Content Delivery & Security Association

APP & CLOUD CONTROL FRAMEWORK

PROJECT LEAD:
BEN SCHOFIELD, TECHNICAL DIRECTOR, CDSA

CDSA TECHNOLOGY COMMITTEE TRI-CHAIRS:
MISCHA ROTH, AMAZON STUDIOS
TODD BURKE, ADOBE
MICAH LITTLETON, TECHNICOLOR

KEY PERSPECTIVES

VOICES FROM THE TECHNOLOGY COMMITTEE CHAIRS

- CONTENT OWNER — amazonstudios
- SOFTWARE PLATFORM — Adobe
- MULTI-PLATFORM SERVICES — technicolor
- CLOUD PLATFORM — Microsoft Azure

MICAH LITTLETON

VICE PRESIDENT, GLOBAL CONTENT SECURITY, TECHNICOLOR

- CONTENT OWNER
- SOFTWARE PLATFORM
- MULTI-PLATFORM SERVICES
- CLOUD PLATFORM

technicolor

TODD BURKE

PRINCIPAL SOLUTIONS ENGINEER, ADOBE

- CONTENT OWNER
- SOFTWARE PLATFORM
- MULTI-PLATFORM SERVICES
- CLOUD PLATFORM

Adobe

JOEL SLOSS

SENIOR PROGRAM MANAGER, MICROSOFT AZURE, AND BOARD MEMBER, CDSA

- CONTENT OWNER
- SOFTWARE PLATFORM
- MULTI-PLATFORM SERVICES
- CLOUD PLATFORM

Microsoft Azure

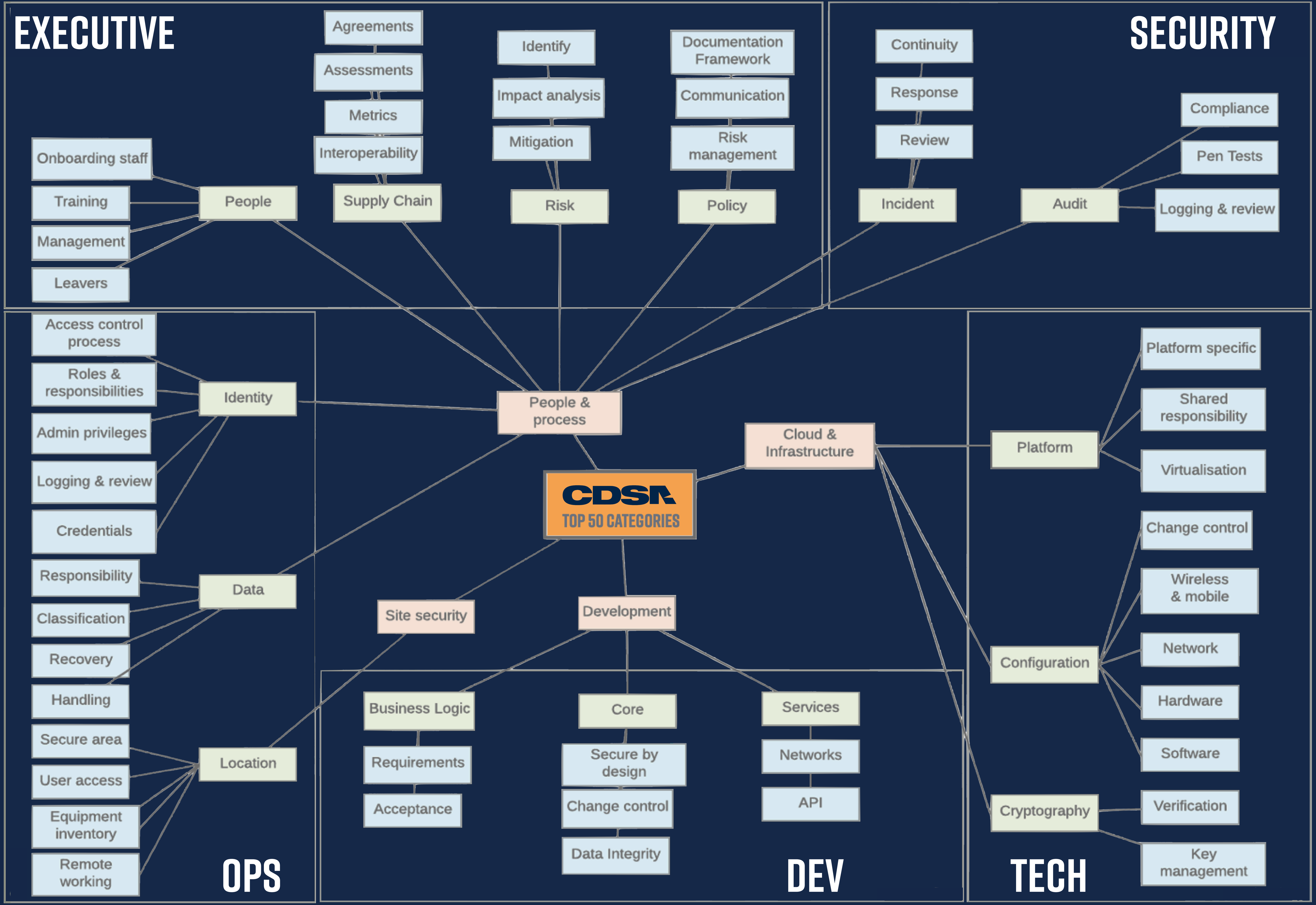
BEN SCHOFIELD

PROJECT MANAGER, CDSA

• CONTENT OWNER	amazonstudios
• SOFTWARE PLATFORM	Adobe
• MULTI-PLATFORM SERVICES	technicolor
• CLOUD PLATFORM	Microsoft Azure

TOP 50 CATEGORIES

- FOCUSED ON SMALL SET OF PRIMARY CONTROLS IN EACH AREA
