement), plus New Tailoring Criteria. When NIST is wrong, everything mapped to it becomes compromised.

**Opportunity:** Leveraging NIST SP 800-53 r5 to complete ©AICPA SOC 2, ©HITRUST, PCI DSS 3.21, CSTAR CCM, DFARS CMMC, ©ISO/IEC 27001 plus Privacy, Processing and Cloud requires detail understanding of these frameworks – i.e., experience completing engagements to do this work, but it can be done. NIST Security and Privacy Controls for Federal Information Systems and Organizations is the most widely recognized matrix of controls.

**Methodology:** Creating **useable** cyber framework mapping is an exercise that drives common language across all Policies and Programs and is necessary to meaningful resilience and compliance.
# Common Resources Necessary to Understanding Control Framework Requirements and Alignment

<table>
<thead>
<tr>
<th>Critical Resource Website link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity &amp; Infrastructure Security Agency</strong></td>
</tr>
<tr>
<td>Homepage</td>
</tr>
<tr>
<td><strong>Cloud Security Alliance</strong></td>
</tr>
<tr>
<td><a href="https://cloudsecurityalliance.org/">https://cloudsecurityalliance.org/</a></td>
</tr>
<tr>
<td><strong>National Institute of Standards and Technology</strong></td>
</tr>
<tr>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Sponsoring Organization for this effort is the Cloud Security Alliance Research Working Group

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

Maintaining cloud governance, risk and compliance is becoming increasingly difficult. The more complex systems become, the less secure they become, even though security technologies improve. With the proliferation of security certifications, industry standards and regulations it is becoming increasingly challenging to keep up with the requirements to stay secure and compliant in the cloud.

Why was the CCM created?
To respond to simplify the process of assessing the overall security risk of a cloud provider, CSA created the Cloud Control Matrix (CCM) and Consensus Assessment Initiative Questionnaire (CAIQ). The CCM provides a controls framework that gives detailed understanding of security controls and principles that are aligned to the best practices outlined in the CSA Security Guidance for Cloud Computing. The CAIQ provides a set of Yes/No questions a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the CCM.

Help Integrate the CCM with CRI’s Financial Services Cybersecurity Profile: CSA is partnering with the Cyber Risk Institute (CRI) to provide the financial community with new resources to map and integrate CSA’s Cloud Control Matrix (CCM) and CRI’s Financial Services Cybersecurity Profile. The goal is to define the scope, objectives and technical specifications of the Cloud Security Framework for Financial Services. To learn more, download our group charter.

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

The leader for this CCM to NIST SP 800-53 is Robin Basham.
Consensus Driven Mapping by Domains, Controls, Enhancements, RACI

The following Mapping for CCM 4.1 to NIST SP 800-53 is the product of:

- 20 CSA Vetted Subject Matter Experts who conducted Three to Seven curated mapping iterations
- Leveraged CSA customer contributed mappings from three enterprises
- Included Map Reduction exercises to enforce a Refined RACI
- Had advanced GRC resources contributed and coordinated by EnterpriseGRC Solutions
- Were steered by CSA Program Leadership to finalize this product across August to November of 2021.

<table>
<thead>
<tr>
<th>CCMv4 Control Domains</th>
<th>Code</th>
<th>#Controls</th>
<th>Progress Status</th>
<th>Reviewer 1 (name of reviewers)</th>
<th>Reviewer 2 (name of reviewers)</th>
<th>Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit and Assurance</td>
<td>A&amp;A 6</td>
<td>Delivered</td>
<td>Angela Dogan</td>
<td>Johan Olivier</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS 7</td>
<td>Delivered</td>
<td>Vani Murthy</td>
<td>Geoff Bird</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Business Continuity Management &amp; Operational Resilience</td>
<td>BCR 11</td>
<td>Delivered</td>
<td>Thomas Sager</td>
<td>Alana James</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Change Control &amp; Configuration Management</td>
<td>CCC 9</td>
<td>Delivered</td>
<td>Geoff Bird</td>
<td>Frank Jaramillo</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Cryptography, Encryption &amp; Key Management</td>
<td>CEK 21</td>
<td>Delivered</td>
<td>Michael Roza</td>
<td>Angell Duran, Vani Murthy, Robin Basham</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Datacenter CENTER Security</td>
<td>DCS 15</td>
<td>Delivered</td>
<td>Johan Olivier</td>
<td>Bala Kaundinya</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Data Security &amp; Privacy Lifecycle Management</td>
<td>DSP 19</td>
<td>Delivered</td>
<td>Robin Basham</td>
<td>Madhav Chablani</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Governance, Risk Management and Compliance</td>
<td>GRC 8</td>
<td>Delivered</td>
<td>Michelle Moore</td>
<td>Angela Dogan, Robin Basham</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Human Resources</td>
<td>HRS 13</td>
<td>Delivered</td>
<td>Johan Olivier</td>
<td>Bala Kaundinya</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Identity &amp; Access Management</td>
<td>IAM 16</td>
<td>Delivered</td>
<td>Claus Matzke</td>
<td>Frank Jaramillo</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Interoperability &amp; Portability</td>
<td>IPY 4</td>
<td>Delivered</td>
<td>Geoff Bird, Kimberley Laris</td>
<td>Robin Basham, Madhav Chablani</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Infrastructure &amp; Virtualization Security</td>
<td>IVS 9</td>
<td>Delivered</td>
<td>Vani Murthy</td>
<td>Evan Jones</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Logging and Monitoring</td>
<td>LOG 13</td>
<td>Delivered</td>
<td>Vani Murthy</td>
<td>Robin Basham</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Security Incident Management, E-Discovery, &amp; Cloud Forensics</td>
<td>SEF 8</td>
<td>Delivered</td>
<td>Denny Dean</td>
<td>Joel John</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Supply Chain Management, Transparency, and Accountability</td>
<td>STA 14</td>
<td>Delivered</td>
<td>Erik Johnson</td>
<td>Robin Basham, Madhav Chablani</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Threat and Vulnerability Management</td>
<td>TVM 10</td>
<td>Delivered</td>
<td>Kimberley Laris</td>
<td>Evan Jones, Robin Basham</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>Universal Endpoint Management</td>
<td>UEM 14</td>
<td>Delivered</td>
<td>Johan Olivier</td>
<td>Geoff Bird</td>
<td></td>
<td>Done</td>
</tr>
</tbody>
</table>
The Cloud Controls Matrix is implemented with several resources including the CCM 4.0 Implementation Guidelines, the CCM and the CAIQ v4.

CCM v4.0 Implementation Guidelines | CSA (cloudsecurityalliance.org)

Cloud Controls Matrix and CAIQ v4 | CSA (cloudsecurityalliance.org)
Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

- Cloud Computing Concepts and Architectures
- Governance and Enterprise Risk Management
- Legal Issues, Contracts and Electronic Discovery
- Compliance and Audit Management
- Information Governance
- Management Plane and Business Continuity
- Infrastructure Security
- Virtualization and Containers
- Incident Response
- Application Security
- Data Security and Encryption
- Identity, Entitlement and Access Management
- Security as a Service
- Related Cloud Technologies

Security Guidance for Critical Areas of Focus in Cloud Computing
| CSA (cloudsecurityalliance.org)
Regardless of NIST Framework experience, CCM Implementation requires Cloud Security Knowledge Competence

- Certificate of Cloud Security Knowledge
- The CCSK certificate is widely recognized as the standard of expertise for cloud security and gives you a cohesive and vendor-neutral understanding of how to secure data in the cloud. The CCSK credential is the foundation to prepare you to earn additional cloud credentials.

Certificate of Cloud Security Knowledge (CCSK) | CSA (cloudsecurityalliance.org)
High Level Understanding

Looking at the Control Families (Domains) to compare coverage of same or similar objectives
CCM to NIST SP 800-53
I bought a boat!
### Top Level Control Families From CCM v4.1 to NIST SP 800-53r5

**Mostly Map – Have Some Grey Areas**

<table>
<thead>
<tr>
<th>CCM Domains</th>
<th>NIST Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit and Assurance - A&amp;A</strong></td>
<td><strong>AT - AWARENESS AND TRAINING</strong></td>
</tr>
<tr>
<td><strong>Application and Interface Security - AIS</strong></td>
<td><strong>AU - AUDIT AND ACCOUNTABILITY</strong></td>
</tr>
<tr>
<td><strong>Business Continuity Management and Operational Resilience - BCR</strong></td>
<td><strong>CA - ASSESSMENT, AUTHORIZATION, AND MONITORING</strong></td>
</tr>
<tr>
<td><strong>Change Control and Configuration Management - CCC</strong></td>
<td><strong>CM - CONFIGURATION MANAGEMENT</strong></td>
</tr>
<tr>
<td><strong>Cryptography, Encryption and Key Management - CEK</strong></td>
<td><strong>CP - CONTINGENCY PLANNING</strong></td>
</tr>
<tr>
<td><strong>Datacenter Security - DCS</strong></td>
<td><strong>IA - IDENTIFICATION AND AUTHENTICATION</strong></td>
</tr>
<tr>
<td><strong>Data Security and Privacy Lifecycle Management - DSP</strong></td>
<td><strong>IR - INCIDENT RESPONSE</strong></td>
</tr>
<tr>
<td><strong>Governance, Risk and Compliance - GRC</strong></td>
<td><strong>MA - MAINTENANCE</strong></td>
</tr>
<tr>
<td><strong>Human Resources - HRS</strong></td>
<td><strong>MP - MEDIA PROTECTION</strong></td>
</tr>
<tr>
<td><strong>Identity and Access Management - IAM</strong></td>
<td><strong>PE - PHYSICAL AND ENVIRONMENTAL PROTECTION</strong></td>
</tr>
<tr>
<td><strong>Interoperability and Portability - IPY</strong></td>
<td><strong>PL - PLANNING</strong></td>
</tr>
<tr>
<td><strong>Infrastructure and Virtualization Security - IVS</strong></td>
<td><strong>PM - PROGRAM MANAGEMENT</strong></td>
</tr>
<tr>
<td><strong>Logging and Monitoring - LOG</strong></td>
<td><strong>PS - PERSONNEL SECURITY</strong></td>
</tr>
<tr>
<td><strong>Security Incident Management, E-Discovery, and Cloud Forensics - SEF</strong></td>
<td><strong>PT - PERSONALLY, IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY</strong></td>
</tr>
<tr>
<td><strong>Supply Chain Management, Transparency, and Accountability - STA</strong></td>
<td><strong>RA - RISK ASSESSMENT</strong></td>
</tr>
<tr>
<td><strong>Threat and Vulnerability Management - TVM</strong></td>
<td><strong>SA - SYSTEM AND SERVICES ACQUISITION</strong></td>
</tr>
<tr>
<td><strong>Universal Endpoint Management - UEM</strong></td>
<td><strong>SC - SYSTEM AND COMMUNICATIONS PROTECTION</strong></td>
</tr>
<tr>
<td><strong>Security Incident Management, E-Discovery, and Cloud Forensics - SEF</strong></td>
<td><strong>SI - SYSTEM AND INFORMATION INTEGRITY</strong></td>
</tr>
<tr>
<td><strong>Supply Chain Management, Transparency, and Accountability - STA</strong></td>
<td><strong>SR - SUPPLY CHAIN RISK MANAGEMENT</strong></td>
</tr>
</tbody>
</table>

The Cloud Control Matrix CCM has 17 Domains, 197 Controls, 262 Tests, 1 CAIQ, 1 Implementation Guide, 1 Security Resource Guide, and 1 Audit Guide.

NIST SP 800-53 r5 has 20 Domains, 298 Controls, 720 Enhancements, and 400 Supporting NISTIR, FIPS, and SP.
Control Mapping always reveals a dominant family

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
When fully implemented, control objectives align, however NIST has at least 25% increased areas of specificity. When including NIST reference materials, it is substantially more.

Cloud Controls Matrix has more specificity in Cloud Service Provider requirements:

- Supply Chain Management, Transparency, and Accountability - STA
- Interoperability and Portability - IPY

NIST SP 800-53 Rev 5 Aligned Mapped 757
Not Assigned - too specific 250
17 CCM v4.1 Control Domains have 1824 NIST Control & Enhancements mappings. This chart shows Count of NIST items and Percentage of NIST mappings assigned to this CCM domain.

The average assignment of NIST items to CCM control is 3.9
For 20 NIST Control Families – This chart shows Number of Mappings (out of 1824) and Percentage of mappings that align with any of the 197 CCM Controls using this NIST Domain.
Beyond the scope of CCM – Areas Too Specific to be Mapped

- All domains are at least partially to the CCM
- Compliance Program Management may choose to augment aligned activity based on their specific requirements
- Program and planning alignment should always focus on the expectations for each risk-based audit

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
If the NIST 800-53 Rev 5 mapped controls are fully implemented, CCM 4.1 readiness would most likely have either **No Gap**, a **Partial Gap**, or a **Full Gap** based on CSTAR Requirements for the following Domains.

![Diagram showing the number of CCM Controls in each category of gap for different domains.]

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ISM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
The Domains, Controls, Enhancements, and Gaps
Format for the mapping product

1. High level summary showing count of controls (N of 298 controls plus their 720 enhancements) that align to this Cloud Control Matrix Domain (1 of 17). Pie Charts are high level count of all controls mapped by NIST Control Families and a Bar chart of controls assigned to the CCM Domain.

2. Pie Chart - Control level Mapping and enhancement numbers grouped as the subset of the 197 CCM controls for this domain and showing the aligned NIST Controls and Enhancements. Followed by a detail level list of controls and enhancement grouped by CCM Control.

3. Bar chart(s) for control to control and enhancement mapping.

4. Gaps, general or specific necessary references, and summary of significant areas that the committee concluded to be too specific or not aligned to Cloud Services, so were never mapped. This section may include notes for NIST and notes for CCM improvements.
Use of NIST SP 800-53 R5 aligning to CCM v4 A&A Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 A&A Controls List

A&A-01 Audit and Assurance Policy and Procedures
• CA-1 Assessment, Authorization, and Monitoring Policy and Procedures

A&A-02 Independent Assessments
• CA-2 Assessments
• CA-2.1 Independent Assessors
• CA-2.2 Specialized Assessments
• CA-2.3 Leveraging Results from External Organizations
• CA-7 Continuous Monitoring
• CA-7.1 Independent Assessment

A&A-03 Risk Based Planning Assessment
• CA-2 Assessments
• CA-2.1 Independent Assessors
• CA-2.2 Specialized Assessments
• CA-2.3 Leveraging Results from External Organizations
• PL-10 Baseline Selection
• PL-11 Baseline Tailoring

A&A-04 Requirements Compliance
• CA-1 Assessment, Authorization, and Monitoring Policy and Procedures

A&A-05 Audit Management Process
• CA-1 Assessment, Authorization, and Monitoring Policy and Procedures
• CA-2 Assessments
• PM-4 Plan of Action and Milestones Process

A&A-06 Remediation
• CA-5 Plan of Action and Milestones
• CA-5.1 Automation Support for Accuracy and Currency
• PM-4 Plan of Action and Milestones Process
Concerns for Audit and Assurance - A&A

CCM Focus

• There are no gaps
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards. The primary domain associated to A&A is CA - ASSESSMENT, AUTHORIZATION, AND MONITORING

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix
• CA-3(7) Information Exchange | Transitive Information Exchanges
• CA-9 Internal System Connections
• CA-9(1) Internal System Connections | Compliance Checks
Use of NIST SP 800-53 R5 aligning to CCM v4 AIS Controls

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 AIS Controls List

AIS-01 Application and Interface Security Policy and Procedures
- CM-3 Configuration Change Control
- CM-3.2 Testing, Validation, and Documentation of Changes
- PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION
- PM-20.1 Privacy Policies on Websites, Applications, and Digital Services
- SA-1 System and Services Acquisition Policy and Procedures
- SA-4 Acquisition Process
- SA-8 Security and Privacy Engineering Principles
- SA-8.29 Repeatable and Documented Procedures
- SA-8.30 Procedural Rigor
- SA-8.31 Secure System Modification
- SA-8.32 Sufficient Documentation
- SA-8.33 Minimization
- SI-17 Fail-Safe Procedures

AIS-02 Application Security Baseline Requirements
- CM-2 Baseline Configuration
- CM-2.2 Automation Support for Accuracy and Currency
- CM-2.3 Retention of Previous Configurations
- CM-3 Configuration Change Control
- CM-3.2 Testing, Validation, and Documentation of Changes
- PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION
- SA-1 System and Services Acquisition Policy and Procedures
- SA-4 Acquisition Process
- SA-8 Security and Privacy Engineering Principles
- SA-8.14 Least Privilege
- SA-8.23 Secure Defaults
- SA-8.29 Repeatable and Documented Procedures
- SA-8.31 Secure System Modification
- SA-8.8 Secure Evolvability
- SI-17 Fail-Safe Procedures

AIS-03 Application Security Metrics
- SA-15 Development Process, Standards, and Tools
- SA-15.1 QUALITY METRICS

