CDSA CPS
App&Cloud Control Framework

May 14th 2020

Introduction

Moderator

Ben Schofield
Project Manager,
CDSA and Product
Manager, TPN

Micah Littleton
Tri-Chair ,
CDSA Technology
Committee

Todd Burke
Tri-Chair ,
CDSA Technology
Committee

Mischa Roth
Tri-Chair ,
CDSA Technology
Committee

NABSHOW EXPRESS CDSA
Cybersecurity & Content Protection VIRTUAL SUMMIT
5.12.20 | 10 a.m – 1 p.m. Pacific

TPN aims

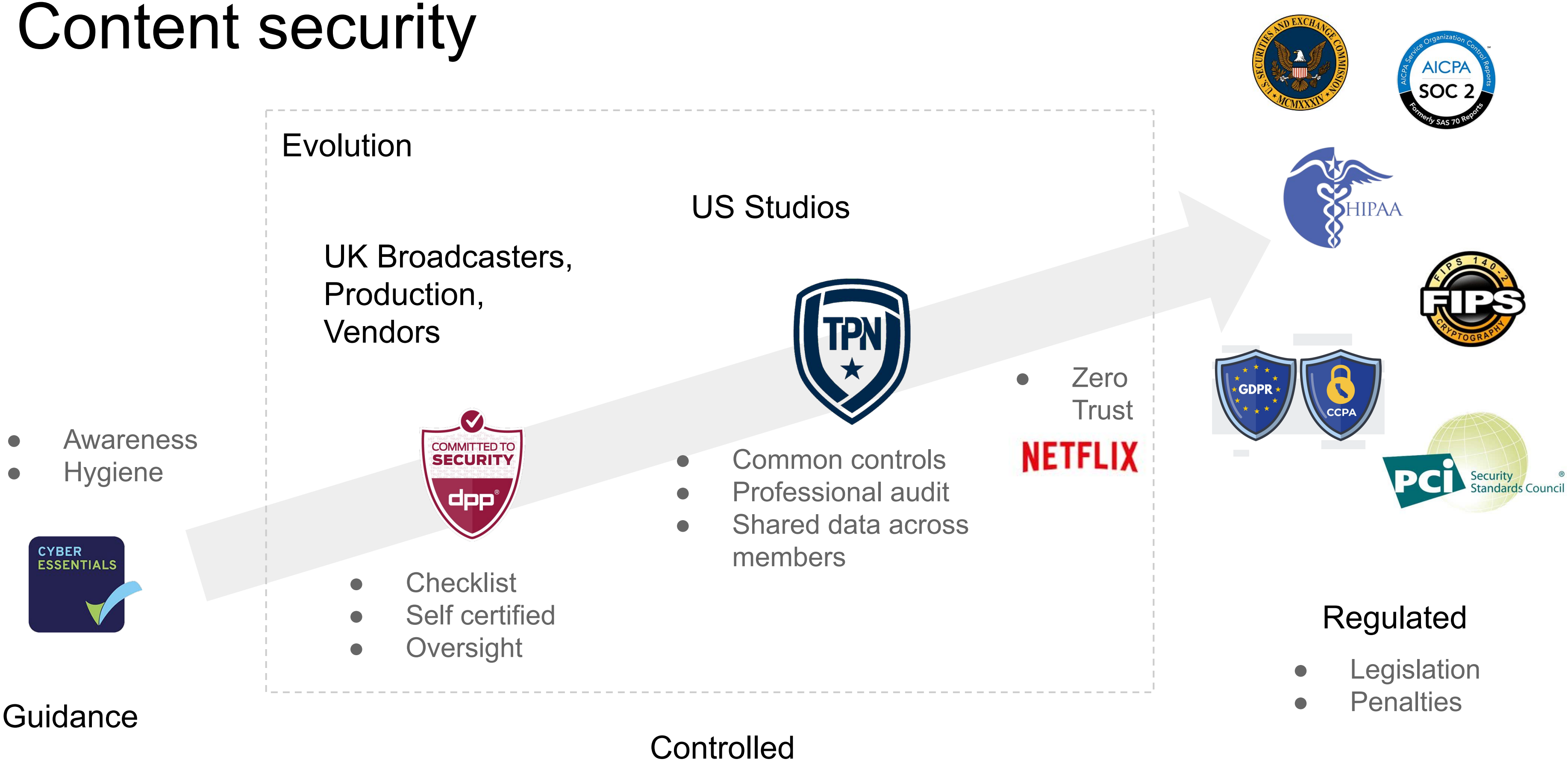
- Improved content security in studio supply chain
- Common control set
- Efficient operations
- Shared audit reports for studios
- Reduced costs for vendors
- Global talent pool for auditors

