
**The Evolution of CDSA's Control Framework**

Thursday, December 16th, 2021 from 2pm to 5pm Pacific

Physically at the Luxe Hotel in LA and Online via Zoom

CDSA
Content Delivery & Security Association

# ANTITRUST STATEMENT

This is an open forum for discussions about our industry.

Please refrain from entering into any conversations that could be seen as anti-competitive or aimed at promoting anti-competitive activities.

If a conversation or activity arises we will remind you to stop the course of the discussion and move on.

CDSA
Content Delivery & Security Association

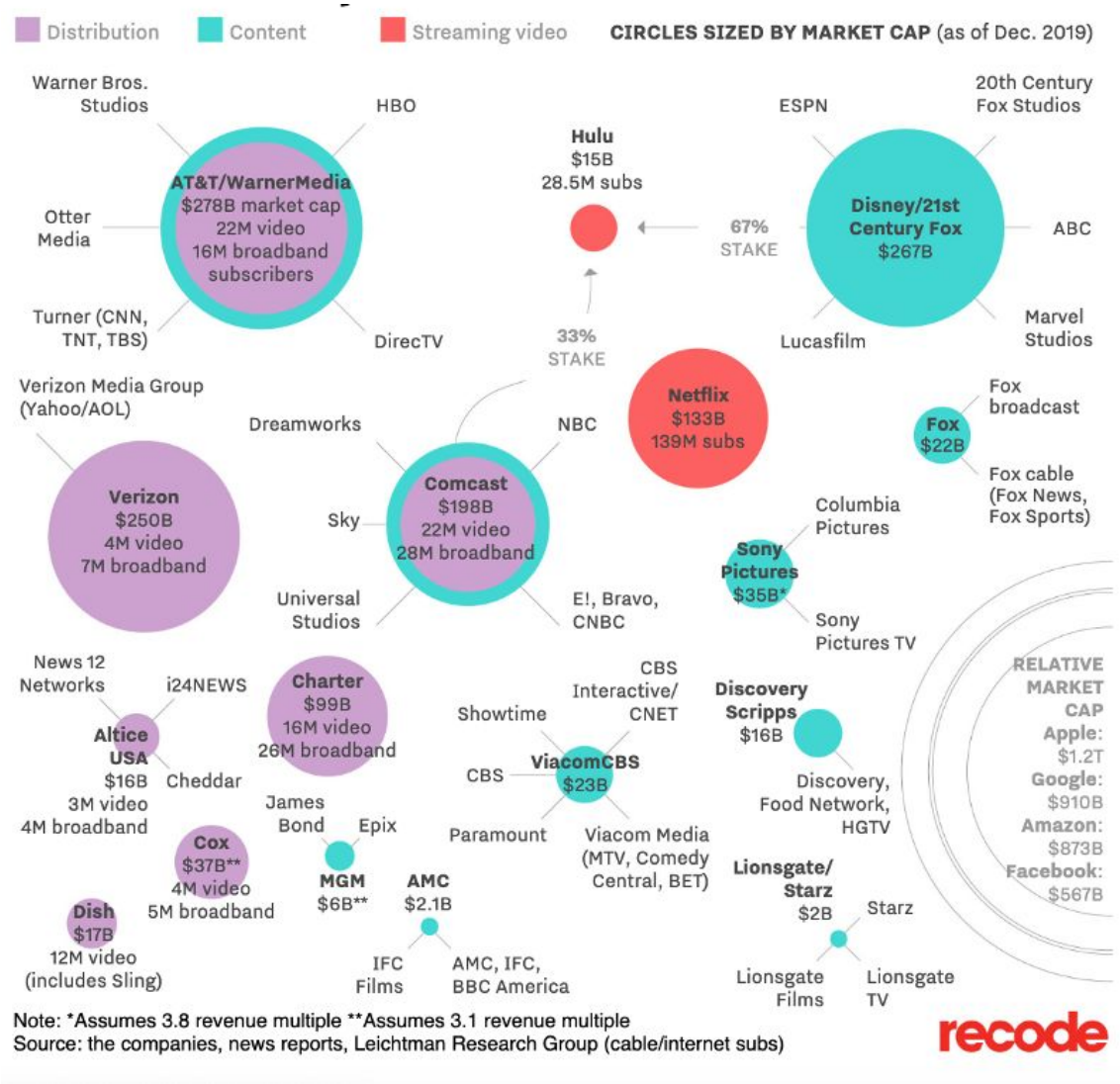
# The problem with security controls….