AIS-04 Secure Application Design and Development
- P-2 System Security and Privacy Plans
- PL-8 Security and Privacy Architectures
- PL-8.1 Defense in Depth
- SA-17 Developer Security Architecture and Design
- SA-17.1 Formal Policy Model
- SA-17.2 Security-relevant Components
- SA-17.3 Formal Correspondence
- SA-17.4 Informal Correspondence
- SA-17.5 Conceptually Simple Design
- SA-17.6 Structure for Testing
- SA-17.7 Structure for Least Privilege
- SA-17.8 Orchestration
- SA-17.9 Design Diversity
- SA-3 System Development Life Cycle
- SA-3.1 Manage Preproduction Environment
- SA-4 Acquisition Process
- SA-4.2 Design and Implementation Information for Controls
- SA-4.3 Development Methods, Techniques, and Practices
- SA-4.8 Continuous Monitoring Plan for Controls
- SA-4.9 Functions, Ports, Protocols, and Services in Use
- SA-5 System Documentation
- SA-8 Security and Privacy Engineering Principles
- SA-8.1 Clear Abstractions
- SA-8.10 Hierarchical Trust
- SA-8.11 Inverse Modification Threshold
- SA-8.12 Hierarchical Protection
- SA-8.13 Minimized Security Elements
- SA-8.15 Predicate Permission
- SA-8.16 Self-reliant Trustworthiness
- SA-8.17 Secure Distributed Composition
- SA-8.18 Trusted Communications Channels
- SA-8.19 Continuous Protection
- SA-8.2 Least Common Mechanism
- SA-8.20 Secure Metadata Management
- SA-8.22 Accountability and Traceability
- SA-8.24 Secure Failure and Recovery
- SA-8.25 Economic Security
- SA-8.26 Performance Security
- SA-8.27 Human Factored Security
- SA-8.28 Acceptable Security
- SA-8.3 Modularity and Layering
- SA-8.30 Procedural Rigor
- SA-8.31 Secure System Modification
- SA-8.32 Sufficient Documentation
- SA-8.33 Minimization
- SA-8.4 Partially Ordered Dependencies
- SA-8.5 Efficiently Mediated Access
- SA-8.6 Minimized Sharing
- SA-8.7 Reduced Complexity
- SA-8.9 Trusted Components

AIS-05 Automated Application Security Testing
- SA-11 Developer Security Testing and Evaluation
- SA-11.1 Static Code Analysis
- SA-11.2 Threat Modeling and Vulnerability Analyses
- SA-11.3 Independent Verification of Assessment Plans and Evidence
- SA-11.4 Manual Code Reviews
- SA-11.5 Penetration Testing
- SA-11.6 Attack Surface Reviews
- SA-11.7 Verify Scope of Testing and Evaluation
- SA-11.8 Dynamic Code Analysis
- SA-11.9 Interactive Application Security Testing
- SA-11.10 Information Input Validation
- SA-11.16 Self-reliant Trustworthiness
- SA-11.17 Secure Data Distribution
- SA-11.18 Trusted Communications Channels
- SA-11.19 Continuous Protection
- SA-11.20 Trust Mechanism
- SA-11.21 Secure Metadata Management
- SA-11.22 Accountability and Traceability
- SA-11.24 Secure Failure and Recovery
- SA-11.25 Economic Security
- SA-11.26 Performance Security
- SA-11.27 Human Factored Security
- SA-11.28 Acceptable Security
- SA-11.3 Modularity and Layering
- SA-11.30 Procedural Rigor
- SA-11.31 Secure System Modification
- SA-11.32 Sufficient Documentation
- SA-11.33 Minimization
- SA-11.4 Partially Ordered Dependencies
- SA-11.5 Efficiently Mediated Access
- SA-11.6 Minimized Sharing
- SA-11.7 Reduced Complexity
- SA-11.8 Trusted Components

AIS-06 Automated Secure Application Deployment
- SA-16 Developer-Provided Training
- SA-3 System Development Life Cycle
- SA-3.2 Use of Live or Operational Data
- SA-3.3 Technology Refresh
- SA-4 Acquisition Process
- SA-4.3 Development Methods, Techniques, and Practices
- SA-8 Security and Privacy Engineering Principles
- SA-8.31 Secure System Modification
- SA-8.32 Sufficient Documentation
- SA-8.33 Minimization
- SA-8.4 Partially Ordered Dependencies
- SA-8.5 Efficiently Mediated Access
- SA-8.6 Minimized Sharing
- SA-8.7 Reduced Complexity
- SA-8.9 Trusted Components

AIS-07 Application Vulnerability Remediation
- SA-11 Developer Security Testing and Evaluation
- SA-11.1 Static Code Analysis
- SA-11.2 Threat Modeling and Vulnerability Analyses
- SA-11.3 Independent Verification of Assessment Plans and Evidence
- SA-11.4 Manual Code Reviews
- SA-11.5 Penetration Testing
- SA-11.6 Attack Surface Reviews
- SA-11.7 Verify Scope of Testing and Evaluation
- SA-11.8 Dynamic Code Analysis
- SA-11.9 Interactive Application Security Testing
- SA-11.10 Information Input Validation
- SA-11.16 Self-reliant Trustworthiness
- SA-11.17 Secure Data Distribution
- SA-11.18 Trusted Communications Channels
- SA-11.19 Continuous Protection
- SA-11.20 Trust Mechanism
- SA-11.21 Secure Metadata Management
- SA-11.22 Accountability and Traceability
- SA-11.24 Secure Failure and Recovery
- SA-11.25 Economic Security
- SA-11.26 Performance Security
- SA-11.27 Human Factored Security
- SA-11.28 Acceptable Security
- SA-11.3 Modularity and Layering
- SA-11.30 Procedural Rigor
- SA-11.31 Secure System Modification
- SA-11.32 Sufficient Documentation
- SA-11.33 Minimization
- SA-11.4 Partially Ordered Dependencies
- SA-11.5 Efficiently Mediated Access
- SA-11.6 Minimized Sharing
- SA-11.7 Reduced Complexity
- SA-11.8 Trusted Components

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 AIS Control Chart
Concerns for Application and Interface Security - AIS

CCM Focus

• There are no gaps.
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards identified as part of controls referenced in SA - SYSTEM AND SERVICES ACQUISITION. The secondary NIST family associated to this CCM domain is SI - SYSTEM AND INFORMATION INTEGRITY
• The AIS Domain is responsible for Cloud System Development Lifecycle and the Security and Privacy Engineering SA-8 control. The depth of control assessment for the CAIQ is likely less than those associated with product control attestations used by Government Agencies (all 465) and as determined necessary by individual product risk analysis. While not part of CCM, Enterprises should review the list of controls not covered in this AIS and the DSP section as part of their overall compliance program risk assessment.

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix
• SA-2 Allocation of Resources
• SA-4(6) Acquisition Process | Use of Information Assurance Products
• SA-4(7) Acquisition Process | NIAP-approved Protection Profiles
• SA-8(21) Security and Privacy Engineering Principles | Self-analysis
• SA-10(2) Developer Configuration Management | Alternative Configuration Management Processes
• SA-10(6) Developer Configuration Management | Trusted Distribution
• SA-20 Customized Development of Critical Components
• SA-21 Developer Screening
• SA-22 Unsupported System Components
• SA-23 Specialization

Also see the extended list of “Never Mapped” controls in Section DSP
Use of NIST SP 800-53 R5 aligning to CCM v4 BCR Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 BCR Control List

**BCR-01 Business Continuity Management Policy and Procedures**
- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- PE-13.1 Detection Systems – Automatic Activation and Notification
- PL-2 System Security and Privacy Plans

**BCR-02 Risk Assessment and Impact Analysis**
- CP-1 Contingency Planning Policy and Procedures

**BCR-03 Business Continuity Strategy**
- CP-2 Contingency Plan
- CP-2.1 Coordinate with Related Plans
- CP-2.2 Capacity Planning
- CP-2.5 Continue Mission and Business Functions
- CP-2.7 Coordinate with External Service Providers

**BCR-04 Business Continuity Planning**
- CP-10 System Recovery and Reconstitution
- CP-2 Contingency Plan
- CP-4 Contingency Plan Testing

**BCR-05 Documentation**
- CP-2 Contingency Plan
- CP-2.1 Coordinate with Related Plans
- CP-2.2 Capacity Planning
- CP-2.3 Resume Mission and Business Functions
- CP-2.8 Identify Critical Assets
- CP-4 Contingency Plan Testing
- CP-4.4 Full Recovery and Reconstitution

**BCR-06 Business Continuity Exercises**
- AT-3 ROLE-BASED SECURITY TRAINING
- AT-3.3 Practical Exercises
- CP-3 Contingency Training
- CP-3.1 Simulated Events
- CP-4 Contingency Plan Testing
- CP-4.4 Full Recovery and Reconstitution
- IR-4 Incident Handling
- IR-4.3 Continuity of Operations

**BCR-07 Communication**
- CP-2 Contingency Plan
- CP-2.1 Coordinate with Related Plans
- PM-8 Critical Infrastructure Plan

**BCR-08 Backup**
- CP-10 System Recovery and Reconstitution
- CP-10.2 Transaction Recovery
- CP-10.4 Restore Within Time Period
- CP-4 Contingency Plan Testing
- CP-4.4 Full Recovery and Reconstitution
- CP-6 Alternate Storage Site
- CP-6.1 Separation from Primary Site
- CP-6.2 Recovery Time and Reconstitution
- CP-6.3 Accessibility
- CP-9 System Backup
- CP-9.6 Redundant Secondary System

**BCR-09 Disaster Response Plan**
- CP-10.2 Transaction Recovery
- CP-10.4 Restore Within Time Period
- CP-2 Contingency Plan
- CP-2.1 Coordinate with Related Plans
- CP-3.1 Simulated Events
- CP-4.1 Coordinate with Related Plans
- CP-8.1 Priority of Service Provisions
- PE-13 Fire Protection
- PE-13.2 Suppression Systems – Automatic Activation and Notification
- PE-13.4 Inspections

**BCR-10 Response Plan Exercise**
- AT-2 SECURITY AWARENESS TRAINING
- AT-2.1 Practical Exercises
- AT-3 ROLE-BASED SECURITY TRAINING
- AT-3.3 Practical Exercises
- AT-4 SECURITY TRAINING RECORDS
- CP-3 Contingency Training
- CP-3.1 Simulated Events
- IR-3 Incident Response Testing
- IR-3.2 Coordination with Related Plans
- IR-3.3 Continuous Improvement
- IR-9 Information Spillage Response

**BCR-11 Equipment Redundancy**
- CP-2 Contingency Plan
- CP-2.2 Capacity Planning
- CP-2.3 Resume Mission and Business Functions
- CP-4 Contingency Plan Testing
- CP-6 Alternate Storage Site
- CP-6.1 Separation from Primary Site
- CP-7 Alternate Processing Site
- CP-8 Telecommunications Services
- CP-8.1 Priority of Service Provisions
- CP-8.2 Single Points of Failure
- CP-8.3 Separation of Primary and Alternate Providers
- CP-9 System Backup
- CP-9.6 Redundant Secondary System

**BCR-12 Information Spillage Response**
- CP-3.1 Simulated Events
- CP-4.1 Coordinate with Related Plans
- CP-8.1 Priority of Service Provisions
- PE-13 Fire Protection
- PE-13.2 Suppression Systems – Automatic Activation and Notification
- PE-13.4 Inspections

**BCR-13 Information Security Management**
- CP-3.1 Simulated Events
- CP-4.1 Coordinate with Related Plans
- CP-8.1 Priority of Service Provisions
- PE-13 Fire Protection
- PE-13.2 Suppression Systems – Automatic Activation and Notification
- PE-13.4 Inspections

**BCR-14 Information Security Management**
- CP-3.1 Simulated Events
- CP-4.1 Coordinate with Related Plans
- CP-8.1 Priority of Service Provisions
- PE-13 Fire Protection
- PE-13.2 Suppression Systems – Automatic Activation and Notification
- PE-13.4 Inspections

**BCR-15 Information Security Management**
- CP-3.1 Simulated Events
- CP-4.1 Coordinate with Related Plans
- CP-8.1 Priority of Service Provisions
- PE-13 Fire Protection
- PE-13.2 Suppression Systems – Automatic Activation and Notification
- PE-13.4 Inspections
Use of NIST SP 800-53 R5 aligning to CCM v4 BCR Control Chart

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.JT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Concerns for Business Continuity Management and Operational Resilience - BCR

CCM Focus

• There are no gaps, however, NIST coverage for Alternate Processing site should be considered for future CCM versions.
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards identified in CP - CONTINGENCY PLANNING domain.

Consideration for what Never Mapped

The following controls were found to be too specific, or a subject matter not considered for alignment to the CCM 4.1 matrix

• CP-2(6) Contingency Plan | Alternate Processing and Storage Sites
• CP-3(2) Contingency Training | Mechanisms Used in Training Environments
• CP-4(2) Contingency Plan Testing | Alternate Processing Site
• CP-4(3) Contingency Plan Testing | Automated Testing
• CP-4(5) Contingency Plan Testing | Self-challenge
• CP-7(1) Alternate Processing Site | Separation from Primary Site
• CP-7(2) Alternate Processing Site | Accessibility
• CP-7(3) Alternate Processing Site | Priority of Service
• CP-7(4) Alternate Processing Site | Preparation for Use
• CP-7(6) Alternate Processing Site | Inability to Return to Primary Site
• CP-8(4) Telecommunications Services | Provider Contingency Plan
• CP-8(5) Telecommunications Services | Alternate Telecommunication Service Testing
• CP-9(3) System Backup | Separate Storage for Critical Information
• CP-9(5) System Backup | Transfer to Alternate Storage Site
• CP-9(7) System Backup | Dual Authorization for Deletion or Destruction
• CP-10(6) System Recovery and Reconstitution | Component Protection
• CP-11 Alternate Communications Protocols
• CP-12 Safe Mode
• CP-13 Alternative Security Mechanisms

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ISM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Change Control and Configuration Management - CCC

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO THE CHANGE CONTROL AND CONFIGURATION MANAGEMENT - CCC DOMAIN

Use of NIST SP 800-53 R5 aligning to CCM v4 CCC Domain

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 CCC Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 CCC Control List

**CCC-01 Change Management Policy and Procedures**
- CM-1 Configuration Management Policy and Procedures
- CM-10 Software Usage Restrictions
- CM-10.1 Open-source Software
- CM-11 User-Installed Software
- CM-9 Configuration Management Plan
- CM-9.1 Assignment of Responsibility
- PM-9 Risk Management Strategy
- PS-8 Personnel Sanctions
- SA-8 Security and Privacy Engineering Principles
- SA-8.1 Clear Abstractions
- SA-8.24 Secure Failure and Recovery
- SA-12 Information Management and Retention

**CCC-02 Quality Testing**
- CM-2 Baseline Configuration
- CM-2.2 Automation Support for Accuracy and Currency
- CM-2.6 Development and Test Environments
- CM-3 Configuration Change Control
- CM-3.2 Testing, Validation, and Documentation of Changes
- CM-3.7 Review System Changes
- CM-3.9 Automated Change Implementation
- CM-3.4 Security and Privacy Representatives
- CM-3.5 Automated Security Response
- CM-3.6 Cryptography Management
- CM-4 Security and Privacy Impact Analyses
- CM-4.1 Separate Test Environments
- CM-5 Access Restrictions for Change
- CM-5.5 Privilege Limitation for Production and Operation
- CM-5.6 Limit Library Privileges
- CM-5.7 Limit Functionality
- CM-7.2 Prevent Program Execution
- CM-7.3 Registration Compliance
- CM-7.4 Unauthorized Software
- CM-7.5 Authorized Software
- CM-7.6 Confined Environments with Limited Privileges
- CM-7.7 Code Execution in Protected Environments
- SA-10.1 Developer Configuration Management
- SA-10.7 Security and Privacy Representatives
- SA-11 Developer Security Testing and Evaluation
- SA-11.9 Interactive Application Security Testing

**CCC-04 Unauthorized Change Protection**
- CA-7 Continuous Monitoring
- CA-7.4 Risk Monitoring
- CM-11 User-Installed Software
- CM-3 Configuration Change Control
- CM-3.1 Automated Documentation, Notification, and Prohibition of Changes
- CM-3.5 Automated Security Response
- CM-3.7 Review System Changes
- CM-3.8 Prevent or Restrict Configuration Changes
- CM-5.2 Automated Access Enforcement
- CM-5.4 Dual Authorization
- CM-5.5 Privilege Limitation for Production and Operation
- CM-5.6 Limit Library Privileges
- CM-7.2 Prevent Program Execution
- CM-7.3 Registration Compliance
- CM-7.4 Unauthorized Software
- CM-7.5 Authorized Software
- CM-7.6 Confined Environments with Limited Privileges
- CM-7.7 Code Execution in Protected Environments
- SA-10.1 Developer Configuration Management
- SA-10.7 Security and Privacy Representatives
- SA-11 Developer Security Testing and Evaluation
- SA-11.9 Interactive Application Security Testing

**CCC-05 Change Agreements**
- CM-3 Configuration Change Control
- CM-3.1 Automated Documentation, Notification, and Prohibition of Changes
- CM-3.2 Testing, Validation, and Documentation of Changes
- CM-6 Configuration Settings
- CM-7 Least Functionality
- SA-10 Developer Configuration Management
- SR-4 Provenance
- SR-5 Acquisition Strategies, Tools, and Methods