TPN
TRUSTED PARTNER NETWORK
MPA
CDSA
CONTENT DELIVERY & SECURITY ASSOCIATION
ENABLE SECURE CONTENT CREATION

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



- Awareness
- Hygiene

Guidance

Evolution

UK Broadcasters,
Production,
Vendors

- Checklist
- Self certified
- Oversight

US Studios

- Common controls
- Professional audit
- Shared data across members

- Zero Trust

Controlled

Regulated

- Legislation
- Penalties

Experience

Moderator

Ben Schofield
Project Manager, CDSA and Product Manager, TPN

Micah Littleton
Tri-Chair , CDSA Technology Committee

Todd Burke
Tri-Chair , CDSA Technology Committee

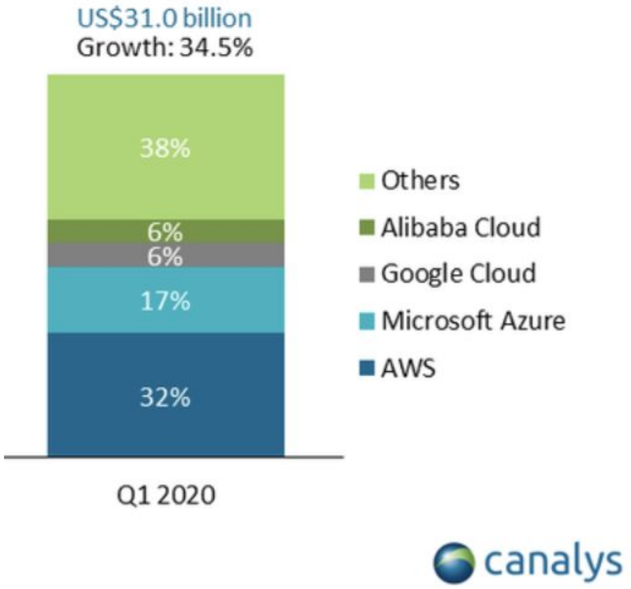
Mischa Roth
Tri-Chair , CDSA Technology Committee

NABSHOW EXPRESS CDSA
Cybersecurity & Content Protection VIRTUAL SUMMIT
5.12.20 | 10 a.m–1 p.m. Pacific