- So many to choose from….
- Specific to the industry
- Rooted in fundamental standards
- Critical to cover risks and response
- Alien language



# New economics of digital and cloud

- Shift in value of content flows
- Common technologies
- Consolidation of media operations
- *(minor global pandemic)*




CDSA
Content Delivery & Security Association

# Custom controls

- Easier to write
- Difficult to maintain
- Subjective perspective

| | | | | | |
|---|---|---|---|---|---|
| TPN App&Cloud | 4.0 | Cryptographic Controls | MC 21.2.1 | Encryption of data at rest is generally an acceptable method for protecting the confidentiality of data at rest that has been stolen. | Mobile Device |
| TPN App&Cloud | 4.0 | Cryptographic Controls | MC 21.2.1.1 | Encryption must be performed using sufficiently strong cryptographic primitives. Sufficiently strong means primitives that have been positively vetted by national organizations or acedemia and with an equivalent key size of 112-bits or greater. Examples of sufficiently strong cryptographic primitives: AES-128/192/256, 3DES, Two-Fish, etc. Examples of insufficiently strong cryptographic primitives: DES, RC4, any algorithm relying on keys with a bit-strength weaker than 112 bits, custom or proprietary cryptosystems | Mobile Device |
| TPN App&Cloud | 4.0 | Cryptographic Controls | MC 21.2.2 | Encryption must be performed such that a sufficiently strong cryptographic mode of operation is incorporated.<br>Examples of sufficiently strong cryptographic modes of operation: CBC, CTR, GCM.<br>Examples of insufficiently strong cryptographic modes of operation: ECB, custom or proprietary modes of operation. | Mobile Device |
| TPN App&Cloud | 4.0 | Cryptographic Controls | MC 21.2.3 | Encryption algorithms that use initialization vectors (IVs) must use them in a manner such that the cryptosystem is not weakened or susceptible to other attacks. Examples of appropriate IV use: Single use, unpredictable, randomly generated. Disclosure of IVs is generally OK – IVs are not meant to be kept confidential once in use. Examples of inappropriate IV use: Predictable IVs, reused IVs, IVs that provide insufficient entropy. | Mobile Device |
| TPN App&Cloud | 4.0 | Cryptographic Controls | MC 21.2.4 | Encryption keys must be sufficiently strong. | Mobile Device |

CDSA
Content Delivery & Security Association

# Phase one

- Initial mapping
- Committee  workstreams, insight from practitioners
- TPN re-alignment
- Focus on new technology, inclusive of site security
- Launch of CDSA Start instance

amazonstudios

CDSA
Content Delivery & Security Association

# Core sources

- Cloud infrastructure
- IT systems and data
- Web software

- Collaboration
- Alignment
- New initiatives

cloud security alliance®

CIS Center for Internet Security®

Creating Confidence in the Connected World.™

OWASP®

ISO

NIST National Institute of Standards and Technology

CDSA Content Delivery & Security Association

## Scope Applicability (Mappings)

An important CCM aspect is that it **maps to other security standards, regulations, and frameworks**. When the CCM was created, there were already many different information security standards, best practices, and regulations in existence (e.g., ISO/IEC 27001 and 27002, PCI DSS, NERC CIP, BITS , BSI). Many companies already had their internal structures and frameworks set up and aligned with those standards.

