CDSA

Content Delivery & Security Association

APP & CLOUD SECURITY CONTROLS FRAMEWORK

COMMUNITY

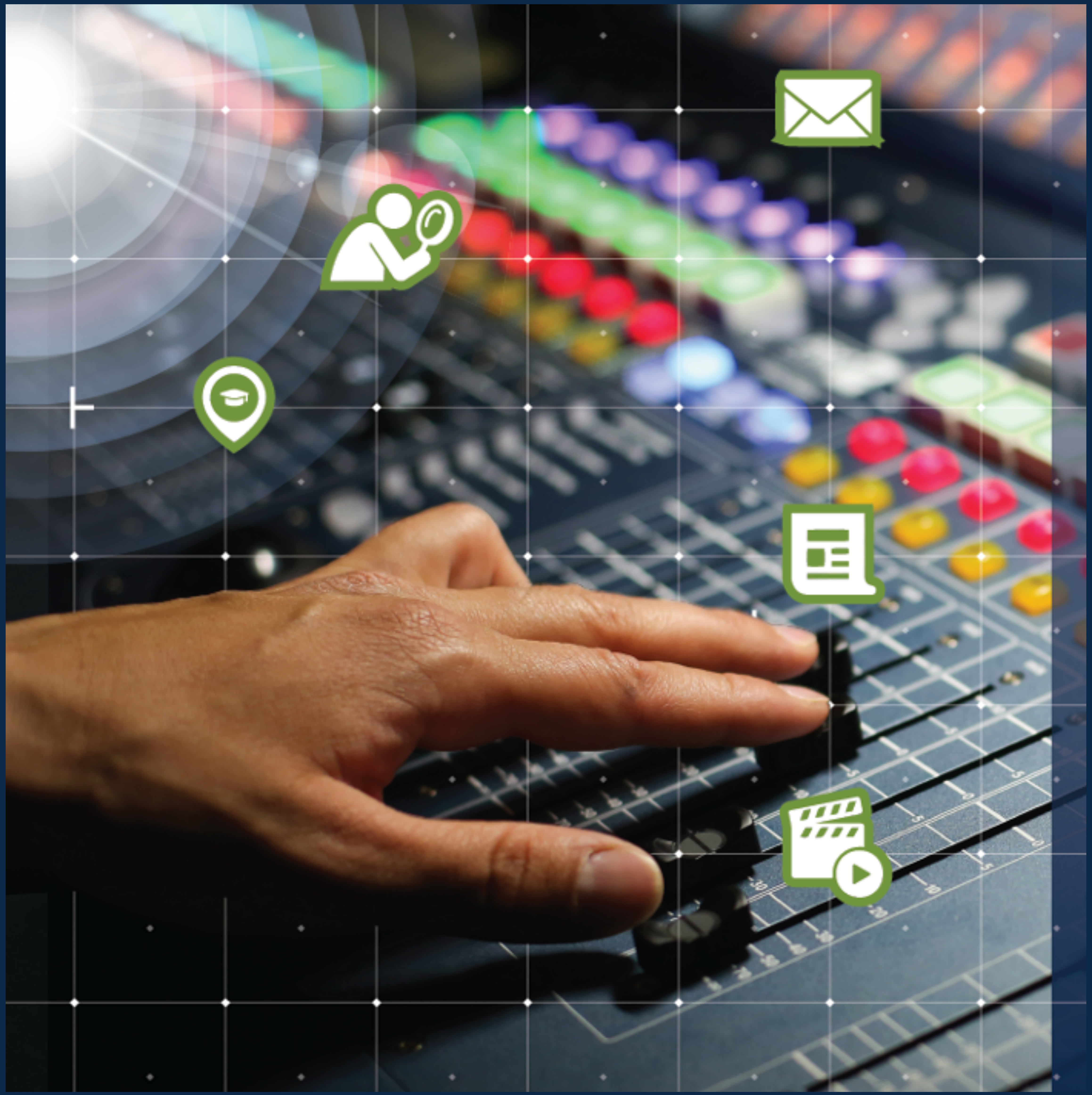
BUILDING ACROSS AN ECOSYSTEM OF CONTENT, SOFTWARE, AND CLOUD

- MAJOR CONTENT OWNERS, CREATORS AND BRANDS
- MAJOR CLOUD PLATFORMS AND SOFTWARE VENDORS
- PRODUCTION, POST, DISTRIBUTION SERVICES
- NATIVE CLOUD SOFTWARE VENDORS AND INTEGRATORS
- AUTOMATED COMPLIANCE AND GOVERNANCE TOOLS

OVERALL 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

PARADIGM SHIFT IN MEDIA & ENTERTAINMENT

- AUDIENCE AND REVENUES MOVING ONLINE
- CONSOLIDATION OF DIGITAL PRODUCTION, POST AND DISTRIBUTION
- RAPID SHIFT TO CLOUD-BASED WORKFLOWS
- BROADER CONSTITUENCY ACROSS M&E SUPPLY CHAIN
- NEW SKILLS AND SECURITY CULTURE REQUIRED