Shift to cloud

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

TPN 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

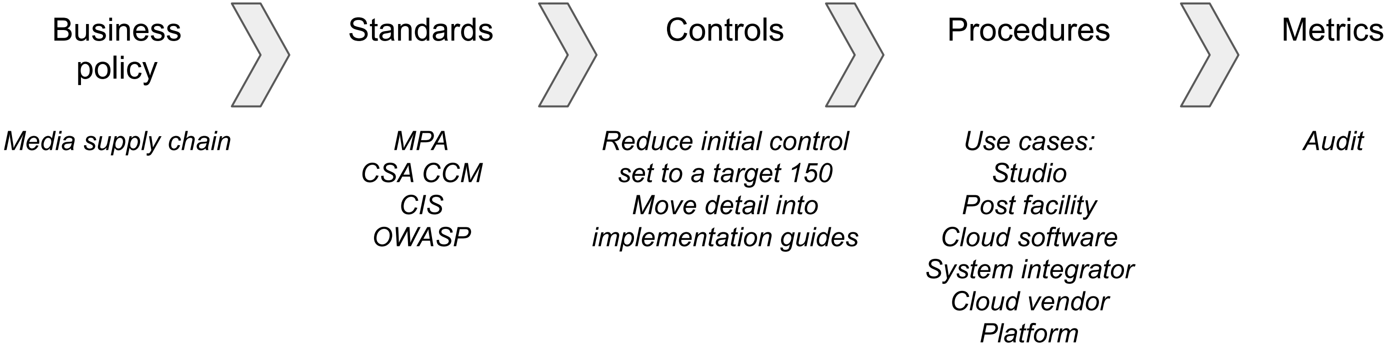
The Walt Disney Company

NBCUniversal

BBC STUDIOS

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



Business policy

Media supply chain

Standards

MPA
CSA CCM
CIS
OWASP

Controls

Reduce initial control set to a target 150
Move detail into implementation guides

