CDSA’s App & Cloud Framework

May 27th 2020

TPN aims

- Improved content security in studio supply chain
- Common control set
- Efficient operations
- Shared audit reports for studios
- Reduced costs for vendors
- Global talent pool for auditors

New challenges

- Audience and revenues moving online
- Consolidation of digital production and distribution
- Rapid shift to cloud-based workflows
- New skills and security culture required

Content security

Evolution

UK Broadcasters, Production, Vendors

US Studios

- Awareness
- Hygiene

- Checklist
- Self certified
- Oversight

- Common controls
- Professional audit
- Shared data across members

- Zero Trust

Regulated

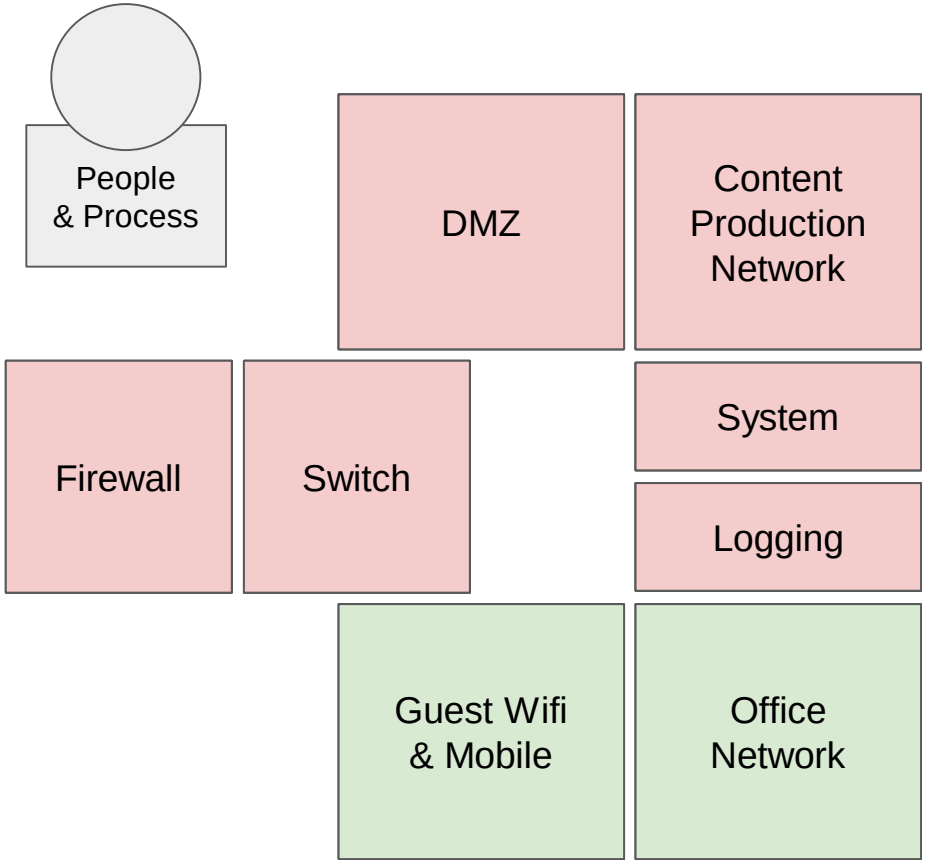
- Legislation
- Penalties

Guidance

Controlled

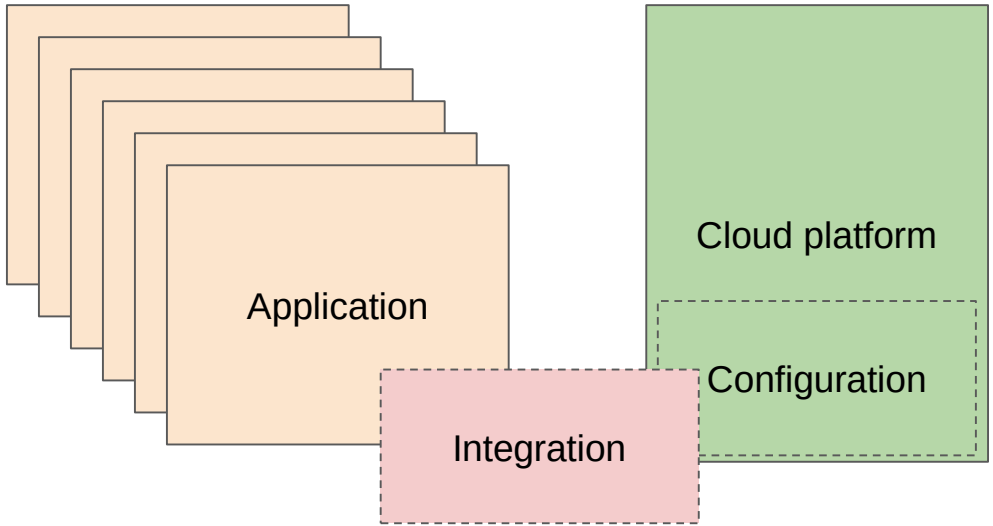
Security audit

- People & process
- Physical
  - Facility
  - Asset management
  - Transport
- Digital
  - Infrastructure
  - Content management
  - Content transfer
- Cloud
  - Software release