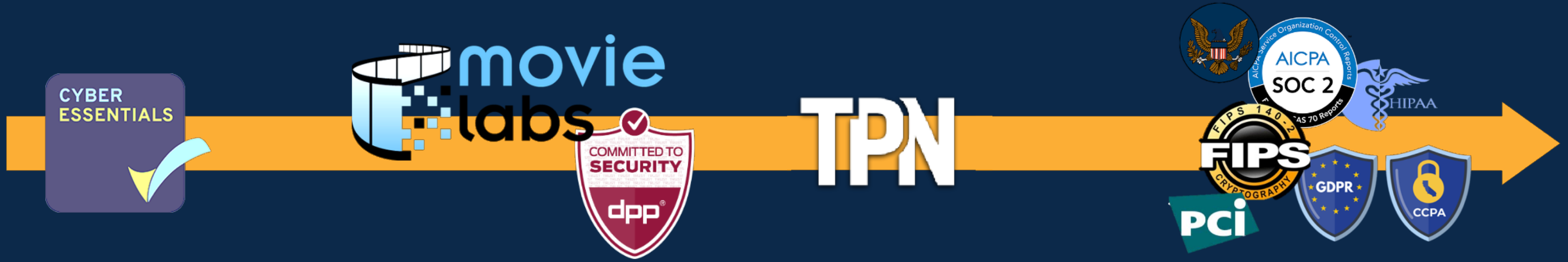
THE EVOLVING M&E INDUSTRY APPROACH

GUIDELINES, PROGRAMS & COMPLIANCE

GUIDANCE

INDUSTRY ALIGNMENT

REGULATION



- Awareness
- Hygiene
- Self Selection

- Checklist
- Self Certified
- Oversight

- Common Controls
- Professional Audit
- Information Sharing

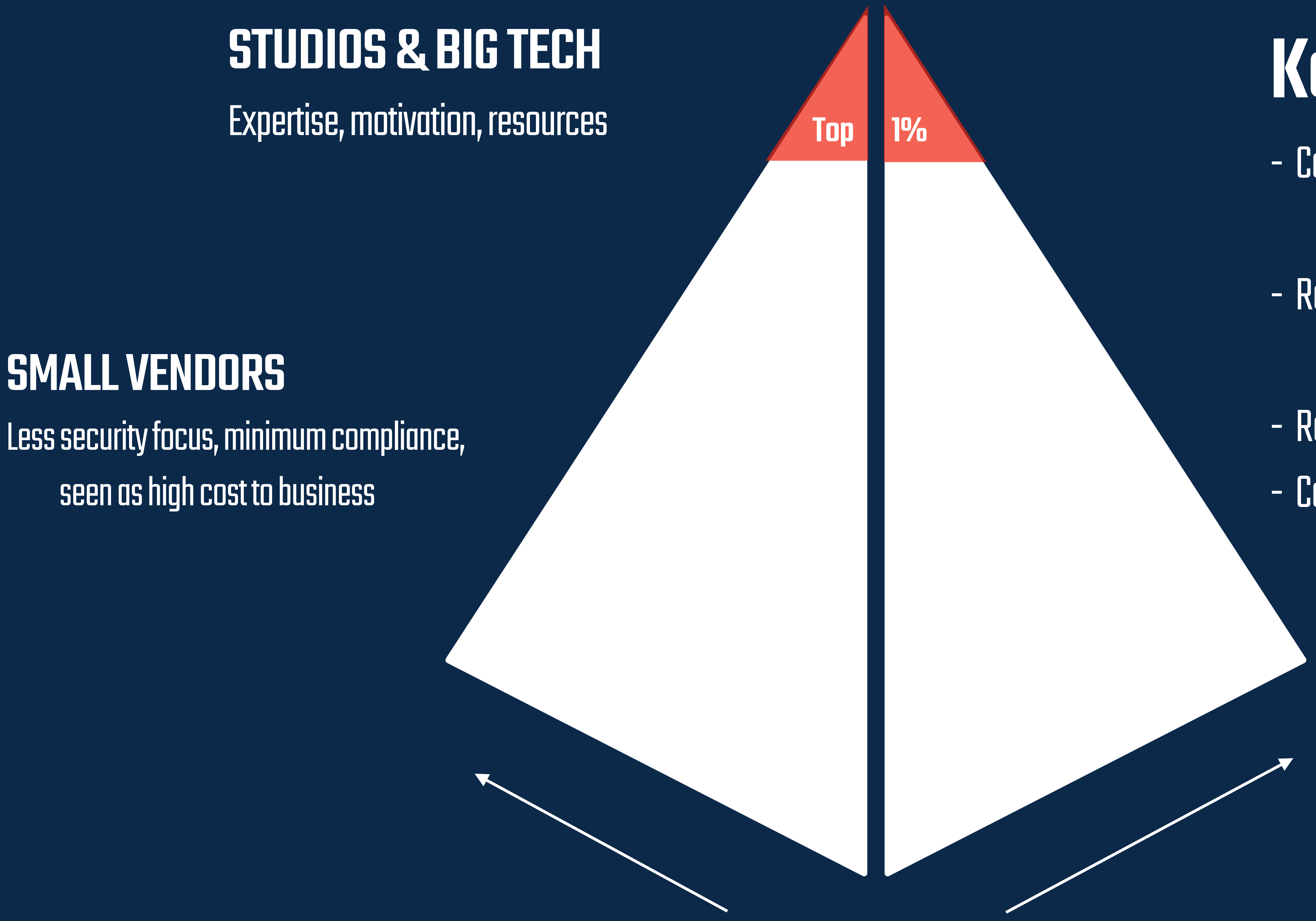
- Industry Acceptance
- Legislation & Penalties
- Repeatability