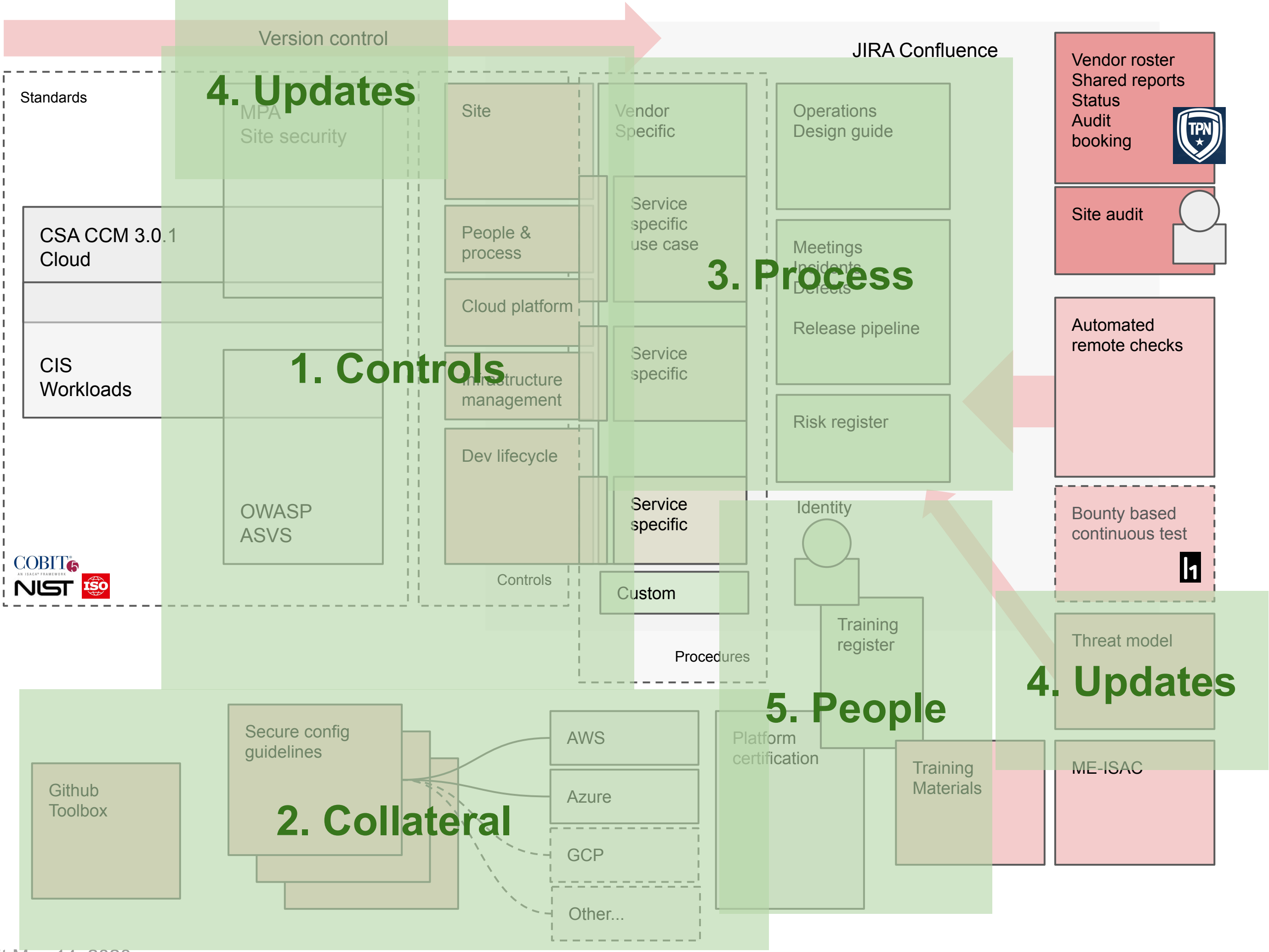
Procedures

Use cases:
Studio
Post facility
Cloud software
System integrator
Cloud vendor
Platform