**CCC-06 Change Management Baseline**
- CM-14 Signed Components
- CM-2 Baseline Configuration
- CM-2.3 Retention of Previous Configurations
- CM-3 Configuration Change Control
- CM-3.1 Automated Documentation, Notification, and Prohibition of Changes
- CM-3.5 Automated Security Response
- CM-3.7 Review System Changes
- CM-3.8 Prevent or Restrict Configuration Changes
- CM-5.1 Automated Access Enforcement
- CM-5.4 Dual Authorization
- CM-5.5 Privilege Limitation for Production and Operation
- CM-6 Configuration Settings
- CM-6.1 Automated Management, Application, and Verification
- CM-6.2 Respond to Unauthorized Changes
- CM-7.2 Prevent Program Execution
- CM-7.3 Registration Compliance
- CM-7.4 Unauthorized Software
- CM-7.5 Authorized Software
- CM-7.6 Confined Environments with Limited Privileges
- CM-7.7 Code Execution in Protected Environments
- SA-10.1 Developer Configuration Management
- SA-10.7 Security and Privacy Representatives
- SA-11 Developer Security Testing and Evaluation
- SA-11.9 Interactive Application Security Testing

**CCC-07 Detection of Baseline Deviation**
- CM-6 Configuration Settings
- CM-6.2 Respond to Unauthorized Changes
- SI-2.2 Automated Flaw Remediation Status
- SI-2.3 Time to Remediate Flaws and Benchmarks for Corrective Actions
- SI-2.4 Automated Patch Management Tools
- SI-2.5 Automatic Software and Firmware Updates
- SI-2.6 Removal of Previous Versions of Software and Firmware

**CCC-08 Exception Management**
- CM-3 Configuration Change Control
- CM-3.1 Automated Documentation, Notification, and Prohibition of Changes

**CCC-09 Change Restoration**
- CM-2 Baseline Configuration
- CM-2.3 Retention of Previous Configurations
- CM-3 Configuration Change Control
- CM-3.3 Automated Change Implementation
- CM-3.7 Review System Changes
- CM-3.8 Prevent or Restrict Configuration Changes
- CM-5.2 Automated Access Enforcement
- CM-5.4 Dual Authorization
- CM-5.5 Privilege Limitation for Production and Operation
- CM-5.6 Limit Library Privileges
- CM-7.2 Prevent Program Execution
- CM-7.3 Registration Compliance
- CM-7.4 Unauthorized Software
- CM-7.5 Authorized Software
- CM-7.6 Confined Environments with Limited Privileges
- CM-7.7 Code Execution in Protected Environments
- SA-10.1 Developer Configuration Management
- SA-10.7 Security and Privacy Representatives
- SA-11 Developer Security Testing and Evaluation
- SA-11.9 Interactive Application Security Testing

**CCC-10 Security and Privacy Engineering Principles**
- SA-8.8 Security and Privacy Engineering Principles
- SA-8.24 Secure Failure and Recovery
- SA-10.1 Software and Firmware Integrity Verification
- SA-10.3 Hardware Integrity Verification
- SA-10.4 Trusted Generation

---

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 CCC Control Chart
CCM Focus

- There are no gaps.
- The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards as identified by reference in the **CONFIGURATION MANAGEMENT** domain.

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix:

- CM-7(8) Least Functionality | Binary or Machine Executable Code
- CM-11(3) User-installed Software | Automated Enforcement and Monitoring
The Cryptography, Encryption and Key Management – CEK domain is the largest of the CCM 17, with 21 distinct CCM Controls and 23 CEK questions in the CAIQ.

Understanding these controls relies heavily on CSA’s resource Security Guidance for Critical Areas of Focus in Cloud Computing | CSA (cloudsecurityalliance.org)

The CEK and DSP domains represent the two largest number of mappings approved by the CCM NIST WG. The total number of recommendations, while to be expected due to their scope of content, are outliers. Although they were reduced, organizations should plan to assign more time and resource to these sections.
Use of NIST SP 800-53 R5 aligning to CCM v4 CEK Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 CEK Control List

**CEK-01 Encryption and Key Management Policy and Procedures**
- SA-9 External System Services
- SA-9.6 Organization-controlled Cryptographic Keys
- SC-1 System and Communications Protection Policy and Procedures
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**CEK-02 CEK Roles and Responsibilities**
- IA-7 Cryptographic Module Authentication
- IA-8 Identification and Authentication (Non-Organizational Users)
- IA-8.5 Acceptance of PIV-I Credentials
- SA-9 External System Services
- SA-9.1 Risk Assessments and Organizational Approvals
- SA-9.6 Organization-controlled Cryptographic Keys
- SC-12 Cryptographic Key Establishment and Management
- SC-12.6 Physical Control of Keys
- SC-13 Cryptographic Protection

**CEK-03 Data Encryption**
- AC-19 Access Control for Mobile Devices
- AC-19.5 Full Device or Container-based Encryption
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-28 Protection of Information at Rest
- SC-28.1 Cryptographic Protection
- SC-28.2 Offline Storage
- SC-28.3 Cryptographic Keys
- SC-8 Transmission Confidentiality and Integrity
- SC-8.1 Cryptographic Protection
- SC-8.3 Cryptographic Protection for Message Externals
- SC-8.4 Conceal or Randomize Communications
- SI-4 System Monitoring
- SI-4.10 Visibility of Encrypted Communications
- SI-7 Software, Firmware, and Information Integrity
- SI-7.6 Cryptographic Protection

**CEK-04 Encryption Algorithm**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-28 Protection of Information at Rest
- SC-28.1 Cryptographic Protection

**CEK-05 Encryption Change Management**
- CM-3 Configuration Change Control
- CM-3.6 Cryptography Management
- PM-31 CONTINUOUS MONITORING STRATEGY
- SC-28 Protection of Information at Rest
- SC-28.1 Cryptographic Protection
- SC-28.3 Cryptographic Keys
- SI-7.6 Cryptographic Protection

**CEK-06 Encryption Change Cost Benefit Analysis**
- CM-3 Configuration Change Control
- CM-3.6 Cryptography Management
- PL-2 System Security and Privacy Plans

**CEK-07 Encryption Risk Management**
- CM-3 Configuration Change Control
- CM-3.6 Cryptography Management
- PM-31 CONTINUOUS MONITORING STRATEGY
- SC-28 Protection of Information at Rest
- SC-28.1 Cryptographic Protection
- SC-28.3 Cryptographic Keys

**CEK-08 CSC Key Management Capability**
- CA-6.2 Joint Authorization — Inter-organization
- CP-9 System Backup
- CP-9.8 Cryptographic Protection
- SA-9 External System Services
- SC-12 Cryptographic Key Establishment and Management
- SC-12.6 Physical Control of Keys
- SC-16.3 Cryptographic Binding

**CEK-09 Encryption and Key Management Audit**
- AU-9 Protection of Audit Information
- AU-9.3 CRYPTOGRAPHIC PROTECTION
- PM-31 CONTINUOUS MONITORING STRATEGY

**CEK-10 Key Generation**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-13 Cryptographic Protection

**CEK-11 Key Purpose**
- IA-5 Authenticator Management
- IA-5.2 Public Key-based Authentication
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**CEK-12 Key Rotation**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-13 Cryptographic Protection

**CEK-13 Key Revocation**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**CEK-14 Key Destruction**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**CEK-15 Key Activation**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-13 Cryptographic Protection

**CEK-16 Key Suspension**
- PM-31 CONTINUOUS MONITORING STRATEGY
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-13 Cryptographic Protection

**CEK-20 Key Recovery**
- CM-3 Configuration Change Control
- CM-3.6 Cryptography Management
- CP-9 System Backup
- CP-9.8 Cryptographic Protection
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**CEK-21 Key Inventory Management**
- SA-9 External System Services
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-12.6 Physical Control of Keys

**CEK-18 Key Archival**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.1 Availability
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys
- SC-28 Protection of Information at Rest
- SC-28.3 Cryptographic Keys

**CEK-19 Key Compromise**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.1 Availability
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**CEK-22 Key Deactivation**
- SC-12 Cryptographic Key Establishment and Management
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**SC-13 Cryptographic Protection**
- SC-12.2 Symmetric Keys
- SC-12.3 Asymmetric Keys

**SC-12.3 Asymmetric Keys**
- SC-12.6 Physical Control of Keys
- SC-12.6 Cryptographic Protective

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 CEK Control Chart
Concerns for Cryptography, Encryption and Key Management - CEK

CCM Focus

• There are no gaps. The high rate of SC-12 and SC-28 mapping is the result of NIST’s enforcement of detail implementation guidance within the associated Referenced SP.
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards found in SC - SYSTEM AND COMMUNICATIONS PROTECTION. Standards of particular importance include:
  • NIST SP 800-57 PART 1 REV. 5
  • NIST SP 800-57 PART 2 REV. 1
  • NIST SP 800-57 PART 3 REV. 1

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix. Based upon the organization’s RMF and scope, these controls may also be necessary to maintaining Cloud Product Operational controls.

• AC-4(4) Information Flow Enforcement | Flow Control of Encrypted Information* This control may also support CCM IPY-04
• MA-4(6) Nonlocal Maintenance | Cryptographic Protection
• SI-19(4) De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers
Use of NIST SP 800-53 R5 aligning to CCM v4 DCS Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 DCS Control List

DCS-01 Off-Site Equipment Disposal Policy and Procedures
- MP-6 Media Sanitization
- MP-6.1 Review, Approve, Track, Document, and Verify
- MP-6.2 Equipment Testing
- MP-6.3 Nondestructive Techniques
- MP-6.8 Remote Purging or Wiping of Information
- MP-7 Media Use
- MP-7.2 Prohibit Use of Sanitization-resistant Media
- MP-8 Media Downgrading

DCS-02 Off-Site Transfer Authorization Policy and Procedures
- AC-1 Access Control Policy and Procedures
- AC-4 Information Flow Enforcement
- CA-3 System Interconnections
- MP-5 Media Transport
- MP-5.3 Custodians
- SC-4 Information in Shared Systems Resources
- SC-4.2 Multilevel or Periods Processing

DCS-03 Secure Area Policy and Procedures
- PE-6 Monitoring Physical Access
- PE-6.1 Intrusion Alarms and Surveillance Equipment
- PE-6.2 Automated Intrusion Recognition and Responses
- PE-6.3 Video Surveillance
- PE-6.4 Monitoring Physical Access to Systems
- SC-15 Collaborative Computing Devices and Applications

DCS-04 Secure Media Transportation Policy and Procedures
- MP-1 Media Protection Policy and Procedures
- MP-5 Media Transport
- MP-5.3 Custodians

DCS-05 Assets Classification
- CM-8 System Component Inventory
- CM-8.1 Updates During Installation and Removal
- CM-8.2 Automated Maintenance
- CM-8.4 Accountability Information
- CM-8.6 Accessed Configurations and Approved Deviations
- CM-8.7 Centralized Repository
- CM-8.9 Assignment of Components to Systems
- PE-20 Asset Monitoring and Tracking
- PM-5 System Inventory
- PM-5.1 Inventory of Personally Identifiable Information

DCS-06 Assets Cataloguing and Tracking
- CM-8 System Component Inventory
- CM-8.1 Updates During Installation and Removal
- CM-8.2 Automated Maintenance
- CM-8.4 Accountability Information
- CM-8.7 Centralized Repository
- CM-8.8 Automated Location Tracking

DCS-07 Controlled Access Points
- AT-3 ROLE-BASED SECURITY TRAINING
- AT-3.2 Physical Security Controls
- PE-2 Physical Access Authorizations
- PE-2.1 Access by Position or Role
- PE-2.3 Restrict Unsecured Access
- PE-3 Physical Access Control
- PE-3.2 Facility and Systems
- PE-3.3 Continuous Guards
- PE-3.4 Lockable Casings
- PE-3.5 Tamper Protection
- PE-3.7 Physical Barriers
- PE-3.8 Access Control Vistas
- PE-6 Monitoring Physical Access
- PE-6.1 Intrusion Alarms and Surveillance Equipment
- PE-6.2 Automated Intrusion Recognition and Responses
- PE-6.3 Video Surveillance
- PE-6.4 Monitoring Physical Access to Systems
- SC-42 Sensor Capability and Data

DCS-08 Equipment Identification
- AC-18 Wireless Access
- AC-18.1 Authentication and Encryption
- IA-3 Device Identification and Authentication
- IA-3.3 Dynamic Address Allocation

DCS-09 Secure Area Authorization
- MP-4 Media Storage
- MP-4.2 Automated Restricted Access
- PE-18 Location of System Components
- PE-3 Physical Access Control
- PE-3.3 Access Control Vistas
- PE-5 Access Control for Output Devices
- PE-6 Monitoring Physical Access
- PE-6.1 Intrusion Alarms and Surveillance Equipment
- PE-6.2 Automated Intrusion Recognition and Responses
- PE-6.3 Video Surveillance
- PE-6.4 Monitoring Physical Access to Systems
- SC-42 Sensor Capability and Data

DCS-10 Surveillance System
- AT-3.2 Physical Security Controls
- PE-6 Monitoring Physical Access
- PE-6.1 Intrusion Alarms and Surveillance Equipment
- PE-6.2 Automated Intrusion Recognition and Responses
- PE-6.3 Video Surveillance
- PE-6.4 Monitoring Physical Access to Systems
- PE-8 Visitor Access Records
- PE-8.1 Automated Records Maintenance and Review

DCS-11 Unauthorized Access Response Training
- AT-3 ROLE-BASED SECURITY TRAINING
- AT-3.2 Physical Security Controls
- IR-2 Incident Response Training
- IR-2.1 Simulated Events
- IR-2.2 Automated Training Environments

DCS-12 Cabling Security
- PE-19 Information Leakage
- PE-19.1 National Emissions and Tempest Policies and Procedures
- PE-9 Power Equipment and Cabling
- PE-9.1 Redundant Cabling
- PE-9.2 Automatic Voltage Controls

DCS-13 Environmental Systems
- MA-6 Timely Maintenance
- MA-6.1 Preventive Maintenance
- MA-6.2 PREDICTIVE MAINTENANCE
- PE-13 Fire Protection
- PE-13.1 Detection Systems – Automatic Activation and Notification
- PE-13.4 Inspections
- PE-14 Temperature and Humidity Controls
- PE-14.1 Automatic Controls
- PE-15 Water Damage Protection
- PE-15.1 Automation Support

DCS-14 Secure Utilities
- MA-6 Timely Maintenance
- MA-6.1 Preventive Maintenance
- MA-6.2 PREDICTIVE MAINTENANCE

DCS-15 Equipment Location
- CM-12 Information Location
- CM-12.1 Automated Tools to Support Information Location
- PE-18 Location of System Components
- PE-23 Facility Location
- IR-2.3 Breach
Use of NIST SP 800-53 R5 aligning to CCM v4 DCS Control Chart

<table>
<thead>
<tr>
<th>Control</th>
<th>CCM v4</th>
<th>DCS Control Chart</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP 1</td>
<td>PE 3</td>
<td>PE 3</td>
</tr>
<tr>
<td>CSP 2</td>
<td>PE 4</td>
<td>PE 4</td>
</tr>
<tr>
<td>CSP 3</td>
<td>PE 5</td>
<td>PE 5</td>
</tr>
<tr>
<td>CSP 4</td>
<td>PE 6</td>
<td>PE 6</td>
</tr>
<tr>
<td>CSP 5</td>
<td>PE 7</td>
<td>PE 7</td>
</tr>
<tr>
<td>CSP 6</td>
<td>PE 8</td>
<td>PE 8</td>
</tr>
<tr>
<td>CSP 7</td>
<td>PE 9</td>
<td>PE 9</td>
</tr>
<tr>
<td>CSP 8</td>
<td>PE 10</td>
<td>PE 10</td>
</tr>
<tr>
<td>CSP 9</td>
<td>PE 11</td>
<td>PE 11</td>
</tr>
<tr>
<td>CSP 10</td>
<td>PE 12</td>
<td>PE 12</td>
</tr>
</tbody>
</table>

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Concerns for Datacenter Security - DCS

CCM Focus

- There are two partial gaps; DCS-02 “The relocation or transfer request requires the written or cryptographically verifiable authorization.” DCS-05 requires that assets are classified according to business risk, whereas NIST implies adherence to classification based upon Federal standards. CCM is lighter and specific to the business context.
- NIST Data Center Security has a higher level of scrutiny within areas of Maintenance, Physical Access records, and responsibilities in response to Disaster and Continuity. Using CCM alone might lead to exposure in the Data Security and Privacy domain for evidence and policy to control information assets.
- The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards as mainly identified within the following control families:
  - CM - CONFIGURATION MANAGEMENT
  - MA – MAINTENANCE
  - PE - PHYSICAL AND ENVIRONMENTAL PROTECTION
  - MP - MEDIA PROTECTION

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix:

- MA-2 Controlled Maintenance
- MA-2(2) Controlled Maintenance | Automated Maintenance Activities
- MA-3 Maintenance Tools
- MA-3(1) Maintenance Tools | Inspect Tools
- MA-3(2) Maintenance Tools | Inspect Media
- MA-3(3) Maintenance Tools | Prevent Unauthorized Removal
- MA-3(5) Maintenance Tools | Execution with Privilege
- MA-3(6) Maintenance Tools | Software Updates and Patches
- MA-4 Nonlocal Maintenance
- MA-4(1) Nonlocal Maintenance | Log and Review
- MA-4(3) Nonlocal Maintenance | Comparable Security and Sanitization
- MA-4(4) Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions

- MA-4(6) Nonlocal Maintenance | Cryptographic Protection
- MA-4(7) Nonlocal Maintenance | Disconnect Verification
- MA-5(1) Maintenance Personnel | Individuals Without Appropriate Access
- MA-6(3) Timely Maintenance | Automated Support for Predictive Maintenance
- MA-7 Field Maintenance
- MP-2 Media Access
- MP-3 Media Marking
- MP-6(7) Media Sanitization | Dual Authorization
- MP-8(1) Media Downgrading | Documentation of Process
- MP-8(2) Media Downgrading | Equipment Testing
- MP-8(3) Media Downgrading | Controlled Unclassified Information
- MP-8(4) Media Downgrading | Classified Information
- PE-2(2) Physical Access Authorizations | Two Forms of Identification
- PE-4 Access Control for Transmission

- PE-5(2) Access Control for Output Devices | Link to Individual Identity
- PE-8(3) Visitor Access Records | Limit Personally Identifiable Information Elements
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-11(1) Emergency Power | Alternate Power Supply — Minimal Operational Capability
- PE-11(2) Emergency Power | Alternate Power Supply — Self-contained
- PE-12 Emergency Lighting
- PE-12(1) Emergency Lighting | Essential Mission and Business Functions
- PE-14(2) Environmental Controls | Monitoring with Alarms and Notifications
- PE-16 Delivery and Removal
- PE-21 Electromagnetic Pulse Protection
- PE-22 Component Marking
• Privacy is an entire Baseline in NIST SP 800-53B. In addition to the new NIST PT domain, aspects of data processing & privacy are prescribed as the (P) attribute used by FedRamp on 97 Controls and Enhancements. This assessment characteristic makes mapping the 19 CCM DSP controls to the 97 NIST Controls and Enhancements comparable to the effort of mapping NIST to the entire of ISO/IEC 27018 (For Processing) AND ISO/IEC 27701 (For Privacy) standards.