App & cloud.. & integration

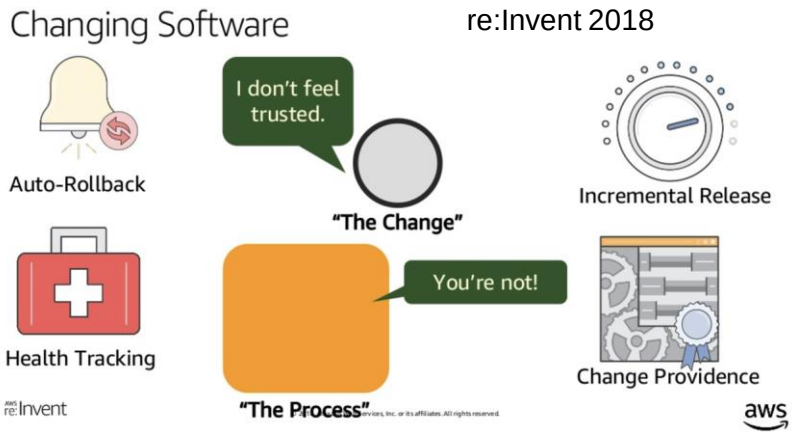
- Code
- Staff
- Partners



Complex software

- Amazon
- Netflix
- Google

Releasing Mission-Critical Software at Amazon (DEV209-R1) - AWS re:Invent 2018



https://www.slideshare.net/AmazonWebServices/releasing-missioncritical-software-at-amazon-dev209r1-aws-reinvent-2018

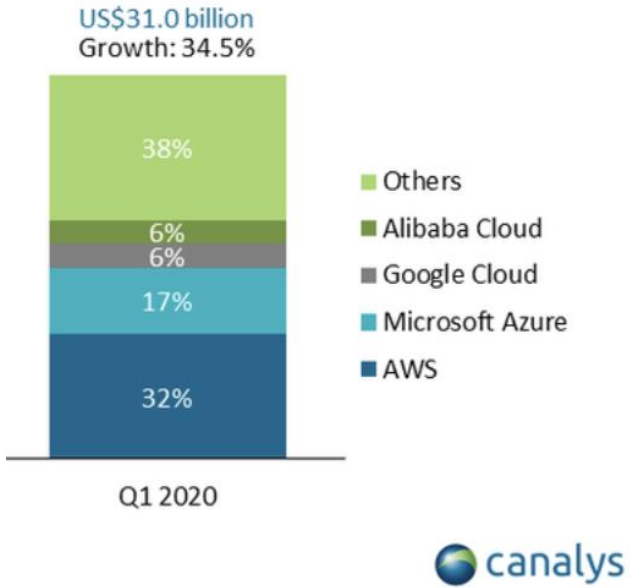
Complex software

- Amazon
- Netflix
- Google

Shift to cloud

- It’s all about software
- New economics - CAPEX to OPEX
- Move the tools and skills to the work
- Frequency of audit

CDSA App & Cloud initiative launched to extend original programme to cover new use cases with a custom control set