- ALIGNED TO KEY ROLES ACROSS THE ORGANIZATION AT ANY SCALE
- HIGH LEVEL SUMMARY NARRATIVE DOCUMENT
- OVERVIEW STRUCTURE FOR TARGET 900 CONTROLS
- SPREADSHEET WITH DETAILED CONTROLS AND LINKS



CDSA TOP 50 CATEGORIES

- People & process
- Cloud & Infrastructure
- Site security
- Development

EXECUTIVE

- People
  - Onboarding staff
  - Training
  - Management
  - Leavers
- Supply Chain
  - Agreements
  - Assessments
  - Metrics
  - Interoperability
- Risk
  - Identify
  - Impact analysis
  - Mitigation
- Policy
  - Documentation Framework
  - Communication
  - Risk management

SECURITY

- Incident
  - Continuity
  - Response
  - Review
- Audit
  - Compliance
  - Pen Tests
  - Logging & review

OPS

- Identity
  - Access control process
  - Roles & responsibilities
  - Admin privileges
  - Logging & review
  - Credentials
- Data
  - Responsibility
  - Classification
  - Recovery
  - Handling
- Location
  - Secure area
  - User access
  - Equipment inventory
  - Remote working

DEV

- Business Logic
  - Requirements
  - Acceptance
- Core
  - Secure by design
  - Change control
  - Data Integrity
- Services
  - Networks
  - API