MPA

BEST PRACTICES - UPDATED 11.11.20

https://www.motionpictures.org/what-we-do/safeguarding-creativity/additional-resources/#content-protection-best-practices

SECURE THE GLOBAL MEDIA SUPPLY CHAIN


STUDIOS & BIG TECH
Expertise, motivation, resources
Top
1%
SMALL VENDORS
Less security focus, minimum compliance, seen as high cost to business

7000+ vendors in ecosystem

Key Program Aims

- Continuity, mapping against solid foundations of MPA & TPN, extended into software driven cloud domain
- Reduce audit costs for vendors and increase consistency of audit for content owners
- Reduce controls editing effort, who needs more custom controls
- Continuous self-audit is essential, software changes fast!

Content Delivery & Security Association

OPEN STANDARDS

CONTROL FRAMEWORK

CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

CLOUD PLATFORMS

ALIGNED SHARED RESPONSIBILITY AND VIRTUALISATION MODELS

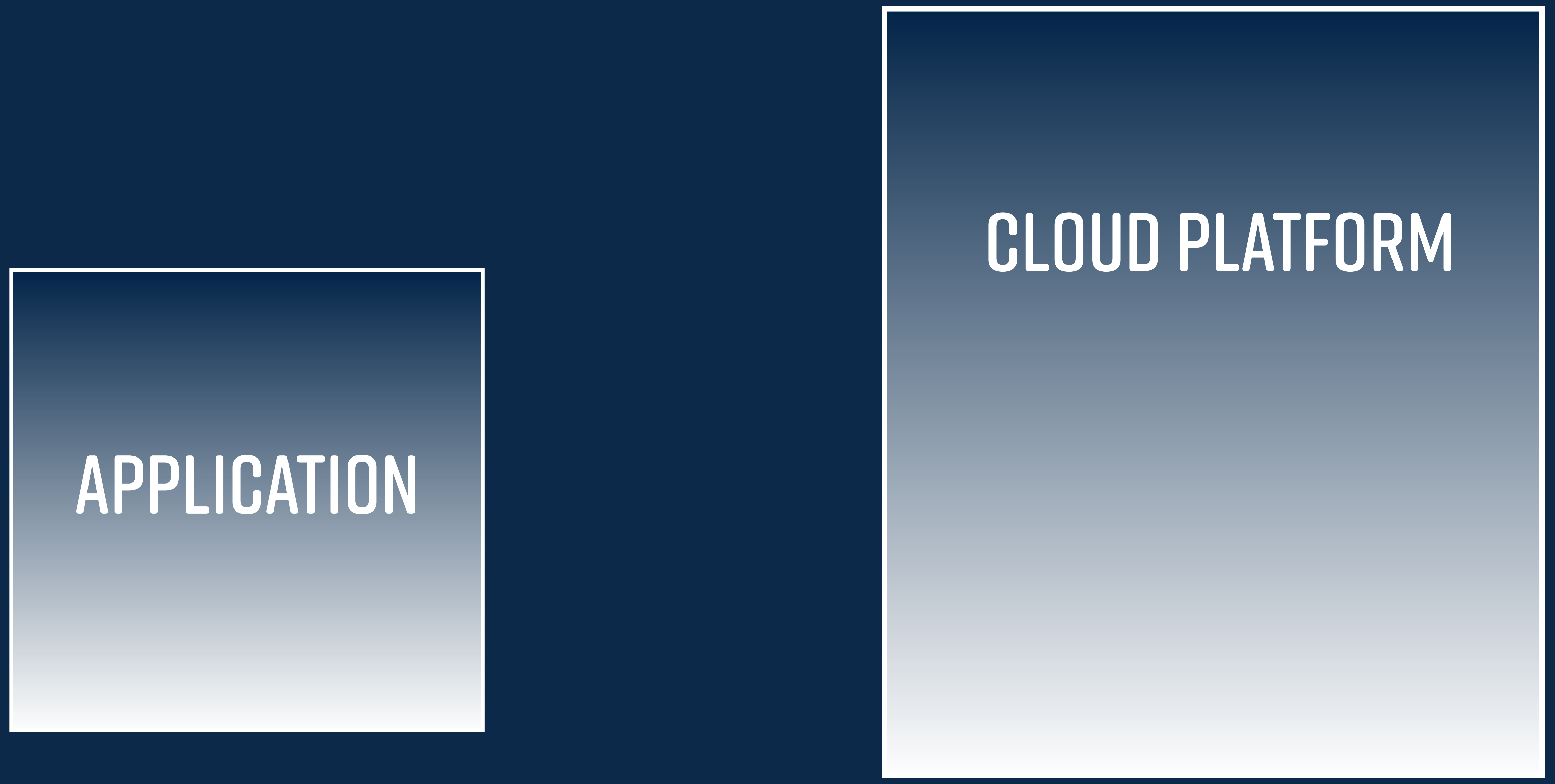
- LATEST “BEST PRACTICE” IMPLEMENTATION ADVICE LINKED TO CONTROLS
  - WHITE PAPERS
  - MEDIA & ENTERTAINMENT PERSPECTIVE
  - PRODUCT SPECIFIC BEST PRACTICE
- COMMON WORKFLOW PATTERNS, END-END SECURITY ADVICE