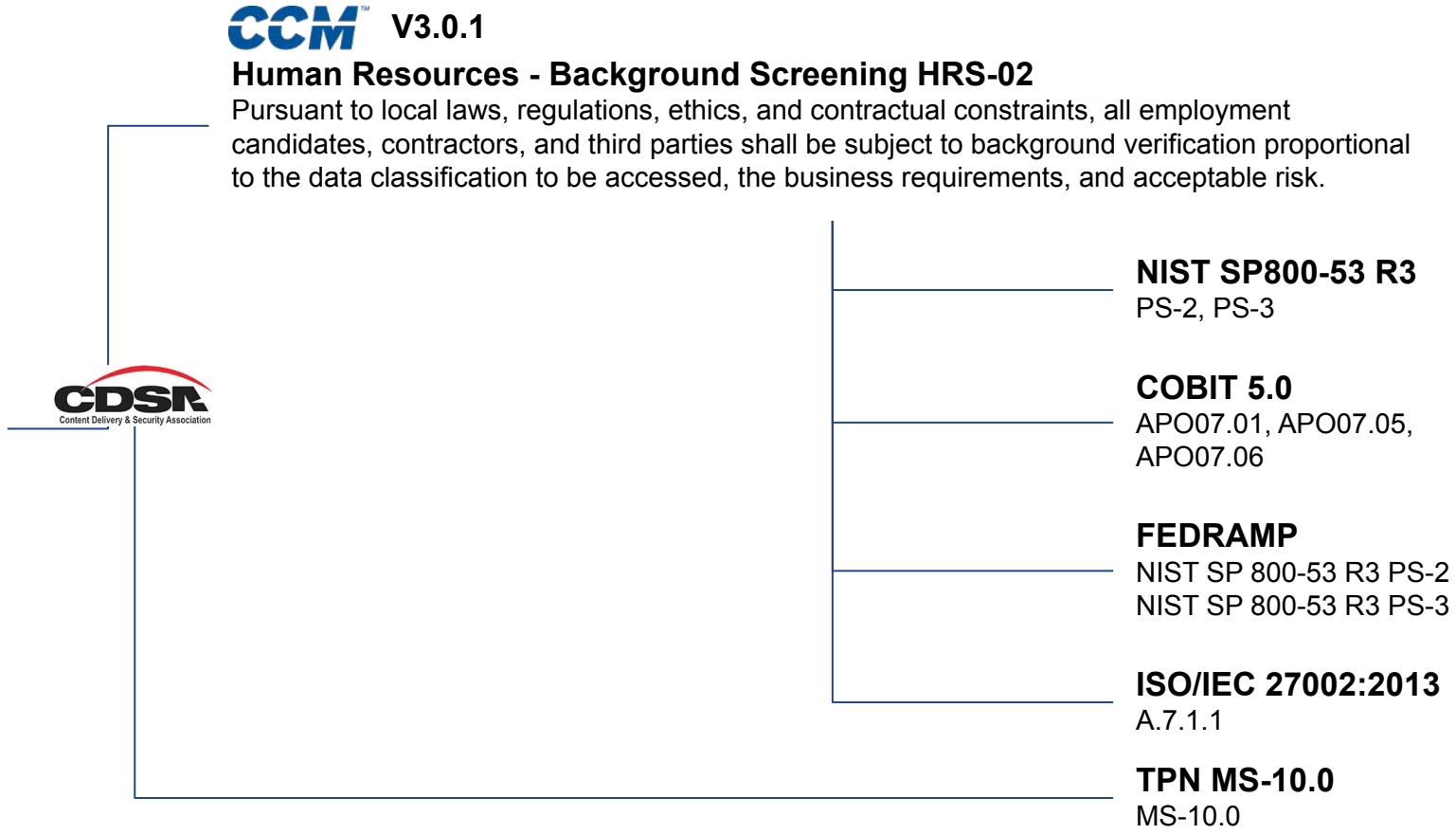
The CSA wanted to provide cloud sector-specific controls while ensuring that organizations had clear paths to **connect their existing control frameworks and programs** with the cloud-relevant controls included in the CCM.