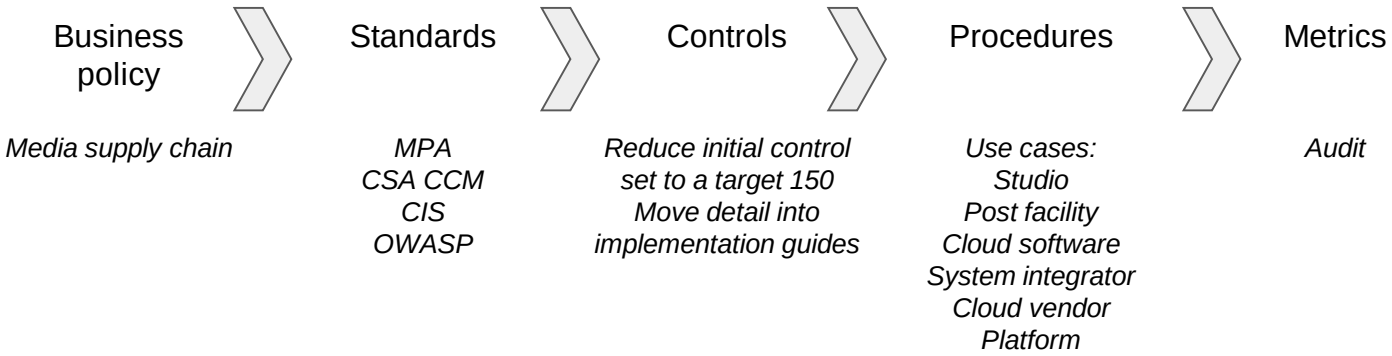


Supply chain assurance

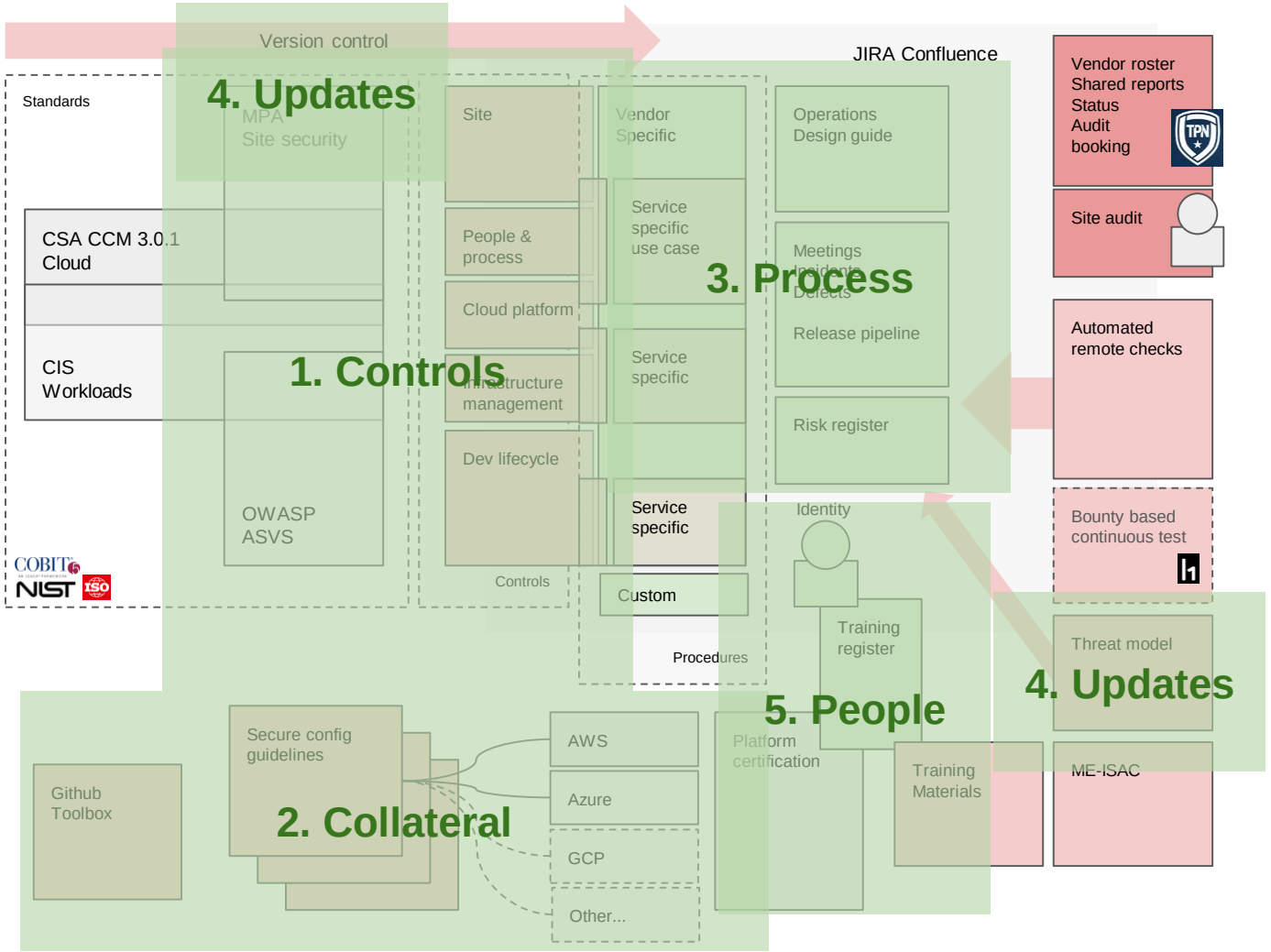
- Range of business sizes & types
- Effective security requires ongoing skills development
- Consistent approach depends on the weakest link in the chain
- Need to establish a security culture from CEO down