Alibaba Cloud aws Microsoft Azure Google Cloud IBM Cloud

APPLICATION & CLOUD

ALIGNED SHARED RESPONSIBILITY AND VIRTUALISATION MODELS

- SOFTWARE REVIEW RELEASE PROCESS AND TEAM SKILLS
- INTERACTION BETWEEN COMPONENTS



APPLICATION

CLOUD PLATFORM

APPLICATION & CLOUD...CONFIGURATION

ALIGNED SHARED RESPONSIBILITY AND VIRTUALISATION MODELS

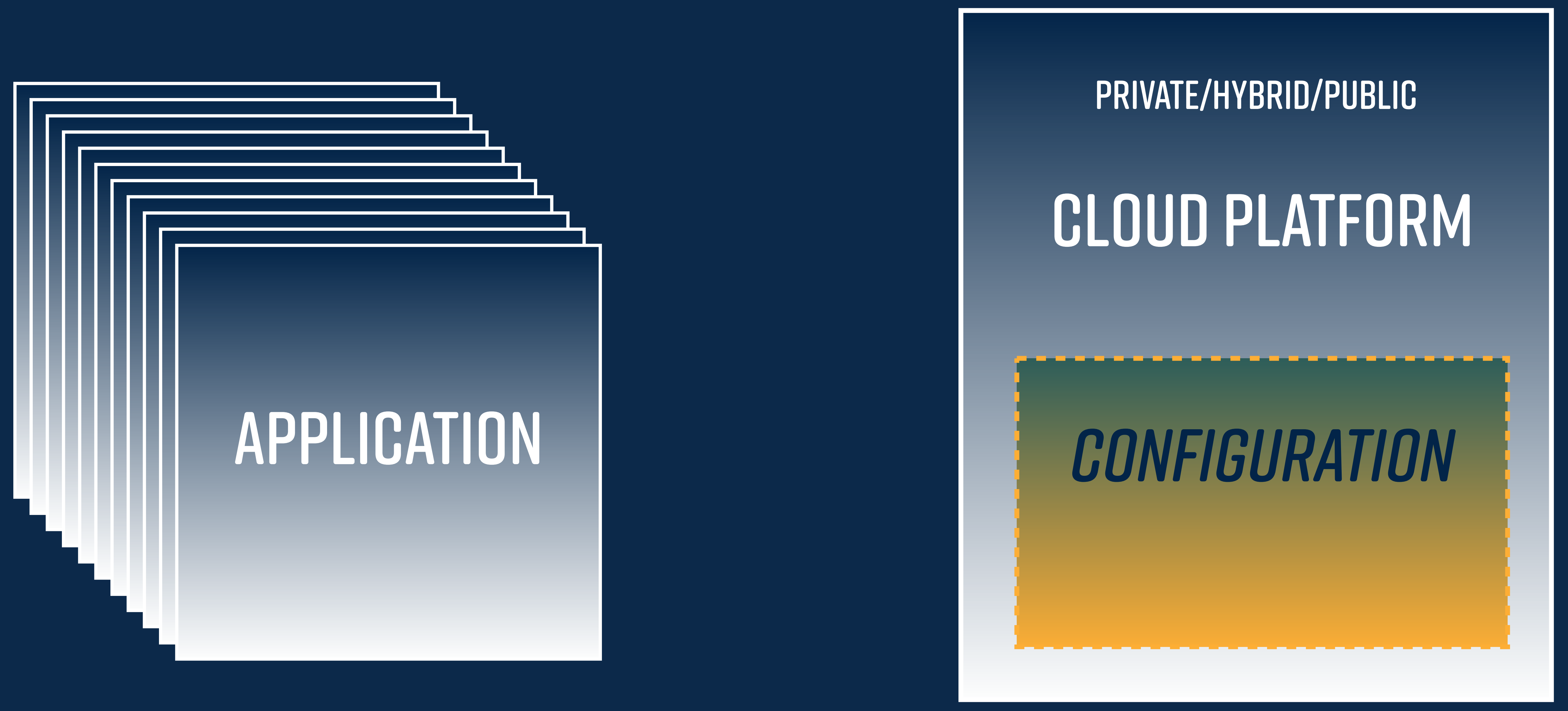
- SOFTWARE REVIEW RELEASE PROCESS AND TEAM SKILLS
- INTERACTION BETWEEN COMPONENTS