# Mapping Example

**1.1.1 Background Checks**

Prior to the first day of employment, background checks and/or reference checks must be conducted for all employees and/or third-party personnel who have access to content where permitted and applicable by local law. Guidelines for background checks include, but are not limited to:

- Methods used should be proportional to the sensitivity of content and risks of content theft or leakage
- Identity, academic, and professional qualification checks should be conducted where permitted and applicable
- When background checks are not allowed by local law, it should be documented, and check all references



# Next steps

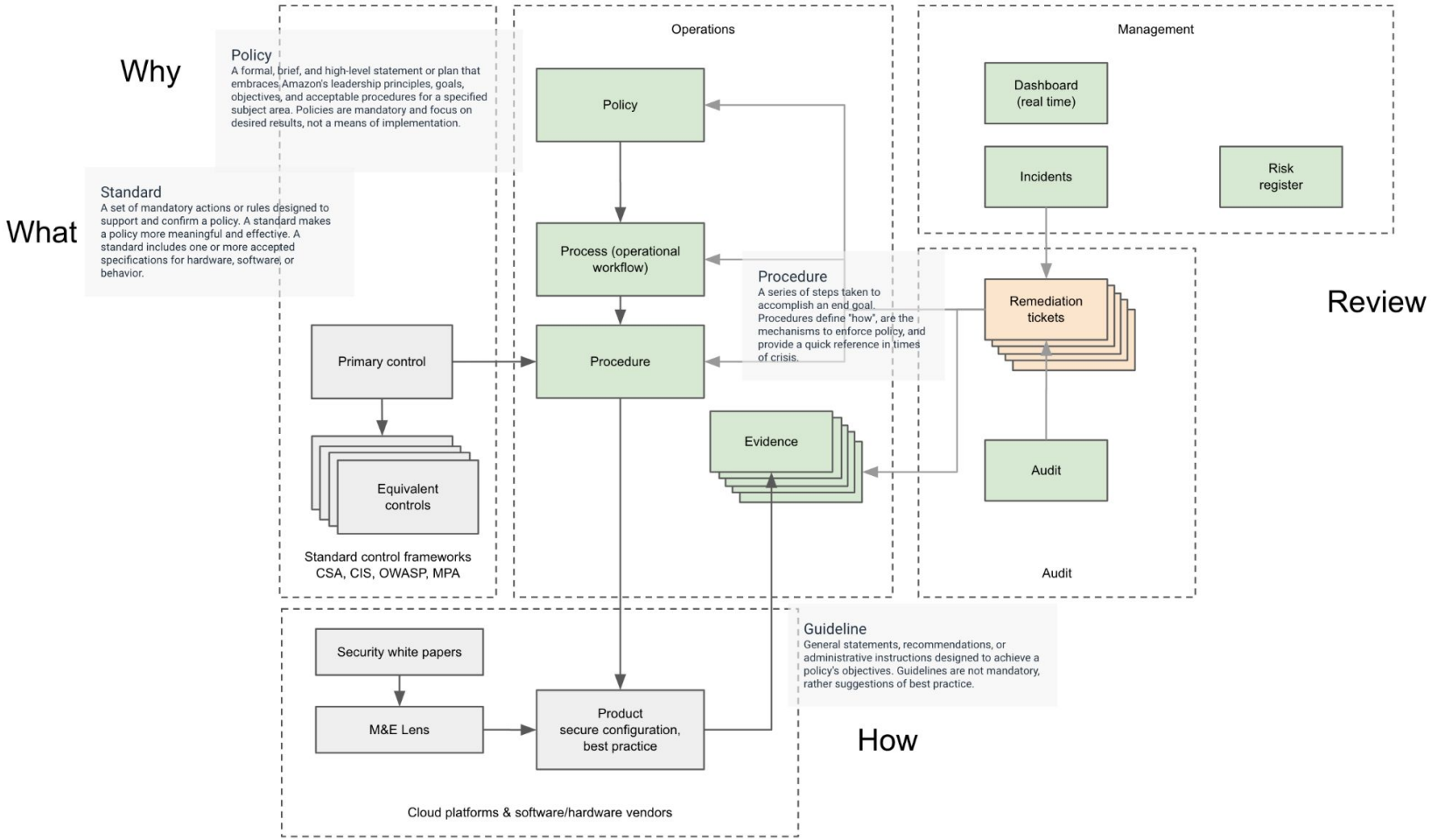
- START Q1 launch
- Cloud & application
- Drive adoption
- Mapping dataset
- Tech stack
- Incident and risk
- Real time
- Security culture