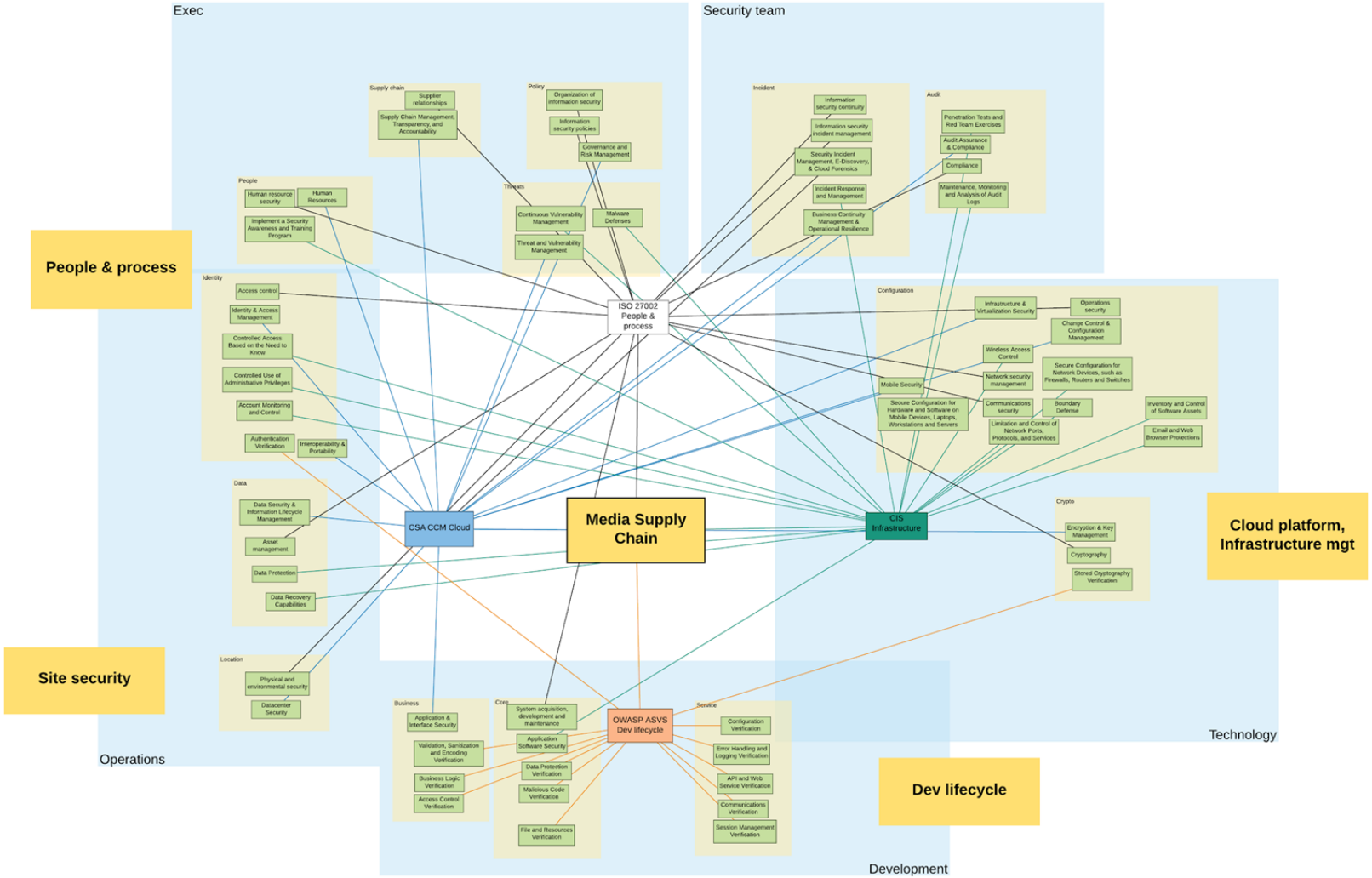
New approach

- Map controls from industry standards, with frequent updates
- Leverage cloud platforms best practice and design patterns
- Deliver documentation in a usable format that is easily applied to any size of business
- Automate tracking and checks to reduce the cost of audit
- Help develop new skills to build a security culture