APPLICATION
CLOUD PLATFORM
CONFIGURATION

APPLICATION & CLOUD...SCALE

ALIGNED SHARED RESPONSIBILITY AND VIRTUALISATION MODELS

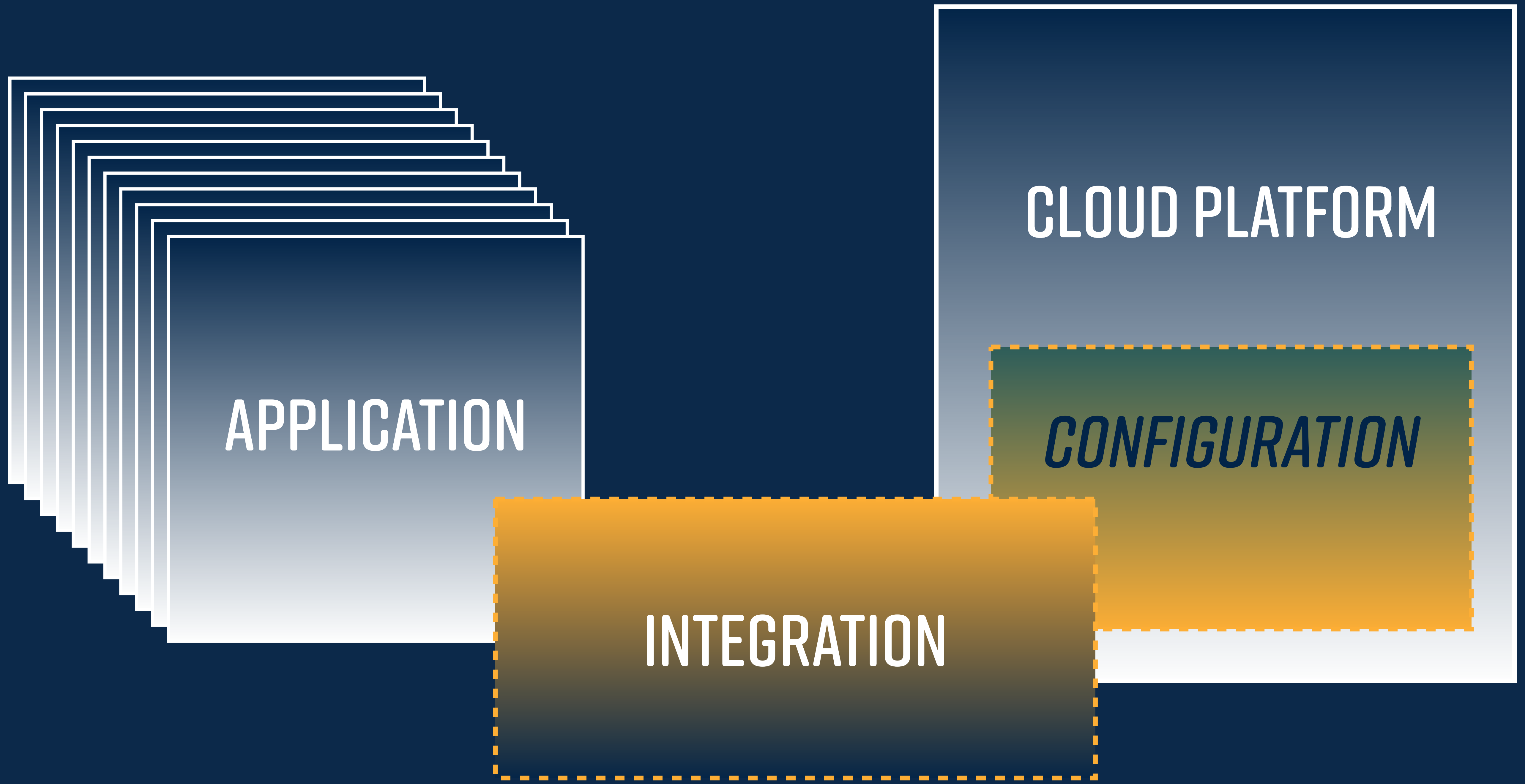
- SOFTWARE REVIEW RELEASE PROCESS AND TEAM SKILLS
- INTERACTION BETWEEN COMPONENTS