# Cloud & application

- Basic core
- Cloud best practice/tech stack
- Align with Amazon Studios vendors
- Practical audit experience
- Review with committee

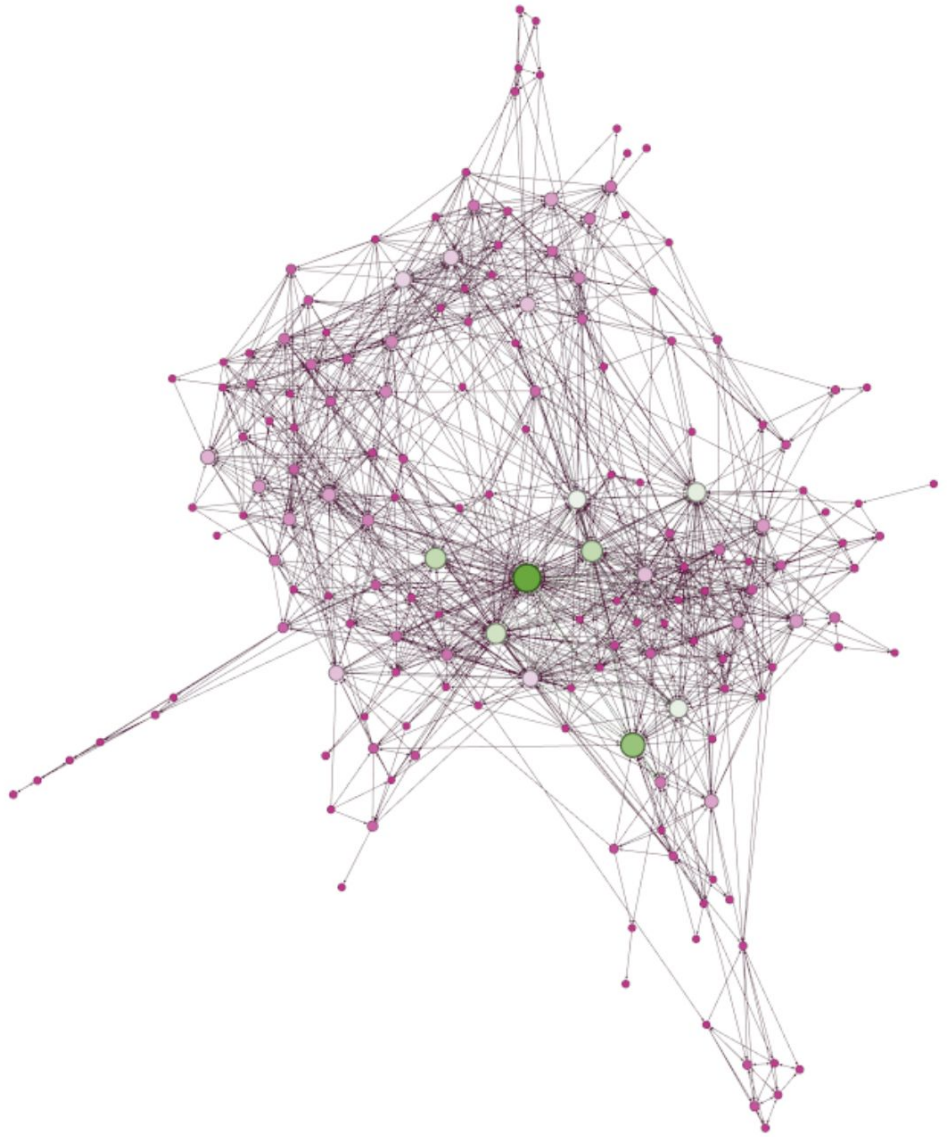
# Drive adoption

- Goals
- Policy
- Standards
- Process
- Best practice
- Evidence



# Graph database

- Compare mappings
- Remove subjectivity
- Identify anomalies
- Workstream expert review to get to consensus



# Tech stack

- Software Bill of Materials
- Best practice evidence
- Cumulative compliance

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| **01** | **Inventory and Control of Enterprise Assets** | | | |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ● | ● | ● |
| 1.2 | Address Unauthorized Assets | ● | ● | ● |
| 1.3 | Utilize an Active Discovery Tool | | ● | ● |