Metrics

Audit

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



Version control

JIRA Confluence

4. Updates

Standards

MPA
Site security

CSA CCM 3.0.1
Cloud

CIS
Workloads

OWASP
ASVS

COBIT 5
NIST ISO

1. Controls

Site

People & process

Cloud platform

Infrastructure management

Dev lifecycle

Controls

Vendor Specific

Service specific use case

Service specific

Service specific

Custom

Procedures

3. Process

Operations
Design guide

Meetings
Incidents
Defects

Release pipeline

Risk register

Vendor roster
Shared reports
Status
Audit
booking

TPN

Site audit

Automated remote checks

Bounty based continuous test

Identity

Training register

5. People

Platform certification

Training Materials

Threat model

4. Updates

ME-ISAC

Github Toolbox

Secure config guidelines

2. Collateral

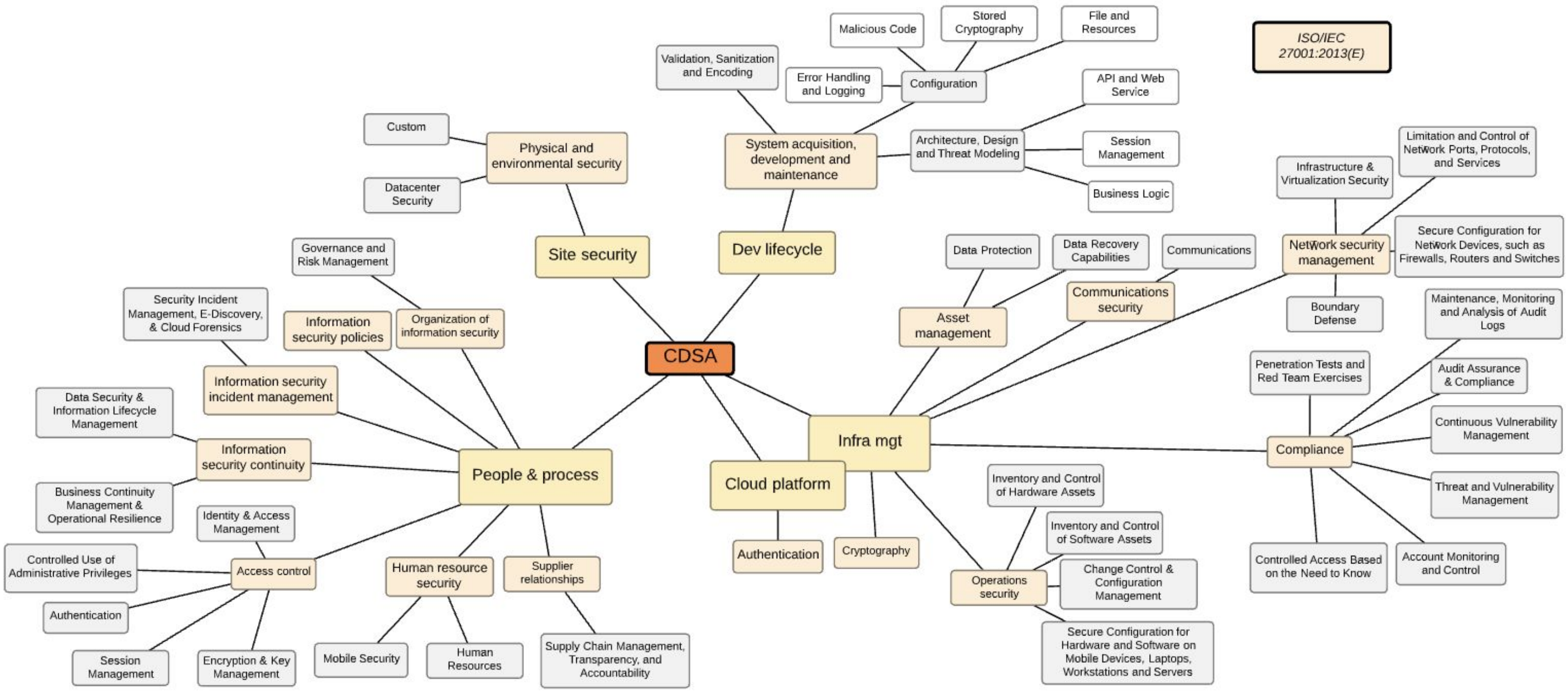
AWS

Azure

GCP

Other...

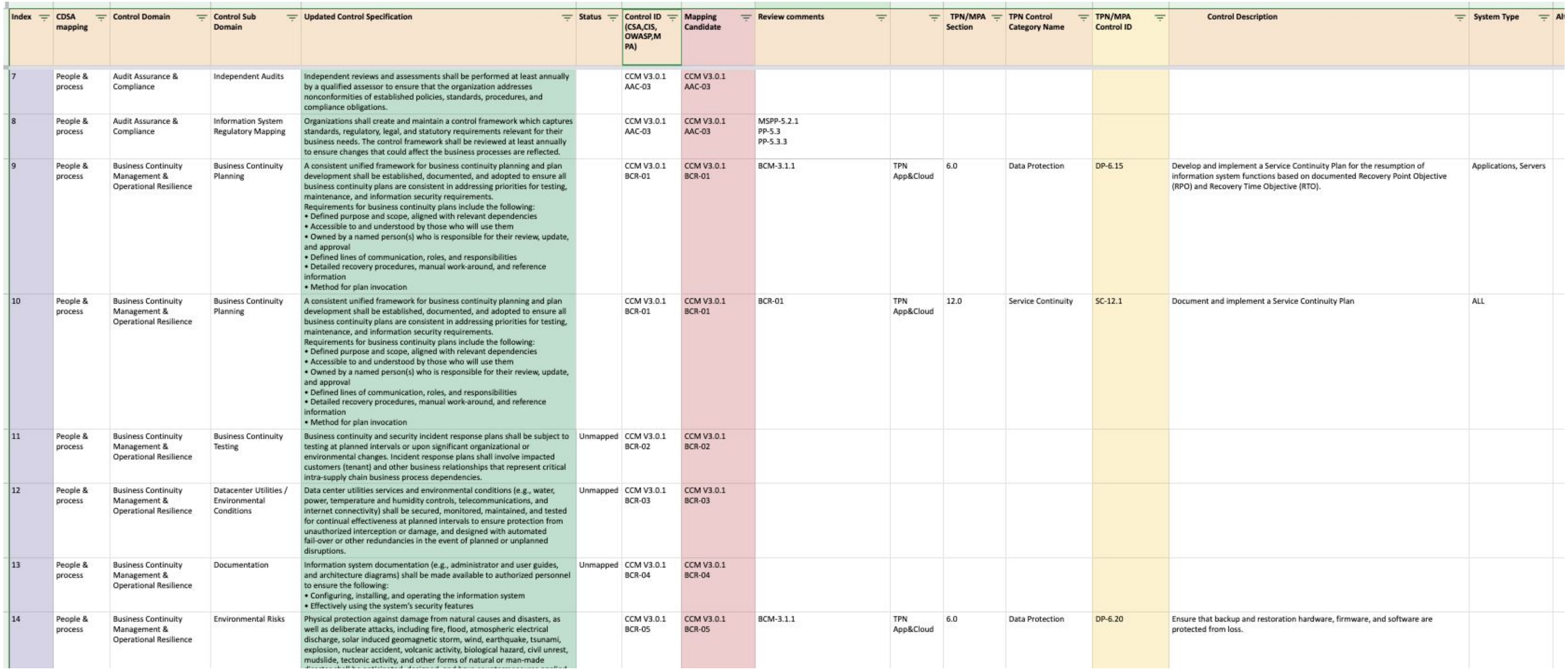
New control framework (draft)