TECH

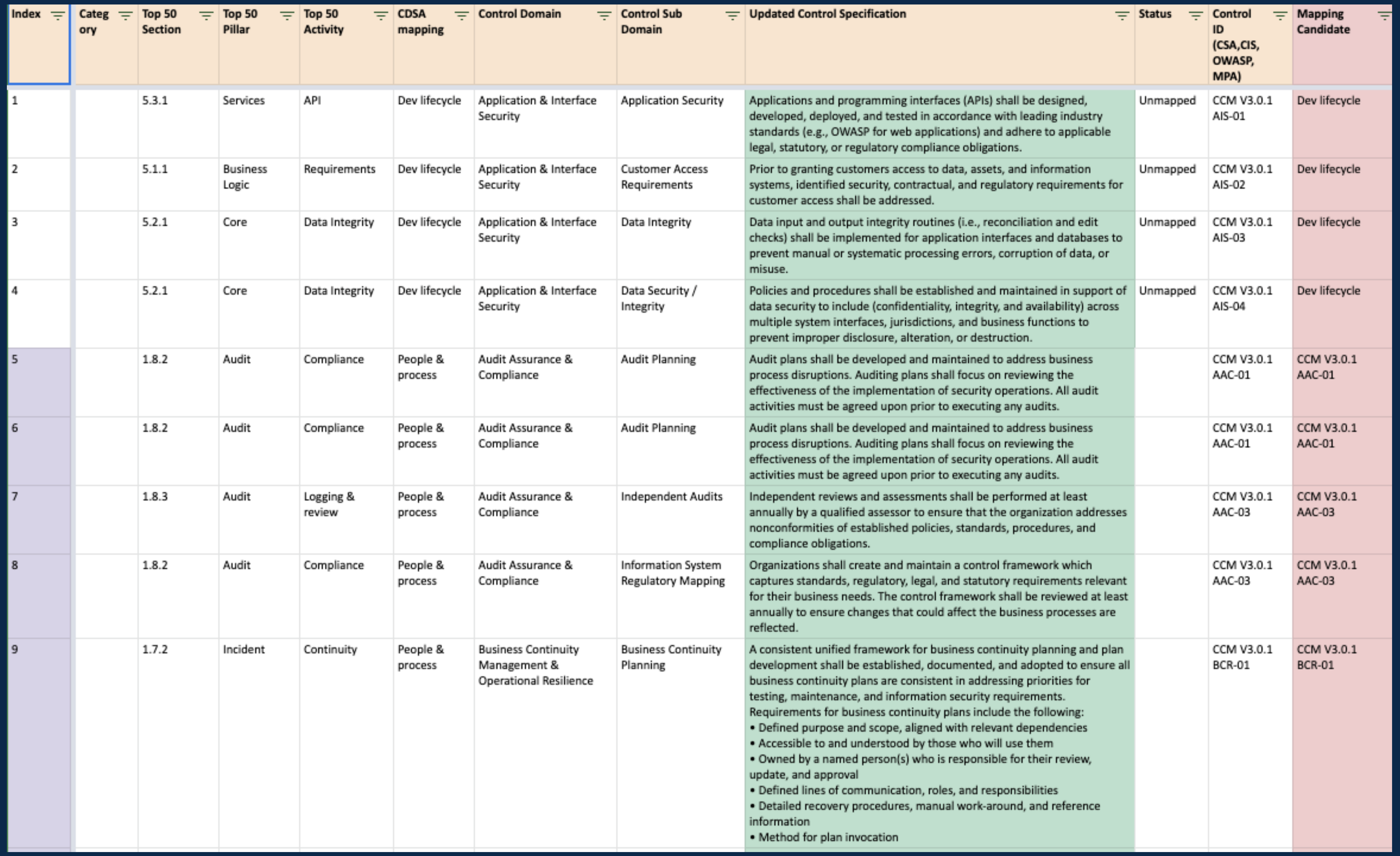
- Platform
  - Platform specific
  - Shared responsibility
  - Virtualisation
- Configuration
  - Change control
  - Wireless & mobile
  - Network
  - Hardware
  - Software
- Cryptography
  - Verification
  - Key management