| 1.4 | Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory | | ● | ● |
| 1.5 | Use a Passive Asset Discovery Tool | | | ● |
| **02** | **Inventory and Control of Software Assets** | | | |
| 2.1 | Establish and Maintain a Software Inventory | ● | ● | ● |
| 2.2 | Ensure Authorized Software is Currently Supported | ● | ● | ● |
| 2.3 | Address Unauthorized Software | ● | ● | ● |
| 2.4 | Utilize Automated Software Inventory Tools | | ● | ● |
| 2.5 | Allowlist Authorized Software | | ● | ● |
| 2.6 | Allowlist Authorized Libraries | | ● | ● |
| 2.7 | Allowlist Authorized Scripts | | | ● |

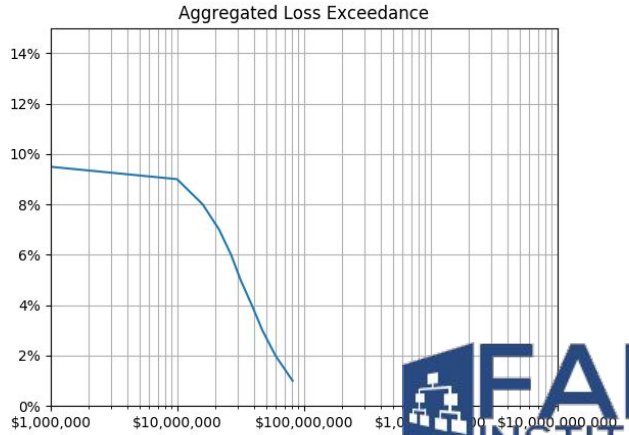
CDSA
Content Delivery & Security Association

CIS Controls®
Version 8

# Incident and risk

- Impact x frequency>mitigation ($)
- Engage business P&L owners
- Shared frequency