ISO/IEC 27001:2013(E)

- CDSA
  - Site security
    - Physical and environmental security
      - Custom
      - Datacenter Security
  - Dev lifecycle
    - System acquisition, development and maintenance
      - Validation, Sanitization and Encoding
      - Configuration
        - Malicious Code
        - Stored Cryptography
        - File and Resources
        - Error Handling and Logging
      - Architecture, Design and Threat Modeling
        - API and Web Service
        - Session Management
        - Business Logic
  - Infra mgt
    - Asset management
      - Data Protection
      - Data Recovery Capabilities
    - Communications security
      - Communications
    - Network security management
      - Infrastructure & Virtualization Security
      - Limitation and Control of Network Ports, Protocols, and Services
      - Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
      - Boundary Defense
    - Compliance
      - Penetration Tests and Red Team Exercises
      - Maintenance, Monitoring and Analysis of Audit Logs
      - Audit Assurance & Compliance
      - Continuous Vulnerability Management
      - Threat and Vulnerability Management
      - Account Monitoring and Control
      - Controlled Access Based on the Need to Know
    - Cryptography
    - Operations security
      - Inventory and Control of Hardware Assets
      - Inventory and Control of Software Assets
      - Change Control & Configuration Management
      - Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
  - Cloud platform
    - Authentication
  - People & process
    - Information security policies
    - Organization of information security
      - Governance and Risk Management
    - Information security incident management
      - Security Incident Management, E-Discovery, & Cloud Forensics
    - Information security continuity
      - Data Security & Information Lifecycle Management
      - Business Continuity Management & Operational Resilience
    - Access control
      - Identity & Access Management
      - Controlled Use of Administrative Privileges
      - Authentication
      - Session Management
      - Encryption & Key Management
    - Human resource security
      - Mobile Security
      - Human Resources
    - Supplier relationships
      - Supply Chain Management, Transparency, and Accountability

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.		

Benefits

Moderator

Ben Schofield
Project Manager,
CDSA and Product
Manager, TPN

Micah Littleton
Tri-Chair ,
CDSA Technology
Committee

Todd Burke
Tri-Chair ,
CDSA Technology
Committee

Mischa Roth
Tri-Chair ,
CDSA Technology
Committee

NAB SHOW EXPRESS CDSA
Cybersecurity & Content Protection VIRTUAL SUMMIT
5.12.20 | 10 a.m–1 p.m. Pacific

Questions?

Thank you!