Content Delivery & Security Association

CONTROL SET REVIEW

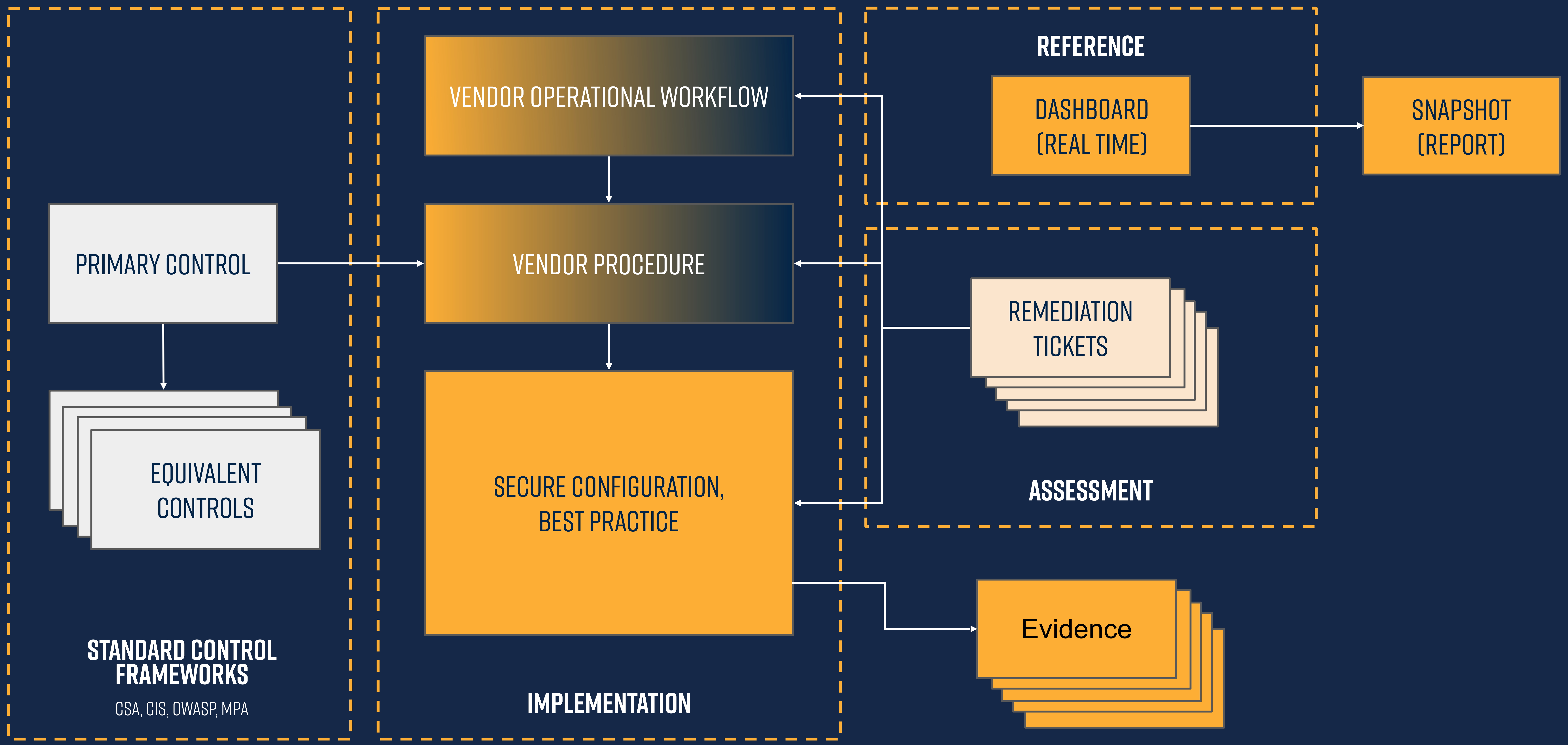
CDSA TECHNOLOGY COMMITTEE: A VOLUNTEER ARMY

- STRONG FOUNDATIONS
- HUGE TEAM EFFORT (THANKS!)
- FRAMEWORK ALIGNMENT
- OPEN SOURCE, PEER REVIEW
- MAPPING, GRAPH TRAVERSAL
- CREDENTIALS, SITE SECURITY