THE NETFLIX TECH BLOG




FAIR INSTITUTE

MEISAC
MEDIA + ENTERTAINMENT
INFORMATION SHARING ANALYSIS CENTER

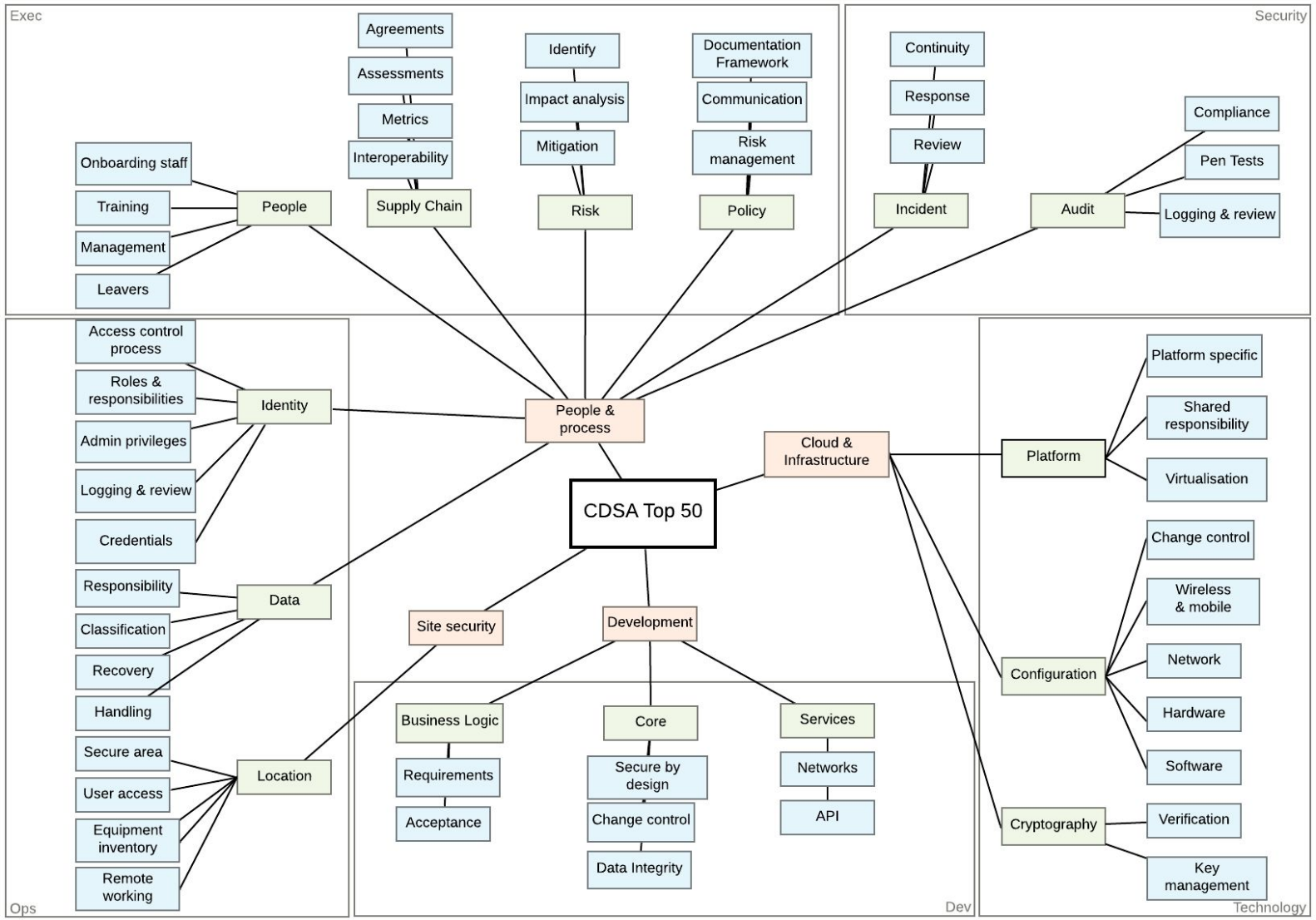
CDSA
Content Delivery & Security Association

# Real time

- Shift from static annual narrative
- Visible posture, evidence based
- Continuous deployment
- Elastic cloud resources
- Identity and permissions
- Secure by design, secure by scenario

# Security culture

- Everyone takes responsibility
- Commercial imperatives




CDSA
Content Delivery & Security Association

# CDSA security controls

- Specific selection of controls for media production and distribution, based on existing frameworks and vetted by panel of industry experts
- Maintaining continuity with existing annual audits for site security
- Evolution towards real-time security across the supply chain encompassing cloud infrastructure and new digital workflows
- Support vendors with consistent best practices for the common tech stack to reduce cost of implementation and improve security culture
- Intention to improve sharing of quantitative risk information through ISAC and incident analysis (Netflix is likely leading industry with approach), need to democratize it across the industry out to the supply chain elements