6.1.3 Information security risk treatment

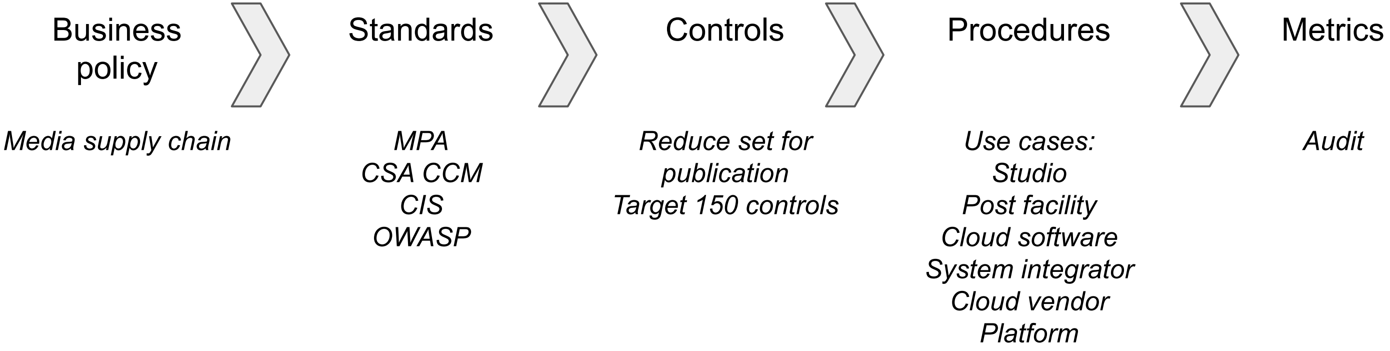
The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) **determine all controls that are necessary** to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source.

Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27001:2013(E) reviewed and confirmed in 2019

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Network security management
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security continuity
- Compliance



Business policy

Media supply chain

Standards

MPA
CSA CCM
CIS
OWASP

Controls

Reduce set for publication
Target 150 controls

Procedures

Use cases:
Studio
Post facility
Cloud software
System integrator
Cloud vendor
Platform

Metrics

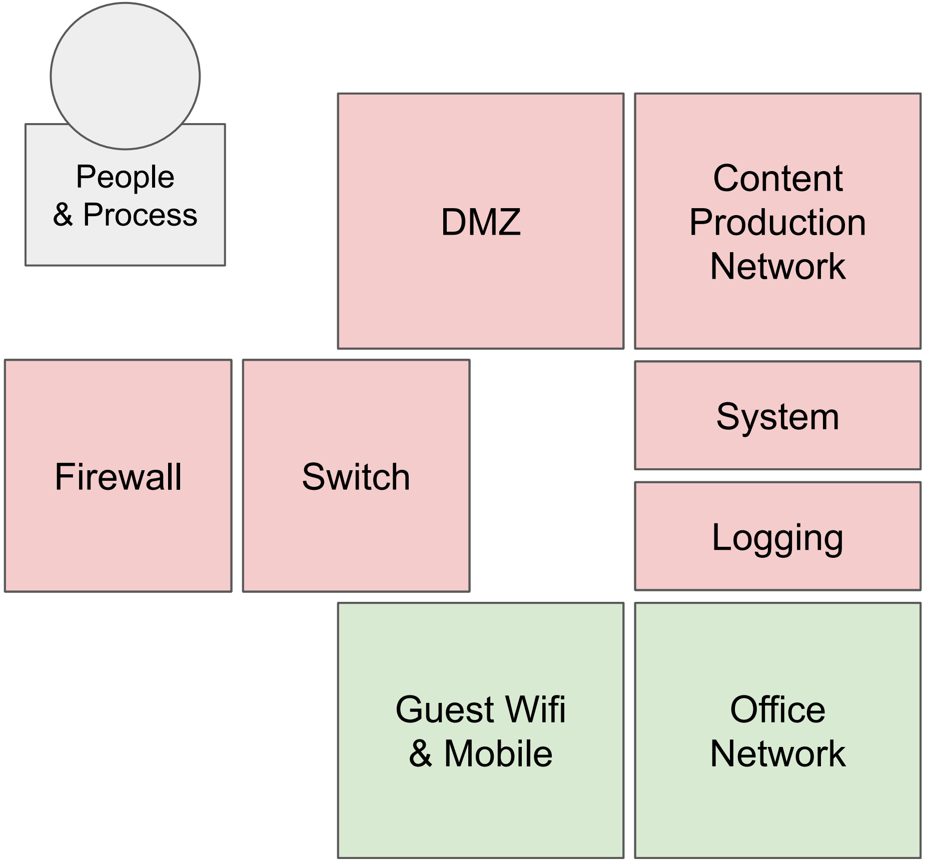
Audit

Use cases

- Studio Production and Post Production
- Cloud software vendor
- Traditional post facility
- System integrator
- Cloud platform