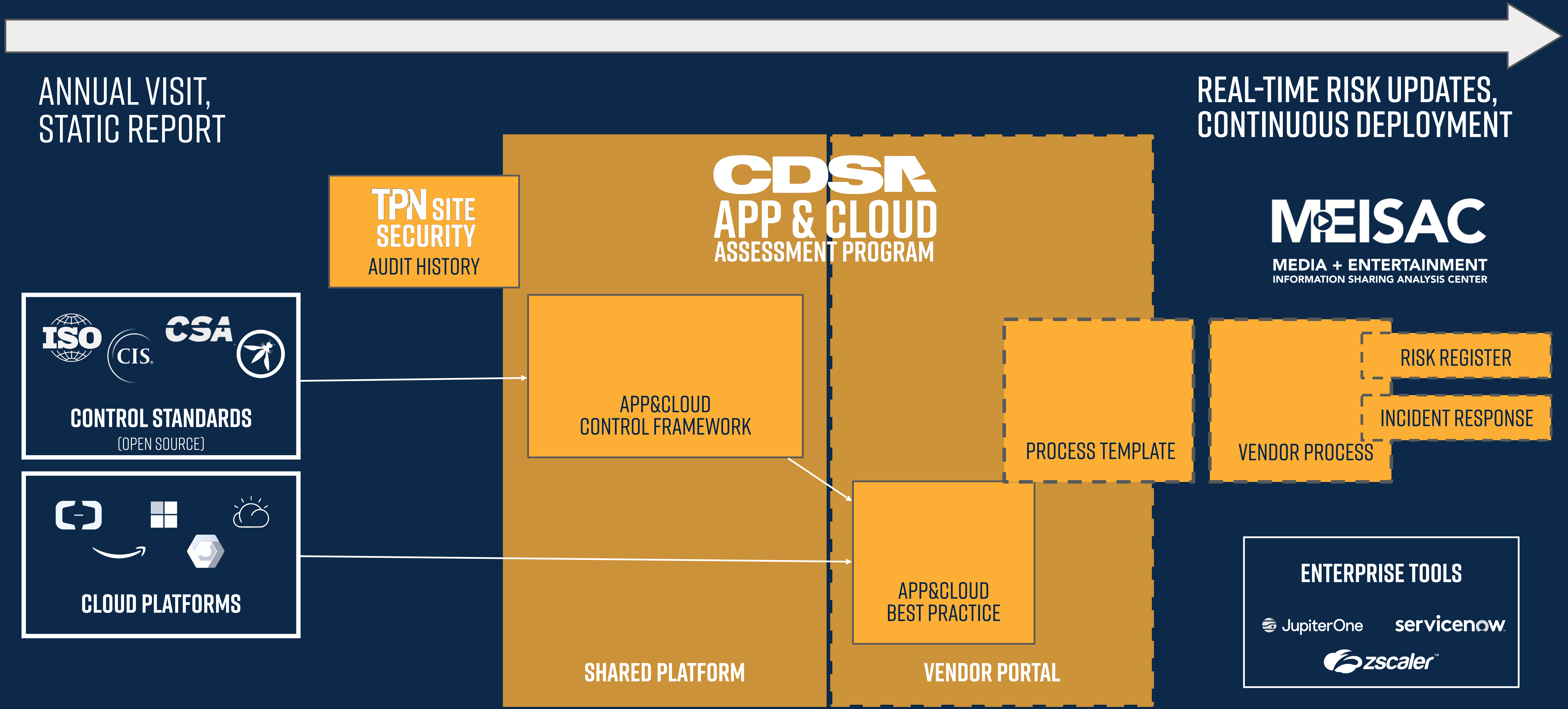


Index	Category	Top 50 Section	Top 50 Pillar	Top 50 Activity	CDSA mapping	Control Domain	Control Sub Domain	Updated Control Specification	Status	Control ID (CSA,CIS, OWASP, MPA)	Mapping Candidate
1		5.3.1	Services	API	Dev lifecycle	Application & Interface Security	Application Security	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Unmapped	CCM V3.0.1 AIS-01	Dev lifecycle
2		5.1.1	Business Logic	Requirements	Dev lifecycle	Application & Interface Security	Customer Access Requirements	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Unmapped	CCM V3.0.1 AIS-02	Dev lifecycle
3		5.2.1	Core	Data Integrity	Dev lifecycle	Application & Interface Security	Data Integrity	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Unmapped	CCM V3.0.1 AIS-03	Dev lifecycle
4		5.2.1	Core	Data Integrity	Dev lifecycle	Application & Interface Security	Data Security / Integrity	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Unmapped	CCM V3.0.1 AIS-04	Dev lifecycle
5		1.8.2	Audit	Compliance	People & process	Audit Assurance & Compliance	Audit Planning	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.		CCM V3.0.1 AAC-01	CCM V3.0.1 AAC-01
6		1.8.2	Audit	Compliance	People & process	Audit Assurance & Compliance	Audit Planning	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.		CCM V3.0.1 AAC-01	CCM V3.0.1 AAC-01
7		1.8.3	Audit	Logging & review	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		1.8.2	Audit	Compliance	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
9		1.7.2	Incident	Continuity	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

CONTROL HEIRARCHY



EVOLUTION



ANNUAL VISIT,
STATIC REPORT

REAL-TIME RISK UPDATES,
CONTINUOUS DEPLOYMENT

TPN SITE SECURITY
AUDIT HISTORY

CDSA
APP & CLOUD
ASSESSMENT PROGRAM

MEISAC
MEDIA + ENTERTAINMENT
INFORMATION SHARING ANALYSIS CENTER

CONTROL STANDARDS
(OPEN SOURCE)

CLOUD PLATFORMS

APP&CLOUD
CONTROL FRAMEWORK

APP&CLOUD
BEST PRACTICE

PROCESS TEMPLATE

VENDOR PROCESS

RISK REGISTER

INCIDENT RESPONSE

SHARED PLATFORM

VENDOR PORTAL

ENTERPRISE TOOLS

QUESTIONS, IDEAS OR COMMENTS?

Contact: bschofield@CDSAonline.org