APPLICATION & CLOUD...INTEGRATION

ALIGNED SHARED RESPONSIBILITY AND VIRTUALISATION MODELS

- SOFTWARE REVIEW RELEASE PROCESS AND TEAM SKILLS
- INTERACTION BETWEEN COMPONENTS



TECHNOLOGY COMMITTEE

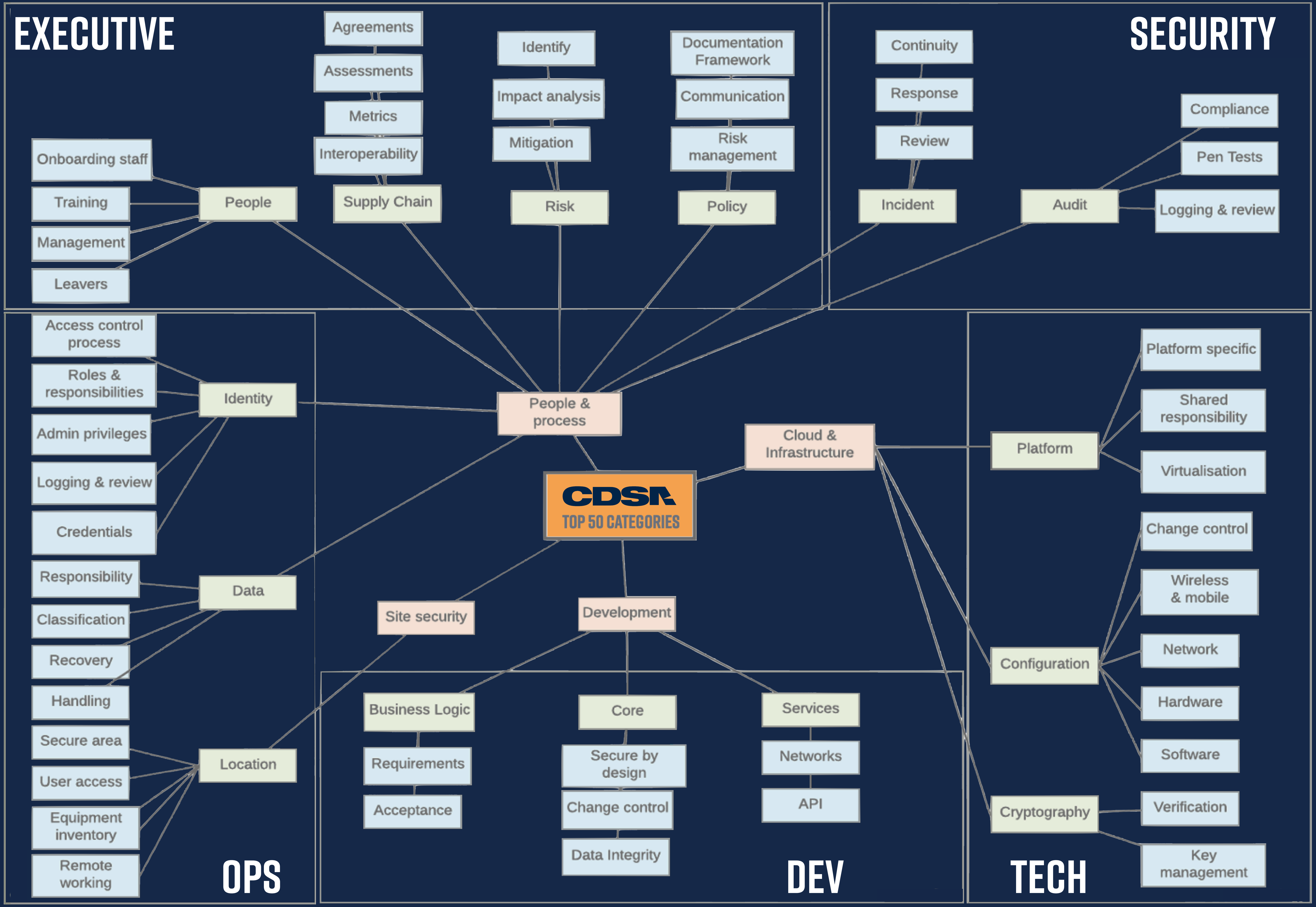
KEY PERSPECTIVES

VOICES FROM THE TECHNOLOGY COMMITTEE CHAIRS

- MAJOR CONTENT OWNER — amazonstudios