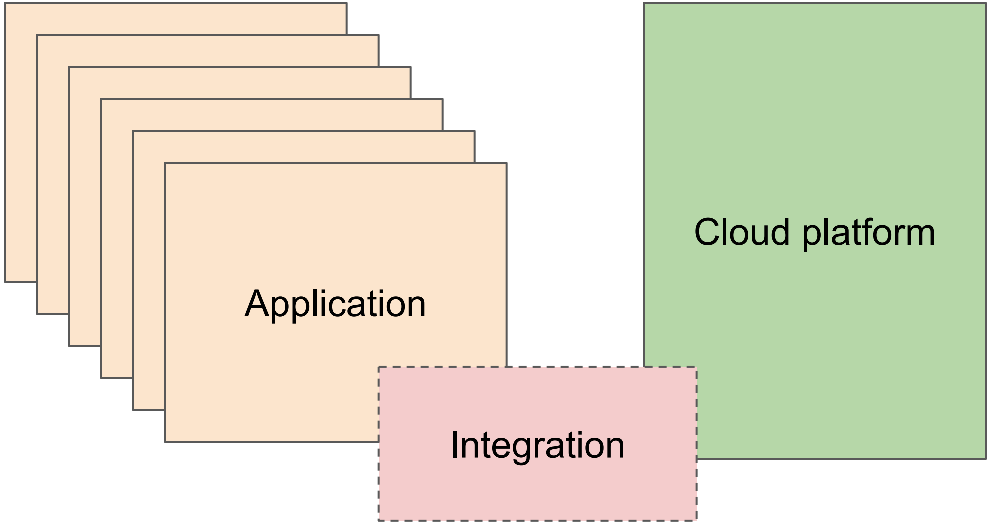
Security audit

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



App & cloud..   & integration

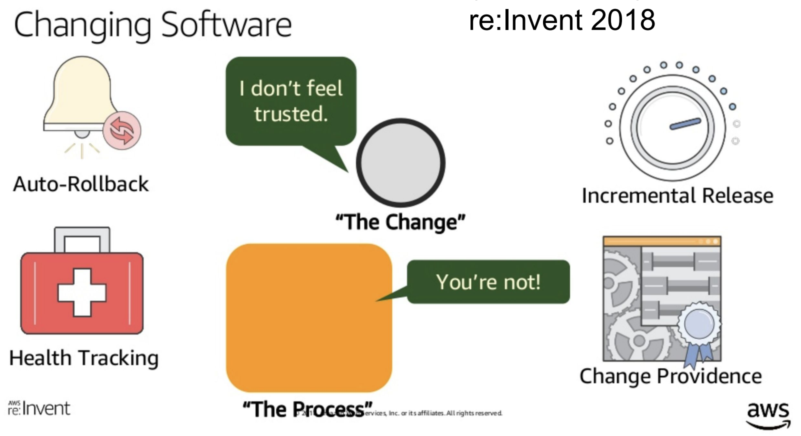
- Code
- Staff
- Partners



Complex software

- Amazon
- Netflix
- Google

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



Changing Software

Auto-Rollback

I don't feel trusted.

"The Change"

Incremental Release

Health Tracking

You're not!

"The Process"

Change Providence

re:Invent
aws

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

Complex software

- Amazon
- Netflix
- Google

NETFLIX

Control set

- Based on fundamental framework, lot of work over past two years
- Major cloud platforms have all agreed common control set, CSA CCM 3.0.1
- Map from CSA to TPN framework
- Strengthen software lifecycle controls based on OWASP SAMM
- Leverage existing cloud certification programmes
- Publish controls in usable framework aligned with common software lifecycle tools
- Seek to automate continuous audit and testing

Timing: first draft mid April