• In the CCM WG effort to make this area of mapping useful, we emphasized confirming that Privacy baseline associated controls and enhancements existed in their appropriate RACI. Wherever possible, we reduced the requirement. It is still big.
Use of NIST SP 800-53 R5 aligning to CCM v4 DSP Control List (1)

DSP-01 Security and Privacy Policy and Procedures
- PL-2 System Security and Privacy Plans
- PL-7 Concept of Operations
- PM-17 Protecting Controlled Unclassified Information on External Systems
- PM-18 Privacy Program Plan
- PM-19 PRIVACY PROGRAM LEADERSHIP ROLE
- PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION
- PM-20.1 Privacy Policies on Websites, Applications, and Digital Services
- PM-23 DATA GOVERNANCE BODY
- PM-24 DATA INTEGRITY BOARD
- PM-26 COMPLAINT MANAGEMENT
- PT-1 Policy and Procedures
- PT-5 Privacy Notice
- PT-5.2 Privacy Act Statements
- PT-6 System of Records Notice
- PT-6.1 Routine Uses
- PT-7 Specific Categories of Personally Identifiable Information
- PT-7.2 First Amendment Information

DSP-02 Secure Disposal
- PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT
- SI-12 Information Management and Retention
- SI-12.3 Information Disposal
- SI-18.1 Automation Support
- SI-18.4 Individual Requests
- SI-18.5 Notice of Correction or Deletion

DSP-03 Data Inventory
- CM-12 Information Location
- CM-12.1 Automated Tools to Support Information Location
- PM-5 System Inventory
- PM-5.1 Inventory of Personally Identifiable Information
- SI-12 Information Management and Retention
- SI-12.1 Limit Personally Identifiable Information Elements
- SI-19 Data Quality Operations
- SI-19.1 Collection
- SI-19.2 Archiving

DSP-04 Data Classification
- AC-16 Security and Privacy Attributes
- AC-16.3 Attribute Reassignment — Regrading Mechanisms
- PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT
- PM-23 DATA GOVERNANCE BODY
- PM-24 DATA INTEGRITY BOARD
- PT-2 Authority to Process Personally Identifiable Information
- PT-2.1 Data Tagging
- PT-7.2 First Amendment Information
- SI-18.2 Data Tags
- SI-19.6 Differential Privacy
- SI-19.7 Social Security Numbers
- SI-19.8 First Amendment Information
- SI-19.9 Information Disposal

DSP-05 Data Flow Documentation
- AC-16 Security and Privacy Attributes
- AC-16.3 Maintenance of Attribute Associations by System
- AC-16.7 Consistent Attribute Interpretation
- AC-16.8 Association Techniques and Technologies
- AC-4 Information Flow Enforcer
- AC-4.1 Object Security and Privacy Attributes
- AC-4.10 Enable and Disable Security or Privacy Policy Filters
- AC-4.12 Data Type Identifiers
- AC-4.13 Decomposition into Policy-relevant Subcomponents
- AC-4.19 Validation of Metadata
- AC-4.2 Processing Domains
- AC-4.3 Dynamic Information Flow Control
- AC-4.5 Embedded Data Types
- AC-4.6 Metadata
- AC-4.7 One-way Flow Mechanisms
- AC-4.8 Security and Privacy Policy Filters
- SI-17 Developer Security Architecture and Design
- SA-17.3 Formal Correspondence
- SA-5 System Documentation
- SC-7 Boundary Protection
- SC-7.24 Personally Identifiable Information

DSP-06 Data Ownership and Stewardship
- PM-18 Privacy Program Plan
- PM-19 PRIVACY PROGRAM LEADERSHIP ROLE
- PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT
- PS-6 Access Agreements
- PS-6.2 Classified Information Requiring Special Protection
- PT-2.1 Data Tagging
- SI-12 Information Management and Retention
- SI-12.1 Limit Personally Identifiable Information Elements
- PM-24 DATA INTEGRITY BOARD
- PM-25 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH
- PT-2 Authority to ProcessPersonally Identifiable Information
- PT-2.2 Automation
- PT-3 Personally Identifiable Information Processing Purposes
- PT-4 Consent
- SA-15 Development Process, Standards, and Tools
- SA-15.12 Minimize Personally Identifiable Information
- SA-3 System Development Life Cycle
- SA-4 Acquisition Process
- SA-5 System Documentation
- SA-8 Security and Privacy Engineering Principles
- SA-8.13 Minimized Security Elements
- SA-8.18 Trusted Communications Channels
- SA-8.20 Secure Metadata Management
- SA-8.22 Accountability and Traceability
- SA-8.23 Secure Defaults
- SA-8.33 Minimization
- SA-8.9 Trusted Components
- SC-28 Protection of Information at Rest
- SC-28.1 Cryptographic Protection
- SC-3 Security Function Isolation
- SC-3.3 Minimize Non-security Functionality
- SC-7 Boundary Protection
- SC-7.24 Personally Identifiable Information
- SC-8 Transmission Confidentiality and Integrity
- SC-8.1 Cryptographic Protection
- SC-8.2 Pre- and Post-transmission Handling
- SC-8.3 Cryptographic Protection for Message Externals

DSP-07 Data Protection by Design and Default
- PM-17 Protecting Controlled Unclassified Information on External Systems
- PM-24 DATA INTEGRITY BOARD

SC-8.4 Conceal or Randomize Communications
- SI-12 Information Management and Retention
- SI-12.1 Limit Personally Identifiable Information Elements
- SI-12.2 Minimize Personally Identifiable Information in Testing, Training, and Research
- SI-12.3 Information Disposal

DSP-08 Data Privacy by Design and Default
- PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT
- PM-24 DATA INTEGRITY BOARD
- PT-1 Policy and Procedures
- PT-2 Authority to Process Personally Identifiable Information
- PT-2.1 Data Tagging
- PT-5 Privacy Notice
- PT-5.1 Just-in-time Notice
- PT-5.2 Privacy Act Statements
- PT-6 System of Records Notice
- PT-8.2 Computer Matching Requirements
- SA-11 Developer Security Testing and Evaluation
- SA-11.3 Independent Verification of Assessment Plans and Evidence
- SI-18 Information Disposal
- SI-18.3 Collection
- SI-19 Data Quality Operations
- SI-19.1 Collection
- SI-19.5 Statistical Disclosure Control
- SI-19.6 Differential Privacy
- SI-19.8 Motivated Intruder
Use of NIST SP 800-53 R5 aligning to CCM v4 DSP Control List (2)
Use of NIST SP 800-53 R5 aligning to CCM v4 DSP Domain
CCM Focus

• There are no gaps
• Data Privacy and Data Protection by Design controls may be managed as an overlay of controls within the AIS domain. Pairing these within AIS would address duplication of effort. Organizations should evaluate methods to automate this area of control. DSP should address requirements identified in IPY-03 and IPY-04. Care to leverage common tests is advised.
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards as found in the following control families:
  • **PM - PROGRAM MANAGEMENT**
  • **PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY**
  • **SA - SYSTEM AND SERVICES ACQUISITION**
  • **SC - SYSTEM AND COMMUNICATIONS PROTECTION**
  • **SI - SYSTEM AND INFORMATION INTEGRITY**

Consideration for what Never Mapped

• While the entirety of the PT domain is mapped to CCM, based on the architecture deployed by Cloud Systems and Services, organizations should reference the following slide containing 101 controls and enhancements never mapped to the CCM. The level of specificity for these controls is generally beyond the detail indicated by the CAIQ.
• In some cases, compliance program management may surreptitiously cover these controls within their collected artifacts. Organizations may choose to add some of the following controls into this and other domains. Simply the following 101 items are more than is required to meet the criteria set by the CCM.
Noteworthy Controls not included in Private Lifecycle Management - DSP

PL-8(2) Security and Privacy Architectures | Supplier Diversity
PL-9 Central Management
SC-2(1) Separation of System and User Functionality | Interfaces for Non-privileged Users
SC-2(2) Separation of System and User Functionality | Disassociability
SC-3(1) Security Function Isolation | Hardware Separation
SC-3(4) Security Function Isolation | Module Coupling and Cohesiveness
SC-3(5) Security Function Isolation | Layered Structures
SC-6 Resource Availability
SC-7(3) Boundary Protection | Access Points
SC-7(14) Boundary Protection | Protect Against Unauthorized Physical Connections
SC-7(15) Boundary Protection | Networked Privileged Accesses
SC-7(16) Boundary Protection | Prevent Discovery of System Components
SC-7(18) Boundary Protection | Fail Secure
SC-7(19) Boundary Protection | Block Communication from Non-organizationally Configured Hosts
SC-7(21) Boundary Protection | Isolation of System Components
SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains
SC-7(23) Boundary Protection | Disable Sender Feedback on Protocol Validation Failure
SC-7(25) Boundary Protection | Unclassified National Security System Connections
SC-7(26) Boundary Protection | Classified National Security System Connections
SC-7(27) Boundary Protection | Unclassified Non-national Security System Connections
SC-7(29) Boundary Protection | Separate Subnets to Isolate Functions
SC-10 Network Disconnect
SC-11(1) Trusted Path | Irretrievable Communications Path
SC-17 Public Key Infrastructure Certificates
SC-20 Secure Name/address Resolution Service (authoritative Source)
SC-20(2) Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity
SC-21 Secure Name/address Resolution Service (Recursive or Caching Resolver)
SC-22 Architecture and Provisioning for Name/address Resolution Service
SC-23(5) Session Authenticity | Allowed Certificate Authorities
SC-24 Fall in Known State
SC-25 Thin Nodes
SC-26 Decoys
SC-30(2) Concealment and Misdirection | Randomness
SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations
SC-30(4) Concealment and Misdirection | Misleading Information
SC-30(5) Concealment and Misdirection | Concealment of System Components
SC-31 Covert Channel Analysis
SC-31(1) Covert Channel Analysis | Test Covert Channels for Exploitability
SC-31(2) Covert Channel Analysis | Maximum Bandwidth
SC-31(3) Covert Channel Analysis | Measure Bandwidth in Operational Environments
SC-32 System Partitioning
SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions
SC-36 Distributed Processing and Storage
SC-36(1) Distributed Processing and Storage | Polling Techniques
SC-36(2) Distributed Processing and Storage | Synchronization
SC-37 Out-of-band Channels
SC-37(1) Out-of-band Channels | Ensure Delivery and Transmission
SC-38 Operations Security
SC-39(1) Process Isolation | Hardware Separation
SC-39(2) Process Isolation | Separate Execution Domain Per Thread
SC-40(1) Wireless Link Protection | Electromagnetic Interference
SC-40(2) Wireless Link Protection | Reduce Detection Potential
SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception
SC-41 Port and I/O Device Access
SC-42(1) Sensor Capability and Data | Reporting to Authorized Individuals or Roles
SC-42(2) Sensor Capability and Data | Authorized Use
SC-42(4) Sensor Capability and Data | Notice of Collection
SC-42(5) Sensor Capability and Data | Collection Minimization
SC-43 Usage Restrictions
SC-45 System Time Synchronization
SC-45(1) System Time Synchronization | Synchronization with Authoritative Time Source
SC-45(2) System Time Synchronization | Secondary Authoritative Time Source
SC-46 Alternate Communications Paths
SC-48(1) Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities
SC-51 Hardware-based Protection
SI-3(6) Malicious Code Protection | Testing and Verification
SI-4(1) System Monitoring | System-wide Intrusion Detection System
SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-time Analysis
SI-4(3) System Monitoring | Automated Tool and Mechanism Integration
SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic
SI-4(7) System Monitoring | Automated Response to Suspicious Events
SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies
SI-4(12) System Monitoring | Automated Organization-generated Alerts
SI-4(13) System Monitoring | Analyze Traffic and Event Patterns
SI-4(14) System Monitoring | Wireless Intrusion Detection
SI-4(15) System Monitoring | Wireless to Wireline Communications
SI-4(16) System Monitoring | Correlate Monitoring Information
SI-4(17) System Monitoring | Integrated Situational Awareness
SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration
SI-4(20) System Monitoring | Privileged Users
SI-4(22) System Monitoring | Unauthorized Network Services
SI-4(25) System Monitoring | Optimize Network Traffic Analysis
SI-5(1) Security Alerts, Advisories, and Directives | Automated Alerts and Advisories
SI-7(15) Software, Firmware, and Information Integrity | Code Authentication
SI-7(16) Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision
SI-11 Error Handling
SI-13 Predictable Failure Prevention
SI-13(1) Predictable Failure Prevention | Transferring Component Responsibilities
SI-13(3) Predictable Failure Prevention | Manual Supervision
SI-13(4) Predictable Failure Prevention | Standby Component Installation and Notification
SI-13(5) Predictable Failure Prevention | Failover Capability
SI-14 Non-persistence
SI-14(1) Non-persistence | Refresh from Trusted Sources
SI-14(2) Non-persistence | Non-persistent Information
SI-14(3) Non-persistence | Non-persistent Connectivity
SI-15 Information Output Filtering
SI-16 Memory Protection
SI-20 Tainting
SI-21 Information Refresh
SI-22 Information Diversity
SI-23 Information FragmentationDSP-09 Data Protection Impact Assessment
Use of NIST SP 800-53 R5 aligning to CCM v4 GRC Control List

GRC-01 Governance Program Policy and Procedures
- AC-1 Access Control Policy and Procedures
- AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
- AU-1 Audit and Accountability Policy and Procedures
- CA-1 Assessment, Authorization, and Monitoring Policy and Procedures
- CM-1 Configuration Management Policy and Procedures
- CP-1 Contingency Planning Policy and Procedures
- IA-1 Identification and Authentication Policy and Procedures
- IR-1 Incident Response Policy and Procedures
- MA-1 System Maintenance

Policy and Procedures
- MP-1 Media Protection Policy and Procedures
- PE-1 Physical and Environmental Protection Policy and Procedures
- PL-1 Planning Policy and Procedures
- PM-1 Information Security Program Plan
- PM-17 Protecting Controlled Unclassified Information on External Systems
- PS-1 Personnel Security Policy and Procedures
- PT-1 Policy and Procedures
- RA-1 Risk Assessment Policy and Procedures
- SA-1 System and Services Acquisition Policy and Procedures
- SC-1 System and Communications Protection

GRC-02 Risk Management Program
- PL-1 Planning Policy and Procedures
- PL-2 System Security and Privacy Plans
- PM-10 Authorization Process
- PM-17 Protecting Controlled Unclassified Information on External Systems

GRC-03 Organizational Policy Reviews
- PL-1 Planning Policy and Procedures
- SC-1 System and Communications Protection

GRC-04 Policy Exception Process
- PL-1 Planning Policy and Procedures
- PM-14 Testing, Training, and Monitoring
- PM-28 RISK FRAMING
- PM-4 Plan of Action and Milestones Process
- PM-9 Risk Management Strategy
- SR-6.1 Testing and Analysis

GRC-05 Information Security Program
- PL-2 System Security and Privacy Plans
- PM-1 Information Security Program Plan
- PM-14 Testing, Training, and Monitoring
- PM-18 Privacy Program Plan
- PM-3 Information Security and Privacy Resources
- PM-31 CONTINUOUS MONITORING STRATEGY

GRC-06 Governance Responsibility Model
- PM-29 RISK MANAGEMENT PROGRAM LEADERSHIP ROLES

GRC-07 Information System Regulatory Mapping
- PL-1 Planning Policy and Procedures

GRC-08 Special Interest Groups
- PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS
- SI-5 Security Alerts, Advisories, and Directives
Use of NIST SP 800-53 R5 aligning to CCM v4 GRC Controls

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Concerns for Governance, Risk and Compliance - GRC

CCM Focus

• There is one partial gap. GRC-08 Special Interest Groups; although the appendix of NIST 800-53 R5 suggests mapping to ISO/IEC 27002 section 6.1, NIST doesn’t have a specific control for contact with cloud-related special interest groups.

• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards identified in PL – PLANNING, PM – PROGRAM MANAGEMENT.

Consideration for what Never Mapped

No controls were found to be too specific for alignment to the CCM 4.1 matrix.
Use of NIST SP 800-53 R5 aligning to CCM v4 HRS Controls

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)

HRS-06 PS-5 Personnel Transfer
HRS-07 PS-9 Position Descriptions
*addition on 11/24/2021 is reflected on Control list.
Use of NIST SP 800-53 R5 aligning to CCM v4 HRS Control List

HRS-01 Background Screening Policy and Procedures
- IA-12 Identity Proofing
- IA-12.2 Identity Evidence
- IA-12.3 Identity Evidence Validation and Verification
- MA-5 Maintenance Personnel
- MA-5.2 Security Clearances for Classified Systems
- MA-5.3 Citizenship Requirements for Classified Systems
- MA-5.4 Foreign Nationals
- PS-1 Personnel Security Policy and Procedures
- PS-2 Position Risk Designation
- PS-3 Personnel Screening
- PS-3.1 Classified Information
- PS-3.2 Formal Indoctrination
- PS-3.4 Citizenship Requirements

HRS-02 Acceptable Use of Technology Policy and Procedures
- PL-4 Rules of Behavior
- PL-4.1 Social Media and External Site/application Usage Restrictions
- PS-6 Access Agreements
- PS-6.2 Classified Information Requiring Special Protection

HRS-03 Clean Desk Policy and Procedures
- AC-11 Device Lock
- AC-11.1 PATTERN-HIDING DISPLAYS

HRS-04 Remote and Home Working Policy and Procedures
- AC-17 Remote Access
- AC-17.6 PROTECTION OF INFORMATION
- AC-17.9 DISCONNECT/DISABLE ACCESS
- AC-20 Use of External Systems
- AC-20.1 Limits on Authorized Use
- AC-20.2 Portable Storage Devices — Restricted Use
- AC-20.3 Non-organizationally Owned Systems — Restricted Use
- AC-20.4 Network Accessible Storage Devices — Prohibited Use
- AC-20.5 Portable Storage Devices — Prohibited Use
- PE-17 Alternate Work Site
- PS-1 Personnel Security Policy and Procedures
- PS-3 Personnel Termination
- PS-4 Personnel Transfer
- PS-5 Personnel Access
- PS-5.6 Post-employment Requirements
- SI-4 System Monitoring
- SI-4.19 Risk for Individuals
- SI-4.21 Probationary Periods

HRS-05 Asset returns
- PS-1 Personnel Security Policy and Procedures
- PS-4 Personnel Termination
- PS-4.1 Post-employment Requirements
- PS-6 Access Agreements

HRS-06 Employment Termination
- AC-17 Remote Access
- AC-17.9 DISCONNECT/DISABLE ACCESS
- PS-1 Personnel Security Policy and Procedures
- PS-4 Personnel Termination
- PS-4.1 Post-employment Requirements
- PS-4.2 Automated Actions
- PS-5 Personnel Transfer
- PS-6 Access Agreements
- PS-6.3 Post-employment Requirements
- SI-4 System Monitoring
- SI-4.19 Risk for Individuals
- SI-4.21 Probationary Periods

HRS-07 Employment Agreement Process
- MA-5 Maintenance Personnel
- PE-3 Physical Access Control
- PE-3.1 System Access
- PS-1 Personnel Security Policy and Procedures
- PS-3.1 Classified Information
- PS-3.2 Formal Indoctrination
- PS-6 Access Agreements
- PS-6.2 Classified Information Requiring Special Protection
- PS-6.3 Post-employment Requirements

HRS-08 Employment Agreement Content
- PS-6.3 Post-employment Requirements
- PS-7 External Personnel Security

HRS-09 Personnel Roles and Responsibilities
- AC-1 Access Control Policy and Procedures
- AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
- AT-2 Insiders
- AT-2.1 Practical Exercises
- AT-2.2 Insider Threat
- AT-2.3 Social Engineering and Mining
- AT-2.4 Suspicious Communications and Anomalous System Behavior
- AT-2.5 Advanced Persistent Threat
- AT-2.6 Cyber Threat Environment

HRS-10 Non-Disclosure Agreements
- PL-2 System Security and Privacy Plans
- PL-4 Rules of Behavior
- PL-4.1 Social Media and External Site/application Usage Restrictions
- PS-6 Access Agreements
- PS-6.2 Classified Information Requiring Special Protection

HRS-11 Security Awareness Training
- AT-3 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
- AT-2 SECURITY AWARENESS TRAINING
- AT-2.1 Practical Exercises
- AT-2.2 Insider Threat
- AT-2.3 Social Engineering and Mining
- AT-2.4 Suspicious Communications and Anomalous System Behavior
- AT-2.5 Advanced Persistent Threat
- AT-2.6 Cyber Threat Environment

HRS-12 Personal and Sensitive Data Awareness and Training
- AT-3 ROLE-BASED SECURITY TRAINING
- AT-3.1 Environmental Controls
- AT-3.2 Physical Security Controls
- AT-3.3 Practical Exercises
- IR-9 Information Spillage Response
- IR-9.2 Training
- PM-12 Insider Threat Program
- PM-16 Threat Awareness Program
- SR-11 Component Authenticity
- SR-11.1 Anti-counterfeit Training

HRS-13 Compliance User Responsibility
- PL-4 Rules of Behavior
- PL-4.1 Social Media and External Site/application Usage Restrictions
- PS-1 Personnel Security Policy and Procedures
- PS-6 Access Agreements
- PS-6.2 Classified Information Requiring Special Protection

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 HRS Controls

Use of NIST SP 800-53 R5 aligning to CCM v4 HRS Controls

HRS-06 PS-5 Personnel Transfer
HRS-07 PS-9 Position Descriptions
*addition on 11/24/2021 is reflected on Control list but are not reflected in this bar graph.
Concerns for Human Resources - HRS

CCM Focus

• There are no gaps
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards found in the control families:
  • PS - PERSONNEL SECURITY
  • PM - PROGRAM MANAGEMENT
  • PL – PLANNING
  • AT - AWARENESS AND TRAINING

Consideration for what Never Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix, however, organizations may consider adding them if they directly apply to the cloud environments prepared for audit.
• AT-3(5) Role-based Training | Processing Personally Identifiable Information
• PM-2 Information Security Program Leadership Role
• PM-13 Security and Privacy Workforce
• PS-3(3) Personnel Screening | Information Requiring Special Protective Measures

Note that HRS-06 PS-5 Personnel Transfer, and HRS-07 PS-9 Position Descriptions are added on 11/24/2021 and are reflected on the Control list. Total numbers mapped and never mapped are updated however this change is not reflected in all Pie and Bar Charts.
Identity and Access Management - IAM

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO IDENTITY AND ACCESS MANAGEMENT - IAM DOMAIN

Use of NIST SP 800-53 RS aligning to CCM v4 IAM Domain
This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training tool to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 IAM Control List (2)

IAM-11 CSCs Approval for Agreed Privileged Access Roles
- AC-6 Least Privilege
- AC-6.4 Separate Processing Domains
- AC-6.6 Privileged Access by Non-organizational Users
- AU-10 Non-repudiation
- AU-10.4 Validate Binding of Information Reviewer Identity
- CA-6 Authorization
- CA-6.2 Joint Authorization — Inter-organization
- IA-2 Identification and Authentication (Organizational Users)
- IA-2.1 Multi-factor Authentication to Privileged Accounts
- IA-2.12 Acceptance of PIV Credentials
- IA-2.2 Multi-factor Authentication to Non-privileged Accounts

IAM-12 Safeguard Logs Integrity
- AC-2 Account Management
- AC-2.11 Usage Conditions
- AC-2.12 Account Monitoring for Atypical Usage
- IA-8 Identification and Authentication (Non-Organizational Users)
- IA-8.4 Use of Defined Profiles
- SA-8 Security and Privacy Engineering Principles
- SA-8.22 Accountability and Traceability

IAM-13 Uniquely Identifiable Users
- AC-24 Access Control Decisions
- AC-24.2 No User or Process Identity
- AC-3 Access Enforcement
- AC-3.14 Individual Access
- AU-10 Non-repudiation
- AU-10.1 Association of Identities
- IA-2 Identification and Authentication (Organizational Users)
- IA-2.1 Multi-factor Authentication to Privileged Accounts
- IA-2.12 Acceptance of PIV Credentials
- IA-2.2 Multi-factor Authentication to Non-privileged Accounts
- IA-2.8 Access to Accounts — Replay Resistant
- IA-3 Device Identification and Authentication
- IA-3.1 Cryptographic Bidirectional Authentication
- IA-3.2 Device Management
- IA-4.1 Prohibit Account Identifiers as Public Identifiers
- SA-8 Security and Privacy Engineering Principles
- SA-8.22 Accountability and Traceability
- SC-23 Session Authenticity
- SC-23.3 Unique System-generated Session Identifiers
- SC-40 Wireless Link Protection
- SC-40.4 Signal Parameter Identification
- SR-4 Provenance
- SR-4.2 Track and Trace

IAM-14 Strong Authentication
- AC-6 Least Privilege
- AC-6.5 Privileged Accounts
- AC-7 Unsuccessful Logon Attempts
- AC-7.4 Use of Alternate Authentication Factor
- AU-10 Non-repudiation
- AU-10.2 Validate Binding of Information Producer Identity
- IA-2 Identification and Authentication (Organizational Users)
- IA-2.1 Multi-factor Authentication to Privileged Accounts
- IA-2.12 Acceptance of PIV Credentials
- IA-2.2 Multi-factor Authentication to Non-privileged Accounts
- IA-2.8 Access to Accounts — Replay Resistant
- IA-3 Device Identification and Authentication
- IA-3.1 Cryptographic Bidirectional Authentication
- IA-4.1 Prohibit Account Identifiers as Public Identifiers
- SA-8 Security and Privacy Engineering Principles
- SA-8.22 Accountability and Traceability
- SC-23 Session Authenticity
- SC-23.3 Unique System-generated Session Identifiers
- SC-40 Wireless Link Protection
- SC-40.4 Signal Parameter Identification
- SR-4 Provenance
- SR-4.2 Track and Trace

IAM-15 Passwords Management
- IA-5.1 Password-based Authentication
- IA-5.2 Public Key-based Authentication
- IA-5.3 Password Managers
- IA-5.8 Multiple System Accounts

IAM-16 Authorization Mechanisms
- AC-12 Session Termination
- AC-12.1 User-initiated Logouts
- AC-20 Use of External Systems
- AC-20.1 Limits on Authorized Use
- AC-3 Access Enforcement
- AC-3.12 Assert and Enforce Application Access
- AC-3.14 Individual Access
- AC-3.5 Security-relevant Information
- IA-5.7 No Embedded Unencrypted Static Authenticators
- IA-5.9 Federated Credential Management
- IA-8 and Authentication (Non-Organizational Users)
- IA-8.1 Acceptance of PIV Credentials from Other Agencies
- IA-8.6 Disassociability
- SC-23 Session Authenticity
- SC-23.3 Unique System-generated Session Identifiers
- SC-23.5 Unique System-generated Session Identifiers
- SC-40 Wireless Link Protection
- SC-40.4 Signal Parameter Identification
- SR-4 Provenance
- SR-4.2 Track and Trace

IAM-17 Authorization Mechanics
- AC-21 Physical or Logical Separation of Information Flows
- AC-22 Access Only
- AC-6 Least Privilege
- AC-6.8 Privilege Levels for Code Execution
- AC-6.9 Log Use of Privileged Functions
- AU-10 Non-repudiation
- AU-10.1 Association of Identities
- AU-10.2 Validate Binding of Information Producer Identity
- IA-2 Identification and Authentication (Organizational Users)
- IA-2.1 Multi-factor Authentication to Privileged Accounts
- IA-2.12 Acceptance of PIV Credentials
- IA-2.2 Multi-factor Authentication to Non-privileged Accounts
- IA-2.8 Access to Accounts — Replay Resistant
- IA-3 Device Identification and Authentication
- IA-3.1 Cryptographic Bidirectional Authentication
- IA-5 Authenticator Management
- IA-5.1 Password-based Authentication
- IA-5.8 Multiple System Accounts

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.J.T, CISSP, CISA, CFM, CEGIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 IAM Controls
Concerns for Identity and Access Management - IAM

CCM Focus

- There are no gaps
- The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards located in the following control families:
  - AC - ACCESS CONTROL
  - IA - IDENTIFICATION AND AUTHENTICATION

### Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix:

<table>
<thead>
<tr>
<th>Control ID</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2(4)</td>
<td>Account Management</td>
</tr>
<tr>
<td>AC-2(13)</td>
<td>Account Management</td>
</tr>
<tr>
<td>AC-3(9)</td>
<td>Access Enforcement</td>
</tr>
<tr>
<td>AC-3(10)</td>
<td>Access Enforcement</td>
</tr>
<tr>
<td>AC-3(9)</td>
<td>Access Enforcement</td>
</tr>
<tr>
<td>AC-3(10)</td>
<td>Access Enforcement</td>
</tr>
<tr>
<td>AC-4(9)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(11)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(14)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(15)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(20)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(26)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(27)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-4(28)</td>
<td>Information Flow Enforcement</td>
</tr>
<tr>
<td>AC-7(3)</td>
<td>Unsuccessful Logon Attempts</td>
</tr>
<tr>
<td>AC-8</td>
<td>System Use Notification</td>
</tr>
<tr>
<td>AC-9(3)</td>
<td>Previous Logon Notification</td>
</tr>
<tr>
<td>AC-9(2)</td>
<td>Previous Logon Notification</td>
</tr>
<tr>
<td>AC-9(3)</td>
<td>Previous Logon Notification</td>
</tr>
<tr>
<td>AC-9(4)</td>
<td>Previous Logon Notification</td>
</tr>
<tr>
<td>AC-10</td>
<td>Concurrent Session Control</td>
</tr>
<tr>
<td>AC-17(1)</td>
<td>Remote Access</td>
</tr>
<tr>
<td>AC-17(10)</td>
<td>Remote Access</td>
</tr>
<tr>
<td>AC-18(3)</td>
<td>Wireless Access</td>
</tr>
<tr>
<td>AC-18(5)</td>
<td>Wireless Access</td>
</tr>
<tr>
<td>AC-21(1)</td>
<td>Information Sharing</td>
</tr>
<tr>
<td>AC-21(2)</td>
<td>Information Sharing</td>
</tr>
<tr>
<td>AC-22</td>
<td>Publicly Accessible Content</td>
</tr>
<tr>
<td>AC-23</td>
<td>Data Mining Protection</td>
</tr>
<tr>
<td>IA-2(5)</td>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>IA-2(13)</td>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>IA-5(13)</td>
<td>Authenticator Management</td>
</tr>
<tr>
<td>IA-5(17)</td>
<td>Authenticator Management</td>
</tr>
<tr>
<td>IA-6</td>
<td>Authentication Feedback</td>
</tr>
<tr>
<td>IA-9</td>
<td>Service Identification and Authentication</td>
</tr>
<tr>
<td>IA-10</td>
<td>Adaptive Authentication</td>
</tr>
</tbody>
</table>

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ISMS, C Gebit, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 IPY Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 IPY Control List

**IPY-01 Interoperability and Portability Policy and Procedures**
- PT-2 Authority to Process Personally Identifiable Information
- PT-2.1 Data Tagging
- PT-3 Personally Identifiable Information Processing Purposes
- PT-3.1 Data Tagging
- SA-8 Security and Privacy Engineering Principles
- SA-8.8 Secure Evolvability
- SC-27 Platform-Independent Applications
- SC-29 Heterogeneity
- SC-29.1 Virtualization Techniques

**IPY-02 Application Interface Availability**
- CM-13 Data Action Mapping
- PT-2 Authority to Process Personally Identifiable Information
- PT-2.1 Data Tagging
- PT-2.2 Automation
- PT-3 Personally Identifiable Information Processing Purposes
- PT-3.1 Data Tagging
- PT-3.2 Automation
- SA-8 Security and Privacy Engineering Principles
- SA-8.20 Secure Metadata Management

**IPY-03 Secure Interoperability and Portability Management**
*(Organizations may elect to combine this control with DSP-07 Data Protection by Design and Default)*
- PT-2 Authority to Process Personally Identifiable Information
- PT-2.2 Automation
- SA-4 Acquisition Process
- SA-8.20 Secure Metadata Management
- SC-16 Transmission of Security and Privacy Attributes
- SC-16.3 Cryptographic Binding

**IPY-04 Data Portability Contractual Obligations**
*(Organizations may elect to combine this control with STA-09 Primary Service and Contractual Agreement)*
- PT-2 Authority to Process Personally Identifiable Information
- PT-2.1 Data Tagging
- PT-3 Personally Identifiable Information Processing Purposes
- PT-3.1 Data Tagging
- PT-4 Consent
- PT-4.3 Revocation
- SA-4 Acquisition Process
- SA-4.12 Data Ownership
- SI-12 Information Management and Retention
- SI-12.3 Information Disposal
Use of NIST SP 800-53 R5 aligning to CCM v4 IPY Controls
Concerns for Interoperability and Portability - IPY

CCM Focus

• There are no gaps, however four independent teams struggled to align a distinct set of requirements as defined in either the current CSA CCM resources or in a specific single area of the NIST SP 800-53. As a Principle, interoperability and portability exist across many domains.