- MAJOR SOFTWARE PLATFORM — Adobe
- MULTI-PLATFORM SERVICES — technicolor

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

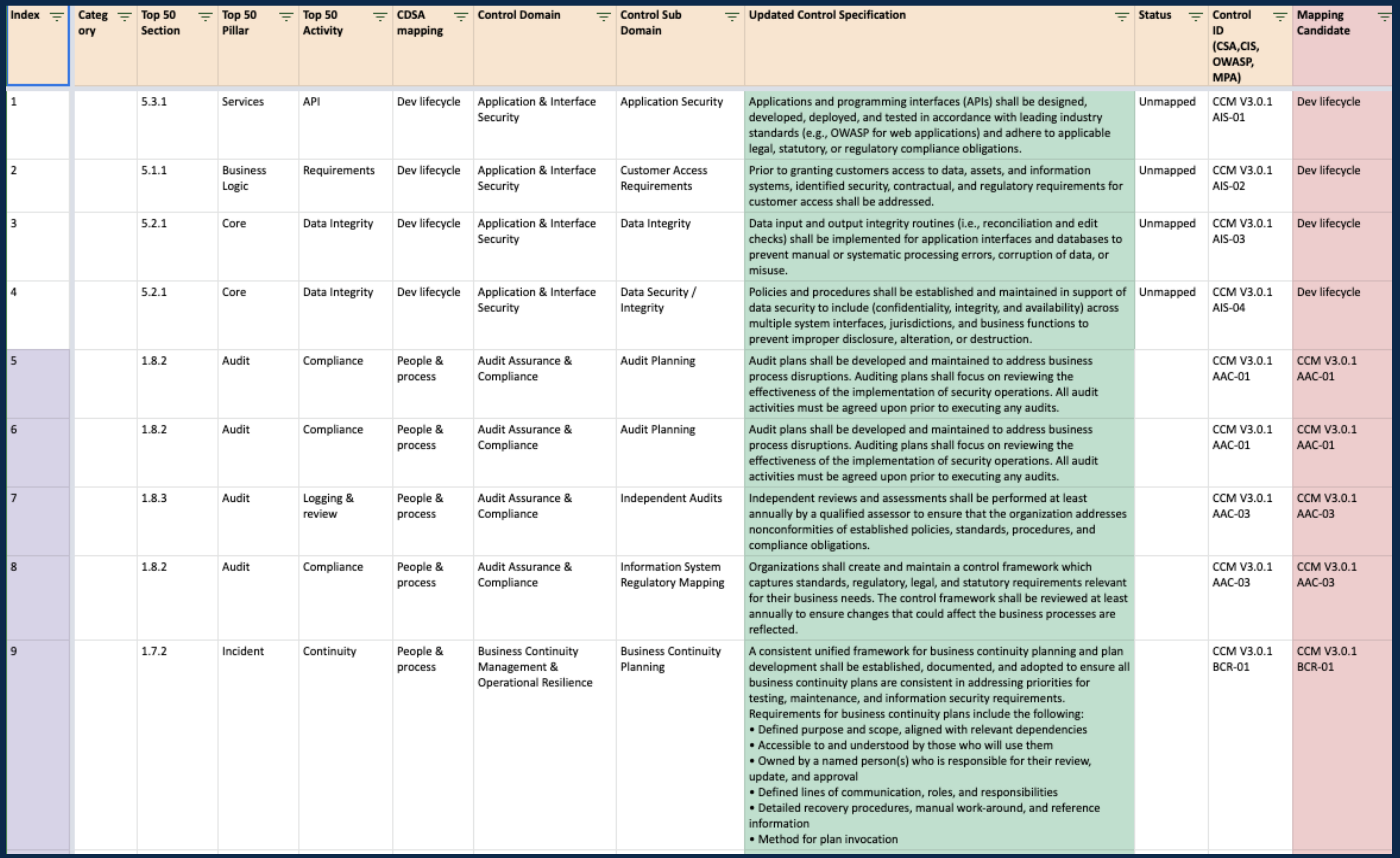
TECH
Platform
Platform specific
Shared responsibility
Virtualisation
Configuration
Change control
Wireless & mobile
Network
Hardware
Software
Cryptography
Verification
Key management