1. Reduce controls maintenance effort
2. Leverage cloud platform collateral
3. Usable documentation, easy to adopt approach
4. Highlight control changes and new threats
5. Enable skills development




Exec
Security team
People & process
Supply chain
Supplier relationships
Supply Chain Management, Transparency, and Accountability
Policy
Organization of information security
Information security policies
Governance and Risk Management
Incident
Information security continuity
Information security incident management
Security Incident Management, E-Discovery, & Cloud Forensics
Incident Response and Management
Business Continuity Management & Operational Resilience
Audit
Penetration Tests and Red Team Exercises
Audit Assurance & Compliance
Compliance
Maintenance, Monitoring and Analysis of Audit Logs
People
Human resource security
Human Resources
Implement a Security Awareness and Training Program
Threats
Continuous Vulnerability Management
Malware Defenses
Threat and Vulnerability Management
Identity
Access control
Identity & Access Management
Controlled Access Based on the Need to Know
Controlled Use of Administrative Privileges
Account Monitoring and Control
Authentication Verification
Interoperability & Portability
ISO 27002
People & process
Configuration
Infrastructure & Virtualization Security
Operations security
Change Control & Configuration Management
Wireless Access Control
Network security management
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Mobile Security
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
Communications security
Boundary Defense
Limitation and Control of Network Ports, Protocols, and Services
Inventory and Control of Software Assets
Email and Web Browser Protections
Data
Data Security & Information Lifecycle Management
Asset management
Data Protection
Data Recovery Capabilities
CSA CCM Cloud
Media Supply Chain
CIS Infrastructure
Crypto
Encryption & Key Management
Cryptography
Stored Cryptography Verification
Cloud platform, Infrastructure mgt
Site security
Location
Physical and environmental security
Datacenter Security
Business
Application & Interface Security
Validation, Sanitization and Encoding Verification
Business Logic Verification
Access Control Verification
Core
System acquisition, development and maintenance
Application Software Security
Data Protection Verification
Malicious Code Verification
File and Resources Verification
OWASP ASVS
Dev lifecycle
Service
Configuration Verification
Error Handling and Logging Verification
API and Web Service Verification
Communications Verification
Session Management Verification
Technology
Operations
Dev lifecycle
Development

Control set

Index	CDSA mapping	Control Domain	Control Sub Domain	Updated Control Specification	Status	Control ID (CSA,CIS, OWASP,MPA)	Mapping Candidate	Review comments		TPN/MPA Section	TPN Control Category Name	TPN/MPA Control ID	Control Description	System Type	Al
7	People & process	Audit Assurance & Compliance	Independent Audits	Independent reviews and assessments shall be performed at least annually by a qualified assessor to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.		CCM V3.0.1 AAC-03	CCM V3.0.1 AAC-03								
8	People & process	Audit Assurance & Compliance	Information System Regulatory Mapping	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.		CCM V3.0.1 AAC-03	CCM V3.0.1 AAC-03	MSPP-5.2.1 PP-5.3 PP-5.3.3							
9	People & process	Business Continuity Management & Operational Resilience	Business Continuity Planning	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation		CCM V3.0.1 BCR-01	CCM V3.0.1 BCR-01	BCM-3.1.1	TPN App&Cloud	6.0	Data Protection	DP-6.15	Develop and implement a Service Continuity Plan for the resumption of information system functions based on documented Recovery Point Objective (RPO) and Recovery Time Objective (RTO).	Applications, Servers	
10	People & process	Business Continuity Management & Operational Resilience	Business Continuity Planning	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation		CCM V3.0.1 BCR-01	CCM V3.0.1 BCR-01	BCR-01	TPN App&Cloud	12.0	Service Continuity	SC-12.1	Document and implement a Service Continuity Plan	ALL	
11	People & process	Business Continuity Management & Operational Resilience	Business Continuity Testing	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Unmapped	CCM V3.0.1 BCR-02	CCM V3.0.1 BCR-02								
12	People & process	Business Continuity Management & Operational Resilience	Datacenter Utilities / Environmental Conditions	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Unmapped	CCM V3.0.1 BCR-03	CCM V3.0.1 BCR-03								
13	People & process	Business Continuity Management & Operational Resilience	Documentation	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Unmapped	CCM V3.0.1 BCR-04	CCM V3.0.1 BCR-04								
14	People & process	Business Continuity Management & Operational Resilience	Environmental Risks	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made		CCM V3.0.1 BCR-05	CCM V3.0.1 BCR-05	BCM-3.1.1	TPN App&Cloud	6.0	Data Protection	DP-6.20	Ensure that backup and restoration hardware, firmware, and software are protected from loss.		