• While the Security Guidance for Critical Areas of Focus in Cloud Computing | CSA (cloudsecurityalliance.org) identifies the need for interoperability, and where portability lists as a requirement of GDPR, HIPAA, and GLBA, and now in the EO 14028 the methods IPY controls achievement are buried within Software Engineering (AIS), Data Security and Privacy (DSP) and are implied by contract within Supply Chain domains SR and STA-09.

• The CCM NIST WG suggests IPY-03 be combined to DSP-07 as implementation guidance, and that IPY-04 be combined as implementation guidance for STA-09. Having found no distinct mappings for these two controls, it is suggested they be withdrawn from future CCM.

• The CCM NIST WG suggests that the Implementation Guidance, Security Guidance for Critical Areas of Focus in Cloud, and Audit Guidance undergo improvements to define what is expected for IPY and what would stand as reasonable evidence within this control domain.

Consideration for what Never Mapped

Suggesting that NIST 800-53 consider adding a control enhancement to SR-12 that would support the IPY-04 requirement

Agreements must include provisions specifying CSCs access to data upon contract termination and will include:

a. Data format
b. Length of time the data will be stored
c. Scope of the data retained and made available to the CSCs
d. Data deletion policy

Never mapped

• SR-12 Component Disposal. This relates to the suggested details for removing information upon CSC contract termination.
Infrastructure and Virtualization Security - IVS

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO THE INFRASTRUCTURE AND VIRTUALIZATION SECURITY - IVS DOMAIN

Use of NIST SP 800-53 R5 aligning to CCM v4 IVS Domain
Use of NIST SP 800-53 R5 aligning to CCM v4 IVS Controls

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 IVS Control List

IVS-01 Infrastructure and Virtualization Security Policy and Procedures
- AC-1 Access Control Policy and Procedures
- CM-1 Configuration Management Policy and Procedures
- IA-1 Identification and Authentication Policy and Procedures
- RA-1 Risk Assessment Policy and Procedures
- SA-1 System and Services Acquisition Policy and Procedures
- SC-1 System and Communications Protection Policy and Procedures
- SC-46
- SC-49 Hardware-enforced Separation and Policy Enforcement
- SC-50 Software-enforced Separation and Policy Enforcement
- SI-1 System and Information Integrity Policy and Procedures

IVS-02 Capacity and Resource Planning
- CP-2 Contingency Plan
- CP-2.2 Capacity Planning
- SC-4 Information in Shared Systems Resources
- SC-5 Denial of Service Protection
- SC-5.2 Capacity, Bandwidth, and Redundancy
- SI-4 System Monitoring
- SI-3 System Monitoring

IVS-03 Network Security
- SC-1 System and Communications Protection Policy and Procedures
- SC-11 Trusted Path
- SC-12 Cryptographic Key Establishment and Management
- SC-16 Transmission of Security and Privacy Attributes
- SC-23 Session Authenticity
- SC-29 Heterogeneity
- SC-29.1 Virtualization Techniques
- SC-4 Information in Shared Systems Resources
- SC-40 Wireless Link Protection
- SC-7 Boundary Protection
- SC-7.11 Restrict Incoming Communications Traffic
- SC-7.4 External Telecommunications Services
- SC-7.5 Deny by Default — Allow by Exception
- SC-7.8 Route Traffic to Authenticated Proxy Servers
- SC-7.9 Restrict Threatening Outgoing Communications Traffic
- SC-8 Transmission Confidentiality and Integrity
- SC-8.1 Cryptographic Protection
- SC-23 Session Authenticity
- SC-29 Heterogeneity
- SC-29.1 Virtualization Techniques
- SC-3 Security Function Isolation
- SC-3.2 Access and Flow Control Functions
- SC-2 Application Partitioning
- SC-29 Heterogeneity
- SC-29.1 Virtualization Techniques
- SC-30 Concealment and Misdirection
- SC-34 Non-Modifiable Executable Programs
- SC-35 Honeyclients
- SC-39 Process Isolation
- SC-44 Detonation Chambers
- SC-7 Boundary Protection
- SC-7.12 Host-based Protection

IVS-04 OS Hardening and Base Controls
- CM-6 Configuration Settings
- CM-6.1 Automated Management, Application, and Verification
- SC-7.6 Cryptographic Protection
- SC-7.7 Integration of Detection and Response
- SC-7.8 Auditing Capability for Significant Events
- SC-7.9 Verify Boot Process

IVS-05 Production and Non-Production Environments
- CM-2 Baseline Configuration
- CM-2.6 Development and Test Environments
- CM-5 Access Restrictions for Change
- CM-5.5 Privilege Limitation for Production and Operation
- SA-3 System Development Life Cycle
- SA-3.1 Manage Preproduction Environment
- SC-8 Security and Privacy Engineering Principles
- SA-8.1 Clear Abstractions
- SA-8.2 Least Common Mechanism
- SA-8.3 Modularity and Layering
- SA-8.6 Minimized Sharing
- SC-3 Security Function Isolation
- SC-3.2 Access and Flow Control Functions
- SC-2 Application Partitioning
- SC-29 Heterogeneity
- SC-29.1 Virtualization Techniques
- SC-30 Concealment and Misdirection
- SC-34 Non-Modifiable Executable Programs
- SC-35 Honeyclients
- SC-39 Process Isolation
- SC-44 Detonation Chambers
- SC-7 Boundary Protection
- SC-7.12 Host-based Protection

IVS-06 Segmentation and Segregation
- SC-3 Security Function Isolation
- SC-7 Boundary Protection
- SC-7.20 Dynamic Isolation and Segregation

IVS-07 Migration to Cloud Environments
- AC-17 Remote Access
- AC-20 Use of External Systems
- SC-12 Cryptographic Key Establishment and Management
- SC-23 Session Authenticity
- SC-29 Heterogeneity
- SC-7 Boundary Protection
- SC-7.28 Connections to Public Networks
- SC-8 Transmission Confidentiality and Integrity
- SC-8.1 Cryptographic Protection
- SI-7.9 Verify Boot Process

IVS-08 Network Architecture Documentation
- PL-8 Security and Privacy Architectures
- PL-8.1 Defense in Depth
- SA-8 Security and Privacy Engineering Principles
- SA-8.17 Secure Distributed Composition
- SA-8.3 Modularity and Layering

IVS-09 Network Defense
- PL-8 Security and Privacy Architectures
- PL-8.1 Defense in Depth
- SC-5 Denial of Service Protection
- SC-5.1 Restrict Ability to Attack Other Systems
- SC-5.3 Detection and Monitoring
- SC-7 Boundary Protection
Use of NIST SP 800-53 R5 aligning to CCM v4 IVS Controls
CCM Focus

• There is one partial gap. For IVS-01, Virtualization is not allocated to have its own policies and procedures. Domains AC, CM, IA, RA, SA, SC and SI have considerations for Virtualization, however CCM asks for one overarching policy which the client may have to derive from all of those areas. It would be simpler to write a virtualization policy and within that reference the array of existing related procedures.

• Systems and Communications Domain provides the largest number of granular controls. With 51 mapped SC items, many remain unmapped.

• Security Guidance for Critical Areas of Focus in Cloud Computing | CSA (cloudsecurityalliance.org) provides extensive guidance to the design and operation of infrastructure and virtual security. NIST controls provide guidance for Virtual Systems regardless of their existence as part of Cloud Services. Care to limit NIST controls to the CCM context is advised.

• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards most identified in the following domains:
  • SC - SYSTEM AND COMMUNICATIONS PROTECTION
  • SI - SYSTEM AND INFORMATION INTEGRITY
  • SA - SYSTEM AND SERVICES ACQUISITION

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix.

• SC-2(1) Separation of System and User Functionality | Interfaces for Non-privileged Users
• SC-2(2) Separation of System and User Functionality | Disassociability
• SC-3(1) Security Function Isolation | Hardware Separation
• SC-3(4) Security Function Isolation | Module Coupling and Cohesiveness
• SC-3(5) Security Function Isolation | Layered Structures
• SC-17 Public Key Infrastructure Certificates
• SC-32 System Partitioning
• SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions
• SC-36 Distributed Processing and Storage
• SC-36(1) Distributed Processing and Storage | Polling Techniques
• SC-36(2) Distributed Processing and Storage | Synchronization
• SC-39(1) Process Isolation | Hardware Separation
• SC-39(2) Process
Logging and Monitoring - LOG

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO THE LOGGING AND MONITORING - LOG DOMAIN

Use of NIST SP 800-53 RS aligning to CCM v4 LOG Domain

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 LOG Domain
## Use of NIST SP 800-53 R5 aligning to CCM v4 LOG Control List

### LOG-01 Logging and Monitoring Policy and Procedures
- AU-1 Audit and Accountability Policy and Procedures

### LOG-02 Audit Logs Protection
- AU-11 Audit Record Retention
- AU-4 Audit Storage Capacity

### LOG-03 Security Monitoring and Alerting
- AU-13 Monitoring for Information Disclosure
- AU-5 Response to Audit Processing Failures
- AU-5.2 Real-time Alerts

### LOG-04 Audit Logs Access and Accountability
- AU-10 Non-repudiation
- AU-9 Protection of Audit Information
- AU-9.4 Access by Subset of Privileged Users

### LOG-05 Audit Logs Monitoring and Response
- AU-6 Audit Review, Analysis, and Reporting
- AU-6.1 Automated Process Integration
- AU-6.5 Integrated Analysis of Audit Records

### LOG-06 Clock Synchronization
- AU-8 Time Stamps

### LOG-07 Logging Scope
- AU-1 Audit and Accountability Policy and Procedures
- AU-14 Session Audit
- AU-16 Cross-Organizational Auditing

### LOG-08 Log Records
- AU-12 Audit Generation
- AU-12.1 System-wide and Time-correlated Audit Trail
- AU-12.2 Standardized Formats
- AU-12.3 Changes by Authorized Individuals
- AU-3 Content of Audit Records
- AU-3.1 Additional Audit Information
- AU-3.3 Limit Personally Identifiable Information Elements
- AU-6 Audit Review, Analysis, and Reporting
- AU-6.8 Full Text Analysis of Privileged Commands

### LOG-09 Log Protection
- AU-12 Audit Generation
- AU-12.2 Standardized Formats
- AU-12.3 Changes by Authorized Individuals
- AU-9 Protection of Audit Information
- AU-9.1 HARDWARE WRITE-ONCE MEDIA
- AU-9.2 AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS
- AU-9.3 CRYPTOGRAPHIC PROTECTION
- AU-9.4 Access by Subset of Privileged Users

### LOG-10 Encryption Monitoring and Reporting
- AU-9 Protection of Audit Information
- AU-9.3 CRYPTOGRAPHIC PROTECTION
- AU-9.6 Read-only Access

### LOG-11 Transaction/Activity Logging
- AU-9 Protection of Audit Information
- AU-9.3 CRYPTOGRAPHIC PROTECTION

### LOG-12 Access Control Logs
- AU-14 Session Audit
- AU-6 Audit Review, Analysis, and Reporting
- AU-6.6 Correlation with Physical Monitoring
- PE-3 Physical Access Control

### LOG-13 Failures and Anomalies Reporting
- AU-16 Cross-Organizational Auditing
- AU-5 Response to Audit Processing Failures
- AU-5.2 Real-time Alerts
- AU-6 Audit Review, Analysis, and Reporting
- AU-6.3 Correlate Audit Record Repositories
- AU-6.4 Central Review and Analysis
- AU-6.5 Integrated Analysis of Audit Records
Use of NIST SP 800-53 R5 aligning to CCM v4 LOG Controls

Use of NIST SP 800-53 R5 aligning to CCM v4 LOG Controls

Control Family and Enhancements

Use of NIST SP 800-53 R5 aligning to CCM v4 LOG Controls

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Concerns for Logging and Monitoring - LOG

CCM Focus

• There are no gaps

• Given 48 mapped items from NIST it is noteworthy that although CCM does not require the additional 19 unmapped items, some of these would support elements of SEF and DSP so may be considered “good practice”.

• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards located in the AU - AUDIT AND ACCOUNTABILITY domain.

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix

AU-2 Event Logging
AU-4(1) Audit Log Storage Capacity | Transfer to Alternate Storage
AU-5(1) Response to Audit Logging Process Failures | Storage Capacity Warning
AU-5(3) Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds
AU-5(4) Response to Audit Logging Process Failures | Shutdown on Failure
AU-5(5) Response to Audit Logging Process Failures | Alternate Audit Logging Capability

AU-6(7) Audit Record Review, Analysis, and Reporting | Permitted Actions
AU-6(9) Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources
AU-7 Audit Record Reduction and Report Generation
AU-7(1) Audit Record Reduction and Report Generation | Automatic Processing
AU-9(5) Protection of Audit Information | Dual Authorization
AU-9(7) Protection of Audit Information | Store on Component with Different Operating System

AU-10(3) Non-repudiation | Chain of Custody
AU-11(1) Audit Record Retention | Long-term Retrieval Capability
AU-12(4) Audit Record Generation | Query Parameter Audits of Personally Identifiable Information
AU-14(1) Session Audit | System Start-up
AU-14(3) Session Audit | Remote Viewing and Listening
AU-16(2) Cross-organizational Audit Logging | Sharing of Audit Information
AU-16(3) Cross-organizational Audit Logging | Disassociability
Security Incident Management, E-Discovery, and Cloud Forensics - SEF

Use of NIST SP 800-53 RS aligning to CCM v4 SEF Domain

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO THE SECURITY INCIDENT MANAGEMENT, E-DISCOVERY, AND CLOUD FORENSICS - SEF DOMAIN

Use of NIST SP 800-53 RS aligning to CCM v4 SEF Domain

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 SEF Controls
Use of NIST SP 800-53 R5 aligning to CCM v4 SEF Control List

**SEF-01 Security Incident Management Policy and Procedures**
- IR-1 Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-2.1 Simulated Events
- IR-2.2 Automated Training Environments
- IR-4 Incident Handling
- IR-4.12 Malicious Code and Forensic Analysis
- IR-4.14 Security Operations Center
- PM-1 Information Security Program Plan
- PM-12 Insider Threat Program
- SC-42 Sensor Capability and Data
- SC-48 Sensor Relocation

**SEF-02 Service Management Policy and Procedures**
- IR-4 Incident Handling
- IR-4.1 Automated Incident Handling Processes
- IR-4.14 Security Operations Center
- IR-4.2 Dynamic Reconfiguration
- IR-4.3 Continuity of Operations
- IR-4.6 Insider Threats
- PM-1 Information Security Program Plan
- PM-6 Measures of Performance

**SEF-03 Incident Response Plans**
- IR-1 Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-2.1 Simulated Events
- IR-2.2 Automated Training Environments
- IR-2.3 Breach
- IR-3 Incident Response Testing
- IR-3.1 Automated Testing
- IR-3.2 Coordination with Related Plans
- IR-3.3 Continuous Improvement
- IR-4 Incident Handling
- IR-4.1 Automated Incident Handling Processes
- IR-4.10 Supply Chain Coordination
- IR-4.11 Integrated Incident Response Team
- IR-4.12 Malicious Code and Forensic Analysis
- IR-4.13 Behavior Analysis
- IR-4.14 Security Operations Center
- IR-4.15 Public Relations and Reputation Repair
- IR-4.2 Dynamic Reconfiguration
- IR-4.3 Continuity of Operations
- IR-4.4 Information Correlation
- IR-4.5 Automatic Disabling of System
- IR-4.6 Insider Threats
- IR-4.7 Insider Threats — Intra-organization Coordination
- IR-4.8 Correlation with External Organizations
- IR-4.9 Dynamic Response Capability
- IR-5 Incident Monitoring
- IR-5.1 Automated Tracking, Data Collection, and Analysis
- IR-6 Incident Reporting
- IR-6.1 Automated Reporting
- IR-6.2 Vulnerabilities Related to Incidents
- IR-6.3 Supply Chain Coordination
- IR-6.4 External Incident Notification
- IR-7 Incident Response Assistance
- IR-7.1 Automation Support for Availability of Information and Support
- IR-7.2 Coordination with External Providers
- IR-8.1 Breaches
- IR-9 Information Spillage Response
- IR-9.2 Training
- IR-9.3 Post-s spill Operations
- IR-9.4 Exposure to Unauthorized Personnel
- SA-15.10 INCIDENT RESPONSE PLAN

**SEF-04 Incident Response Testing**
- IR-2 Incident Response Training
- IR-2.1 Simulated Events
- IR-2.2 Automated Training Environments
- IR-2.3 Breach
- IR-3 Incident Response Testing
- IR-3.1 Automated Testing
- IR-3.2 Coordination with Related Plans
- IR-3.3 Continuous Improvement
- IR-8 Incident Response Plan
- IR-9 Information Spillage Response
- IR-9.2 Training

**SEF-05 Incident Response Metrics**
- CA-7 Continuous Monitoring
- CA-7.3 Trend Analyses
- CA-7.4 Risk Monitoring
- CA-7.5 Consistency Analysis
- CA-7.6 Automation Support for Monitoring
- IR-4 Incident Handling
- IR-4.1 Automated Incident Handling Processes
- IR-4.12 Malicious Code and Forensic Analysis
- IR-4.13 Behavior Analysis
- IR-4.3 Continuity of Operations
- IR-4.4 Information Correlation
- IR-4.5 Dynamic Response Capability
- IR-4.6 Insider Threats
- IR-4.7 Insider Threats — Intra-organization Coordination
- IR-4.8 Correlation with External Organizations
- IR-4.9 Dynamic Response Capability
- IR-6 Incident Reporting
- IR-6.3 Supply Chain Coordination

**SEF-06 Event Triage Processes**
- CA-7 Continuous Monitoring
- CA-7.3 Trend Analyses
- CA-7.4 Risk Monitoring
- CA-7.5 Consistency Analysis
- CA-7.6 Automation Support for Monitoring
- IR-4 Incident Handling
- IR-4.1 Automated Incident Handling Processes
- IR-4.12 Malicious Code and Forensic Analysis
- IR-4.13 Behavior Analysis
- IR-4.3 Continuity of Operations
- IR-4.4 Information Correlation
- IR-4.5 Dynamic Response Capability
- IR-4.6 Insider Threats
- IR-4.7 Insider Threats — Intra-organization Coordination
- IR-4.8 Correlation with External Organizations
- IR-4.9 Dynamic Response Capability
- IR-6 Incident Reporting
- IR-6.3 Supply Chain Coordination

**SEF-07 Security Breach Notification**
- AU-13 Monitoring for Information Disclosure
- AU-13.1 Use of Automated Tools
- AU-13.2 Review of Monitored Sites
- AU-13.3 Unauthorized Replication of Information
- IR-4 Incident Handling
- IR-4.1 Automated Incident Handling Processes
- IR-4.15 Public Relations and Reputation Repair
- IR-4.6 Insider Threats
- IR-6.3 Incident Reporting

**SEF-08 Points of Contact Maintenance**
- IR-4 Incident Handling
- IR-4.10 Supply Chain Coordination
- IR-4.15 Public Relations and Reputation Repair
- IR-4.6 Insider Threats
- IR-4.7 Insider Threats — Intra-organization Coordination
- IR-4.8 Correlation with External Organizations
- IR-7 Incident Response Assistance
- IR-7.1 Automation Support for Availability of Information and Support
- IR-7.2 Coordination with External Providers
- MA-3.4 Restricted Tool Use
- MA-4.5 Approvals and Notifications
- MA-5.5 Non-system Maintenance
- PM-21 ACCOUNTING OF DISCLOSURES
- PM-23 DATA GOVERNANCE BODY

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training tool to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ISMS, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 SEF Domain

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Concerns for Security Incident Management, E-Discovery, and Cloud Forensics - SEF

CCM Focus

• There is one partial gap, SEF-01 Security Incident Management Policy and Procedures, which requires an E-Discovery Policy. This type of policy is normally required in Federal Space so may be aligned to FedRamp guidance; however, it is not explicitly called out by a NIST 800-53 control.

• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards primarily found in the IR - INCIDENT RESPONSE domain.

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix. In some cases, these controls may support the LOG, SEF, and TVM domains.

• SI-4(1) System Monitoring | System-wide Intrusion Detection System
• SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-time Analysis
• SI-4(3) System Monitoring | Automated Tool and Mechanism Integration
• SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic
• SI-4(7) System Monitoring | Automated Response to Suspicious Events
• SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies
• SI-4(12) System Monitoring | Automated Organization-generated Alerts
• SI-4(13) System Monitoring | Analyze Traffic and Event Patterns
• SI-4(14) System Monitoring | Wireless Intrusion Detection
• SI-4(15) System Monitoring | Wireless to Wireline Communications
• SI-4(16) System Monitoring | Correlate Monitoring Information
• SI-4(17) System Monitoring | Integrated Situational Awareness
• SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration
• SI-4(20) System Monitoring | Privileged Users
• SI-4(22) System Monitoring | Unauthorized Network Services
• SI-4(25) System Monitoring | Optimize Network Traffic Analyses
Supply Chain Management, Transparency, and Accountability - STA

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO THE SUPPLY CHAIN MANAGEMENT, TRANSPARENCY, AND ACCOUNTABILITY - STA DOMAIN

Use of NIST SP 800-53 RS aligning to CCM v4 STA Domain
### Use of NIST SP 800-53 R5 aligning to CCM v4 STA Control List

<table>
<thead>
<tr>
<th>STA-01</th>
<th>SSMR Policy and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-30</td>
<td>SUPPLY CHAIN RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>SA-4</td>
<td>Acquisition Process</td>
</tr>
<tr>
<td>SA-4.1</td>
<td>Functional Properties of Controls</td>
</tr>
<tr>
<td>SA-4.10</td>
<td>Use of Approved PIV Products</td>
</tr>
<tr>
<td>SA-4.2</td>
<td>Design and Implementation Information for Controls</td>
</tr>
<tr>
<td>SA-4.5</td>
<td>System, Component, and Service Configurations</td>
</tr>
<tr>
<td>SA-4.9</td>
<td>Functions, Ports, Protocols, and Services in Use</td>
</tr>
<tr>
<td>SR-1</td>
<td>Policy and Procedures</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-3</td>
<td>Supply Chain Controls and Processes</td>
</tr>
<tr>
<td>SR-5</td>
<td>Acquisition Strategies, Tools, and Methods</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-02</th>
<th>SSMR Supply Chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-30</td>
<td>SUPPLY CHAIN RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>SR-1</td>
<td>Policy and Procedures</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-3</td>
<td>Supply Chain Controls and Processes</td>
</tr>
<tr>
<td>SR-5</td>
<td>Acquisition Strategies, Tools, and Methods</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-03</th>
<th>SSMR Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-30</td>
<td>SUPPLY CHAIN RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>SR-1</td>
<td>Policy and Procedures</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-2.1</td>
<td>Establish SCRM Team</td>
</tr>
<tr>
<td>SR-3</td>
<td>Supply Chain Controls and Processes</td>
</tr>
<tr>
<td>SR-3.1</td>
<td>Diverse Supply Base</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-04</th>
<th>SSMR Control Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-1</td>
<td>Policy and Procedures</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-2.1</td>
<td>Establish SCRM Team</td>
</tr>
<tr>
<td>SR-3</td>
<td>Supply Chain Controls and Processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-05</th>
<th>SSMR Documentation Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-1</td>
<td>Policy and Procedures</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-3</td>
<td>Supply Chain Controls and Processes</td>
</tr>
<tr>
<td>SR-6</td>
<td>Supplier Assessments and Reviews</td>
</tr>
<tr>
<td>SR-6.1</td>
<td>Testing and Analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-06</th>
<th>SSMR Control Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-4</td>
<td>Acquisition Process</td>
</tr>
<tr>
<td>SA-4.11</td>
<td>System of Records</td>
</tr>
<tr>
<td>SR-1</td>
<td>Policy and Procedures</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-3</td>
<td>Supply Chain Controls and Processes</td>
</tr>
<tr>
<td>SR-3.1</td>
<td>Diverse Supply Base</td>
</tr>
<tr>
<td>SR-3.2</td>
<td>Limitation of Harm</td>
</tr>
<tr>
<td>SR-3.3</td>
<td>Sub-tier Flow Down</td>
</tr>
<tr>
<td>SR-5</td>
<td>Acquisition Strategies, Tools, and Methods</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-07</th>
<th>Supply Chain Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-8</td>
<td>System Component Inventory</td>
</tr>
<tr>
<td>CM-8.4</td>
<td>Accountability Information</td>
</tr>
<tr>
<td>SR-4</td>
<td>Provenance</td>
</tr>
<tr>
<td>SR-4.1</td>
<td>Identity</td>
</tr>
<tr>
<td>SR-4.2</td>
<td>Track and Trace</td>
</tr>
<tr>
<td>SR-4.3</td>
<td>Validate as Genuine and Not Altered</td>
</tr>
<tr>
<td>SR-4.4</td>
<td>Supply Chain Integrity — Pedigree</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-08</th>
<th>Supply Chain Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-2.1</td>
<td>Establish SCRM Team</td>
</tr>
<tr>
<td>SR-4</td>
<td>Provenance</td>
</tr>
<tr>
<td>SR-5</td>
<td>Acquisition Strategies, Tools, and Methods</td>
</tr>
<tr>
<td>SR-5.1</td>
<td>Adequate Supply</td>
</tr>
<tr>
<td>SR-5.2</td>
<td>Assessments Prior to Selection, Acceptance, Modification, or Update</td>
</tr>
<tr>
<td>SR-6</td>
<td>Supplier Assessments and Reviews</td>
</tr>
<tr>
<td>SR-6.1</td>
<td>Testing and Analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-09</th>
<th>Primary Service and Contractual Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-4</td>
<td>Acquisition Process</td>
</tr>
<tr>
<td>SA-4.1</td>
<td>Functional Properties of Controls</td>
</tr>
<tr>
<td>SA-4.10</td>
<td>Use of Approved PIV Products</td>
</tr>
<tr>
<td>SA-4.2</td>
<td>Design and Implementation Information for Controls</td>
</tr>
<tr>
<td>SA-4.5</td>
<td>System, Component, and Service Configurations</td>
</tr>
<tr>
<td>SA-4.9</td>
<td>Functions, Ports, Protocols, and Services in Use</td>
</tr>
<tr>
<td>SR-8</td>
<td>Notification Agreements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-10</th>
<th>Supply Chain Agreement Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-30</td>
<td>SUPPLY CHAIN RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>PM-30.1</td>
<td>Suppliers of Critical or Mission-essential Items</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-6</td>
<td>Supplier Assessments and Reviews</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-11</th>
<th>Internal Compliance Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-30</td>
<td>SUPPLY CHAIN RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>PM-30.1</td>
<td>Suppliers of Critical or Mission-essential Items</td>
</tr>
<tr>
<td>SR-2.1</td>
<td>Establish SCRM Team</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-12</th>
<th>Supply Chain Service Agreement Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-9</td>
<td>External System Services</td>
</tr>
<tr>
<td>SA-9.5</td>
<td>Processing, Storage, and Service Location</td>
</tr>
<tr>
<td>SR-6</td>
<td>Supplier Assessments and Reviews</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Governance Review</td>
</tr>
<tr>
<td>SA-9.1</td>
<td>Risk Assessments and Organizational Approvals</td>
</tr>
<tr>
<td>SA-9.2</td>
<td>Identification of Functions, Ports, Protocols, and Services</td>
</tr>
<tr>
<td>SA-9.3</td>
<td>Establish and Maintain Trust Relationship with Providers</td>
</tr>
<tr>
<td>SA-9.4</td>
<td>Consistent Interests of Consumers and Providers</td>
</tr>
<tr>
<td>SA-9.5</td>
<td>Processing, Storage, and Service Location</td>
</tr>
<tr>
<td>SA-9.6</td>
<td>Organization-controlled Cryptographic Keys</td>
</tr>
<tr>
<td>SA-9.7</td>
<td>Organization-controlled Integrity Checking</td>
</tr>
<tr>
<td>SA-9.8</td>
<td>Processing and Storage Location — U.S. Jurisdiction</td>
</tr>
<tr>
<td>SR-2</td>
<td>Supply Chain Risk Management Plan</td>
</tr>
<tr>
<td>SR-2.1</td>
<td>Establish SCRM Team</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-13</th>
<th>Supply Chain Data Security Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-23</td>
<td>DATA GOVERNANCE BODY</td>
</tr>
<tr>
<td>PM-30</td>
<td>SUPPLY CHAIN RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>SA-9</td>
<td>External System Services</td>
</tr>
<tr>
<td>SA-9.5</td>
<td>Processing, Storage, and Service Location</td>
</tr>
<tr>
<td>SR-6</td>
<td>Supplier Assessments and Reviews</td>
</tr>
<tr>
<td>SR-6.1</td>
<td>Testing and Analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STA-14</th>
<th>Supply Chain Governance Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-9.1</td>
<td>Risk Assessments and Organizational Approvals</td>
</tr>
<tr>
<td>SA-9.2</td>
<td>Identification of Functions, Ports, Protocols, and Services</td>
</tr>
<tr>
<td>SA-9.3</td>
<td>Establish and Maintain Trust Relationship with Providers</td>
</tr>
<tr>
<td>SA-9.4</td>
<td>Consistent Interests of Consumers and Providers</td>
</tr>
<tr>
<td>SA-9.5</td>
<td>Processing, Storage, and Service Location</td>
</tr>
<tr>
<td>SA-9.6</td>
<td>Organization-controlled Cryptographic Keys</td>
</tr>
</tbody>
</table>

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. is a TM belonging to Robin Basham, M.Ed., M.I.T, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 STA Controls
Concerns for Supply Chain Management, Transparency, and Accountability - STA

CCM Focus - CCM V4 SSRM Focus

Two full gaps, and six partial gaps exist in the STA domain. Each control has mapped areas that address part of the requirement; however, they lack policy and process related to the CSP’s customer security responsibilities. Without this detail, even with fully implemented mappings the CCM control would have a partial or full failure when used alone as the evidence and response for this domain of the CAIQ.

Issue: NIST 800-53 has several high-level controls (and reference NIST.SP.800-161) that can be construed to include cloud SSRM concepts and management among their broader supply chain risk management requirements. However, 800-53 does not have controls that specifically or precisely address the cloud shared security responsibility model (SSRM) and requirements for CSPs to delineate customer security responsibilities specifically the way that FedRamp and the CSA CCM V4 does. In addition to the recommended mapping, this would need to be added to policy and artifacts.

In the US Federal/FISMA space, cloud-specific requirements are generally addressed by the FedRAMP PMO rather than NIST. FedRAMP does have mature artifacts and repeatable processes for SSRM execution (i.e., the CIS & CRM and FedRAMP SSP artifacts) and management - albeit at the program rather than in specific SSRM-related controls.

Impact:
- STA-01 SSRM Policy and Procedures (Partial Gap)
- STA-02 SSRM Supply Chain (Partial Gap)
- STA-03 SSRM Guidance (Full Gap)
- STA-04 SSRM Control Ownership (Full Gap)
- STA-05 SSRM Documentation Review (Partial Gap)
- STA-06 SSRM Control Implementation (Partial Gap)
- STA-09 Primary Service and Contractual Agreement (Partial Gap)

The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards found in the SR - SUPPLY CHAIN RISK MANAGEMENT domain.

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix and could potentially align with programs that would supply a missing CSP administrative interface requirement, they are explicitly tied to the CSP customer responsibility so are not mapped to CCM.

- SA-4(6) Acquisition Process | Use of Information Assurance Products
- SA-4(7) Acquisition Process | NIAP-approved Protection Profiles
- SA-8(21) Security and Privacy Engineering Principles | Self-analysis

- SA-10(2) Developer Configuration Management | Alternative Configuration Management Processes
- SA-10(6) Developer Configuration Management | Trusted Distribution
- SA-20 Customized Development of Critical Components
- SA-21 Developer Screening
- SA-22 Unsupported System Components
- SA-23 Specialization
- SR-10 Inspection of Systems or Components
- SR-12 Component Disposal
Threat and Vulnerability Management - TVM

Use of NIST SP 800-53 R5 aligning to CCM v4 TVM Domain

NIST CONTROL FAMILIES AND THE PERCENTAGE OF USE IN MAPPING TO THE THREAT AND VULNERABILITY MANAGEMENT - TVM DOMAIN

Use of NIST SP 800-53 R5 aligning to CCM v4 TVM Domain
Use of NIST SP 800-53 R5 aligning to CCM v4 TVM Control List

TVM-01 Threat and Vulnerability Management Policy and Procedures
- PM-16 Threat Awareness Program
- PM-16.1 Automated Means for Sharing Threat Intelligence
- PM-31 CONTINUOUS MONITORING STRATEGY
- RA-5 Vulnerability Scanning
- RA-5.5 Privileged Access
- SA-11 Developer Security Testing and Evaluation
- SA-11.2 Threat Modeling and Vulnerability Analyses
- SA-11.5 Penetration Testing
- SA-15 Development Process, Standards, and Tools
- SA-15.5 ATTACK SURFACE REDUCTION
- SA-15.8 REUSE OF THREAT / VULNERABILITY INFORMATION

TVM-02 Malware Protection Policy and Procedures
- RA-3 Risk Assessment
- RA-3.3 Dynamic Threat Awareness
- RA-5 Vulnerability Scanning
- RA-5.3 Breadth and Depth of Coverage
- RA-5.5 Privileged Access
- SI-3 Malicious Code Protection
- SI-3.10 Malicious Code Analysis

TVM-03 Vulnerability Remediation Schedule
- RA-3 Risk Assessment
- RA-3.1 Supply Chain Risk Assessment
- RA-5 Vulnerability Scanning
- RA-5.2 Update Vulnerabilities to Be Scanned
- RA-5.3 Breadth and Depth of Coverage
- RA-5.4 Discoverable Information
- RA-5.6 Automated Trend Analyses
- SI-3 Malicious Code Protection
- SI-3.10 Malicious Code Analysis

TVM-04 Detection Updates
- CM-7 Least Functionality
- CM-7.4 Unauthorized Software
- RA-3 Risk Assessment
- RA-3.3 Dynamic Threat Awareness
- RA-5 Vulnerability Scanning
- RA-5.2 Update Vulnerabilities to Be Scanned
- SA-10 Developer Configuration Management
- SA-10.5 Mapping Integrity for Version Control
- SA-11 Developer Security Testing and Evaluation
- SA-11.2 Threat Modeling and Vulnerability Analyses

TVM-05 External Library Vulnerabilities
- SI-8.2 Automatic Updates
- SI-8.3 Continuous Learning Capability
- TVM-05 External Library Vulnerabilities
- RA-5 Vulnerability Scanning
- RA-5.3 Breadth and Depth of Coverage
- SA-11 Developer Security Testing and Evaluation
- SA-11.2 Threat Modeling and Vulnerability Analyses
- SA-11.5 Penetration Testing

TVM-06 Penetration Testing
- CA-8 Penetration Testing
- CA-8.1 Independent Penetration Testing Agent or Team
- CA-8.2 Red Team Exercises
- CA-8.3 Facility Penetration Testing
- SA-11 Developer Security Testing and Evaluation
- SA-11.2 Threat Modeling and Vulnerability Analyses
- SA-11.5 Penetration Testing
- TVM-07 Vulnerability Identification
- RA-5 Vulnerability Scanning
- RA-5.4 Discoverable Information
- RA-5.5 Privileged Access
- SA-11 Developer Security Testing and Evaluation
- SA-11.5 Penetration Testing
- SA-15.5 ATTACK SURFACE REDUCTION
- SC-7 Boundary Protection
- SC-7.10 Prevent Exfiltration
- SI-3 Malicious Code Protection
- SI-3.10 Malicious Code Analysis
- SI-3.8 Detect Unauthorized Commands
- SI-7 Software, Firmware, and Information Integrity
- SI-7.9 Verify Boot Process

TVM-08 Vulnerability Prioritization
- RA-2 Security Categorization
- RA-2.1 Impact-level Prioritization
- SA-11 Developer Security Testing and Evaluation
- SA-11.5 Penetration Testing
- TVM-09 Vulnerability Management Reporting
- RA-5 Vulnerability Scanning
- RA-5.11 Public Disclosure Program
- RA-5.8 Review Historic Audit Logs
- SA-15 Development Process, Standards, and Tools
- SA-15.1 QUALITY METRICS

TVM-10 Vulnerability Management Metrics
- PM-31 CONTINUOUS MONITORING STRATEGY
- RA-5.5.10 Correlated Scanning Information
- RA-5.6 Automated Trend Analyses
- RA-5.8 Review Historic Audit Logs
- SA-15 Development Process, Standards, and Tools
- SA-15.1 QUALITY METRICS
- SI-2 Flaw Remediation
- SI-3.2 Time to Remediate Flaws and Benchmarks for Corrective Actions
Use of NIST SP 800-53 R5 aligning to CCM v4 TVM Controls
Concerns for Threat and Vulnerability Management - TVM

CCM Focus

- There are no gaps
- The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards in the RA - RISK ASSESSMENT, SA - SYSTEM AND SERVICES ACQUISITION, SI - SYSTEM AND INFORMATION INTEGRITY, domains.
- Note that IR-1 associates to the https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf which is Malware handling for endpoints.

Consideration for what Never Mapped

The following controls were found to be too specific for alignment to the CCM 4.1 matrix:
- RA-3(2) Risk Assessment | Use of All-source Intelligence
- RA-3(4) Risk Assessment | Predictive Cyber Analytics
- RA-6 Technical Surveillance Countermeasures Survey
- RA-7 Risk Response
- RA-9 Criticality Analysis
- RA-10 Threat Hunting
- SI-4(1) System Monitoring | System-wide Intrusion Detection System
- SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-time Analysis
- SI-4(3) System Monitoring | Automated Tool and Mechanism Integration
- SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic
- SI-4(7) System Monitoring | Automated Response to Suspicious Events
- SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies
- SI-4(12) System Monitoring | Automated Organization-generated Alerts
- SI-4(13) System Monitoring | Analyze Traffic and Event Patterns
- SI-4(14) System Monitoring | Wireless Intrusion Detection
- SI-4(15) System Monitoring | Wireless to Wireline Communications
- SI-4(16) System Monitoring | Correlate Monitoring Information
- SI-4(17) System Monitoring | Integrated Situational Awareness
- SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration
- SI-4(20) System Monitoring | Privileged Users
- SI-4(22) System Monitoring | Unauthorized Network Services
- SI-4(25) System Monitoring | Optimize Network Traffic Analysis

This presentation is Copyright of EnterpriseGRC Solutions, Inc. and is provided for distribution by and at the discretion of The Cloud Security Alliance. These materials serve as a training product to support use of the CCM to NIST Working Group mapping. No part may be reproduced or shared without CSA or EnterpriseGRC Solutions Permission. (EnterpriseGRC Solutions, Inc. Is a TM belonging to Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com)
Use of NIST SP 800-53 R5 aligning to CCM v4 UEM Controls

**UEM-01 Endpoint Devices Policy and Procedures**
- AC-19 Access Control for Mobile Devices
- AC-19.4 Restrictions for Classified Information
- AC-19.5 Full Device or Container-based Encryption
- IA-2 Identification and Authentication (Organizational Users)
- IA-2.6 Access to Accounts — Separate Device
- PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION
- PM-20.1 Privacy Policies on Websites, Applications, and Digital Services
- SC-7 Boundary Protection
- SC-7.7 Split Tunneling for Remote Devices

**UEM-02 Application and Service Approval**
- CM-11 User-Installed Software
- CM-11.2 Software Installation with Privileged Status
- CM-7 Least Functionality
- CM-7.6 Confined Environments with Limited Privileges
- CM-8 System Component Inventory
- CM-8.3 Automated Unauthorized Component Detection
- SA-4 Acquisition Process
- SA-4.10 Use of Approved PIV Products
- SC-18 Mobile Code
- SC-18.2 Acquisition, Development, and Use
- SC-18.3 Prevent Downloading and Execution
- SC-18.4 Prevent Automatic Execution
- SC-18.5 Allow Execution Only in Confined Environments

**UEM-03 Compatibility**
- AC-18 Wireless Access
- AC-18.4 Restrict Configurations by Users

**UEM-04 Endpoint Inventory**
- CM-8 System Component Inventory
- CM-8.7 Centralized Repository
- CM-8.8 Automated Location Tracking
- PM-5 System Inventory
- PM-5.1 Inventory of Personally Identifiable Information

**UEM-05 Endpoint Management**
- AC-24 Access Control Decisions
- AC-24.1 Transmit Access Authorization Information
- CM-2 Baseline Configuration
- CM-2.2 Automation Support for Accuracy and Currency
- CM-8 System Component Inventory
- CM-8.3 Automated Unauthorized Component Detection
- SC-5 Denial of Service Protection
- SC-5.1 Restrict Ability to Attack Other Systems

**UEM-06 Automatic Lock Screen**
- AC-11 Device Lock
- AC-11.1 PATTERN-HIDING DISPLAYS
- AC-12 Session Termination
- AC-12.2 Termination Message
- AC-16 Security and Privacy Attributes
- AC-16.5 Attribute Displays on Objects to be Output
- AC-2 Account Management
- AC-2.5 Inactivity Logout
- SC-23 Session Authenticity
- SC-23.1 Invalidated Session Identifiers at Logout

**UEM-07 Operating Systems**
- CM-8 System Component Inventory
- CM-8.3 Automated Unauthorized Component Detection
- SC-18 Mobile Code
- SC-18.1 Identify Unacceptable Code and Take Corrective Actions
- SI-2 Flaw Remediation
- SI-2.5 Automatic Software and Firmware Updates
- SI-4 System Monitoring
- SI-4.23 Host-based Devices

**UEM-08 Storage Encryption**
- AC-19 Access Control for Mobile Devices
- AC-19.5 Full Device or Container-based Encryption
- AC-20 Use of External Systems
- AC-20.2 Portable Storage Devices — Restricted Use
- SC-28 Protection of Information at Rest
- SC-28.1 Cryptographic Protection
- SC-28.2 Offline Storage

**UEM-09 Anti-Malware Detection and Prevention**
- SC-18 Mobile Code
- SC-18.1 Identify Unacceptable Code and Take Corrective Actions
- SC-18.3 Prevent Downloading and Execution
- SC-18.4 Prevent Automatic Execution
- SC-18.5 Allow Execution Only in Confined Environments
- SI-7 Software, Firmware, and Information Integrity
- SI-7.17 Runtime Application Self-protection

**UEM-10 Software Firewall**
- AC-17 Remote Access
- AC-17.3 MANAGED ACCESS CONTROL POINTS
- SC-7 Boundary Protection
- SC-7.12 Host-based Protection
- SC-7.17 Automated Enforcement of Protocol Formats

**UEM-11 Data Loss Prevention**
- SA-8 Security and Privacy Engineering Principles
- SA-8.18 Trusted Communications Channels
- SC-7 Boundary Protection
- SC-7.10 Protect Exfiltration
- SC-7.12 Host-based Protection
- SC-7.7 Split Tunneling for Remote Devices

**UEM-12 Remote Locate**
- AC-17 Remote Access
- AC-17.2 PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION
- CM-8 System Component Inventory
- CM-8.8 Automated Location Tracking

**UEM-13 Remote Wipe**
- AC-7 Unsuccessful Logon Attempts
- AC-7.2 Purge or Wipe Mobile Device
- MP-6 Media Sanitization
- MP-6.8 Remote Purging or Wiping of Information

**UEM-14 Third-Party Endpoint Security Posture**
- SA-3 System Development Life Cycle
- SA-3.3 Technology Refresh
- SR-11 Component Authenticity
- SR-11.2 Configuration Control for Component Service and Repair
- SR-5 Acquisition Strategies, Tools, and Methods
- SR-5.2 Assessments Prior to Selection, Acceptance, Modification, or Update
- SR-6 Supplier Assessments and Reviews
- SR-6.1 Testing and Analysis
Use of NIST SP 800-53 R5 aligning to CCM v4 UEM Controls

The end.
Concerns for Universal Endpoint Management - UEM

CCM Focus

• There are no gaps
• Care should be given to the scope and conditions that make endpoint devices within the assessment risk profile. The location and manner of endpoint use determine if those devices are part of any audit.
• The implementation of NIST SP 800-53 Matrix relies upon the associated and requisite templates and standards located the following domains. (See Consideration for Never Mapped)

  SA - SYSTEM AND SERVICES ACQUISITION
  SI - SYSTEM AND INFORMATION INTEGRITY
  SA - SYSTEM AND SERVICES ACQUISITION
  AC - ACCESS CONTROL

Consideration for what Never Mapped

“Help Desk” or IT Support for end point computing is not emphasized within the scope of Federal Audits. There are no controls found to be too specific for alignment to the CCM 4.1 matrix. CCM consumers should organize answers to questions in the CAIQ, rather than attempt a NIST first approach. Answers for endpoint may be comingled in the mappings however, they will likely be too broad an may miss the RACI for the laptop, phone and workstation.

There are eleven specific NIST standards associated to mobile computing. This one standard offers the most direct recommendations for endpoint controls relative to Federal Systems. Guidelines for Managing the Security of Mobile Devices in the Enterprise (nist.gov)
What’s so hard about mapping?
How to map

• Have a workplan
• Identify what sources and domains should map – line up the full schema
• Iterate
• Finalize
• Negative Map (what should have but didn’t)
• Map the Missing
• QA
• Communicate back to content owners
For Each Control Statement gather keywords, concepts and suitable common domains

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

<table>
<thead>
<tr>
<th>Control Test ID</th>
<th>Control Test Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Communication Privacy Policy and Procedures</td>
</tr>
<tr>
<td>2</td>
<td>鉴别 Personal Information from PII</td>
</tr>
<tr>
<td>3</td>
<td>Analyze Privacy Policy and Procedures</td>
</tr>
<tr>
<td>4</td>
<td>Protect Personal Information</td>
</tr>
<tr>
<td>5</td>
<td>Monitor Personal Information</td>
</tr>
<tr>
<td>6</td>
<td>Review Privacy Policy and Procedures</td>
</tr>
<tr>
<td>7</td>
<td>Identify Personal Information</td>
</tr>
<tr>
<td>8</td>
<td>Prepare Privacy Policy and Procedures</td>
</tr>
<tr>
<td>9</td>
<td>Review Personal Information</td>
</tr>
</tbody>
</table>
Correctly Formatted Mappings Accessible/Usable
Imagine Regulating Federal E-Commerce Cloud Based Medical Service

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

©Copyright EnterpriseGRC Solutions, Inc. Robin Basham, M.Ed., M.IT, CISSP, CISA, ITSM, CGEIT, CRISC, Master ACC, CRP, VRP, HISP - robin@enterprisegrc.com
Mappers benefit by mapping technical controls to frameworks, frameworks to client domains, configurations to policy.

<table>
<thead>
<tr>
<th>Risk Drivers</th>
<th>Detail Control Description (OIC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known weakness affecting data in the process is driven by the requirement to gain access to the data while the application is online e.g. a Progressive Web App.</td>
<td>When offline access is not a requirement, follow these steps:</td>
</tr>
<tr>
<td>- Authenticate the user against the backend system</td>
<td>- Add a salt from the client/user session storage (e.g., HTTP cookies) to the current password hash.</td>
</tr>
<tr>
<td>- Send back the salt to the client (e.g., via a cookie)</td>
<td>- Log events to audit the salt distribution and the back-end system's changes.</td>
</tr>
<tr>
<td>- Role-based access control</td>
<td>- Add a salt to the password hash and store the new hash.</td>
</tr>
<tr>
<td>- Always update the password hash</td>
<td>- Update the salt in the database.</td>
</tr>
</tbody>
</table>

Security Compass is a CSA Partner. This image shows work completed by EnterpriseGRC for Security Compass and is shown here to demonstrate the mapping beneath a highly complex cybersecurity product. EnterpriseGRC supplies mapping services to companies like Security Compass who are essential to providing automation for continuous cloud compliance.

|---------------------------------|----------------------------------|-------------------------------------|---------------------------------|--------------------------------|----------------------------|-----------------------------|-----------------------------|-------------------------------|-------------------------------|-------------------------------|-----------------------------|-------------------------------|---------------------------------|-------------------------------------------------|-------------------------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|

**SECURITY ATTRIBUTE OUTPUT DRIVER**

- **Privacy Attribute Output Driver**
- **Trusted Distribution Sharing Process**
- **Business Control Security Controls**
- **Life Cycle Security Controls**
- **Architecture and Deployment**
- **Compliance Security Controls**
- **General Security Controls**
- **Development Security Controls**
- **Data Storage Security Controls**
- **Application Security Controls**
- **Network Security Controls**
- **Identity Security Controls**
- **Software Development Life Cycle (SDLC)**
- **Incident Management and Security Event Handling Controls**
- **Compliance Test and Software Compliance Testing**
- **Risk Management and Information Security Program Controls**
- **Access Management and Access Control Management**
- **Audit and Monitoring Controls**
- **Legal and Compliance Controls**
- **Business Continuity Management Controls**

**SECURITY ATTIBUTE OUTPUT DRIVER**

- **Privacy Attribute Output Driver**
- **Trusted Distribution Sharing Process**
- **Business Control Security Controls**
- **Life Cycle Security Controls**
- **Architecture and Deployment**
- **Compliance Security Controls**
- **General Security Controls**
- **Development Security Controls**
- **Data Storage Security Controls**
- **Application Security Controls**
- **Network Security Controls**
- **Identity Security Controls**
- **Software Development Life Cycle (SDLC)**
- **Incident Management and Security Event Handling Controls**
- **Compliance Test and Software Compliance Testing**
- **Risk Management and Information Security Program Controls**
- **Access Management and Access Control Management**
- **Audit and Monitoring Controls**
- **Legal and Compliance Controls**
- **Business Continuity Management Controls**
If ANY of these practices are not achieved, they NEED TO FACTOR into the RMF.
The Product of Mapping is Security & Risk Program Management

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.
Recap: Management Strategy First + Why r5 CCM 4 Now

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

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

*EnterpriseGRC Solutions wants to share work product delivered to a CSA partner and has approval to share their name during this conversation. This presentation is Copyright of EnterpriseGRC Solutions, Inc. No part may be reproduced or shared without EnterpriseGRC Solutions Permission.*