Content Delivery & Security Association

CONTROL SET REVIEW

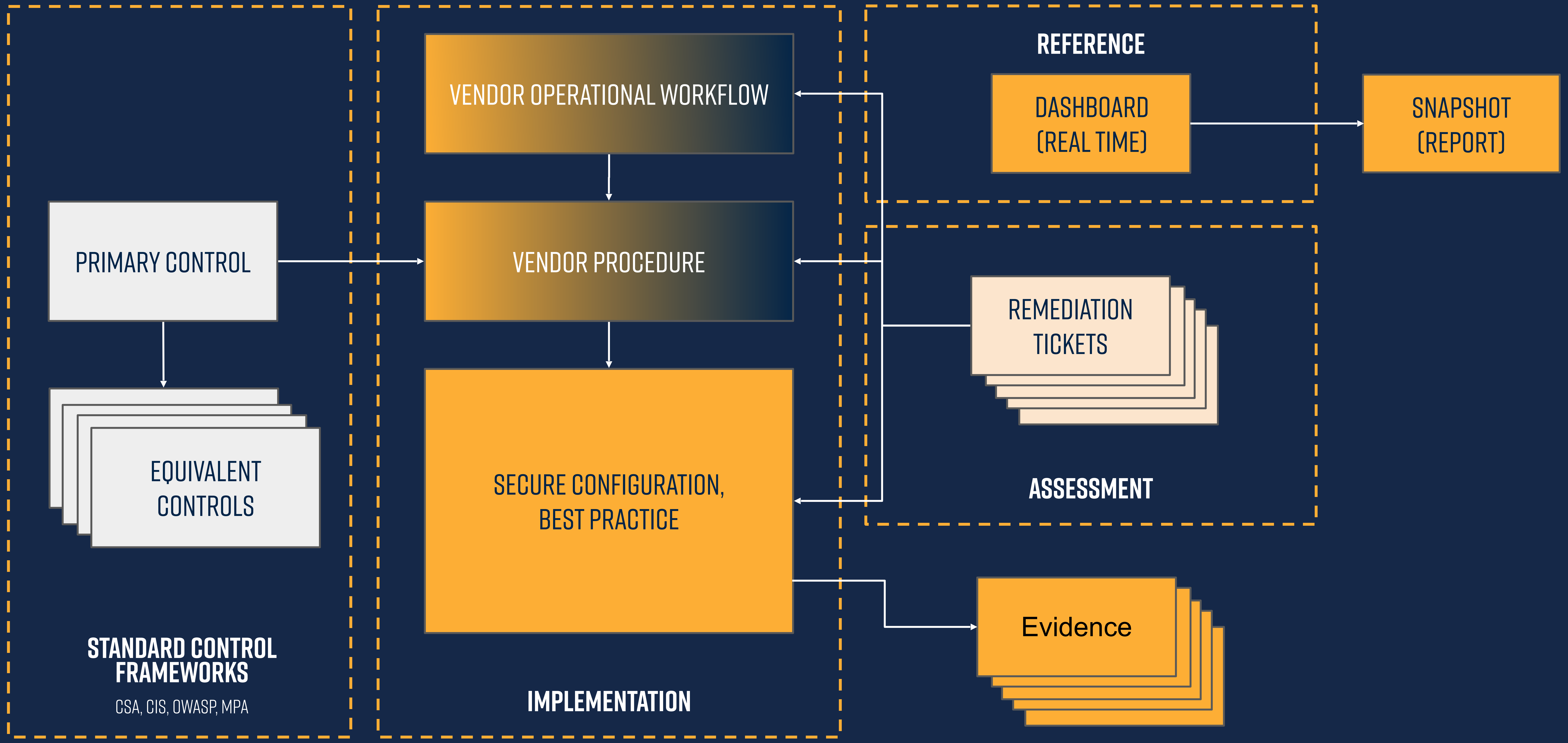
CDSA TECHNOLOGY COMMITTEE: A VOLUNTEER ARMY

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



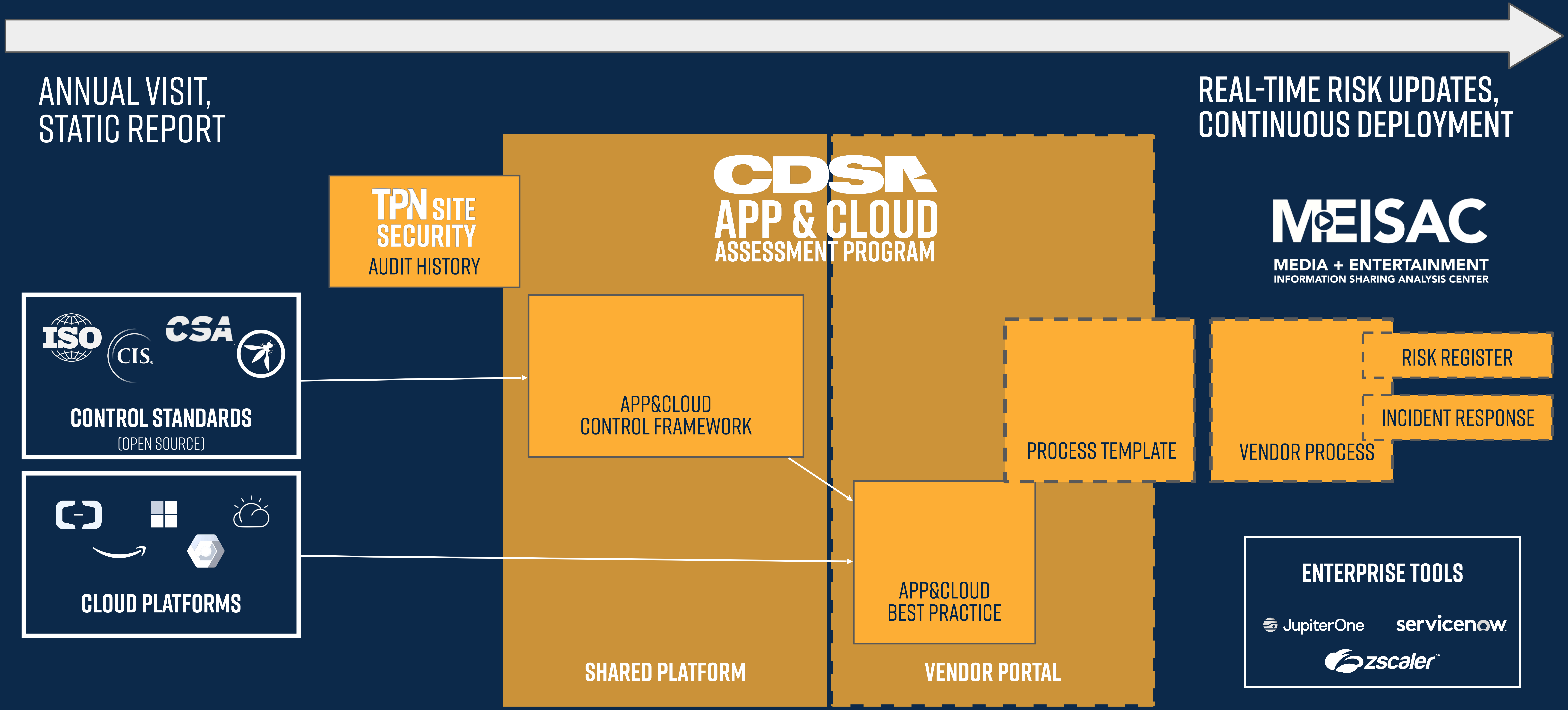
Index	Category	Top 50 Section	Top 50 Pillar	Top 50 Activity	CDSA mapping	Control Domain	Control Sub Domain	Updated Control Specification	Status	Control ID (CSA,CIS, OWASP, MPA)	Mapping Candidate
1		5.3.1	Services	API	Dev lifecycle	Application & Interface Security	Application Security	Applications and 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



CDSA
Content Delivery & Security Association

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

ISO CIS CSA

CONTROL STANDARDS
(OPEN SOURCE)

CLOUD PLATFORMS

APP&CLOUD
CONTROL FRAMEWORK

APP&CLOUD
BEST PRACTICE

PROCESS TEMPLATE

VENDOR PROCESS

RISK REGISTER

INCIDENT RESPONSE

SHARED PLATFORM

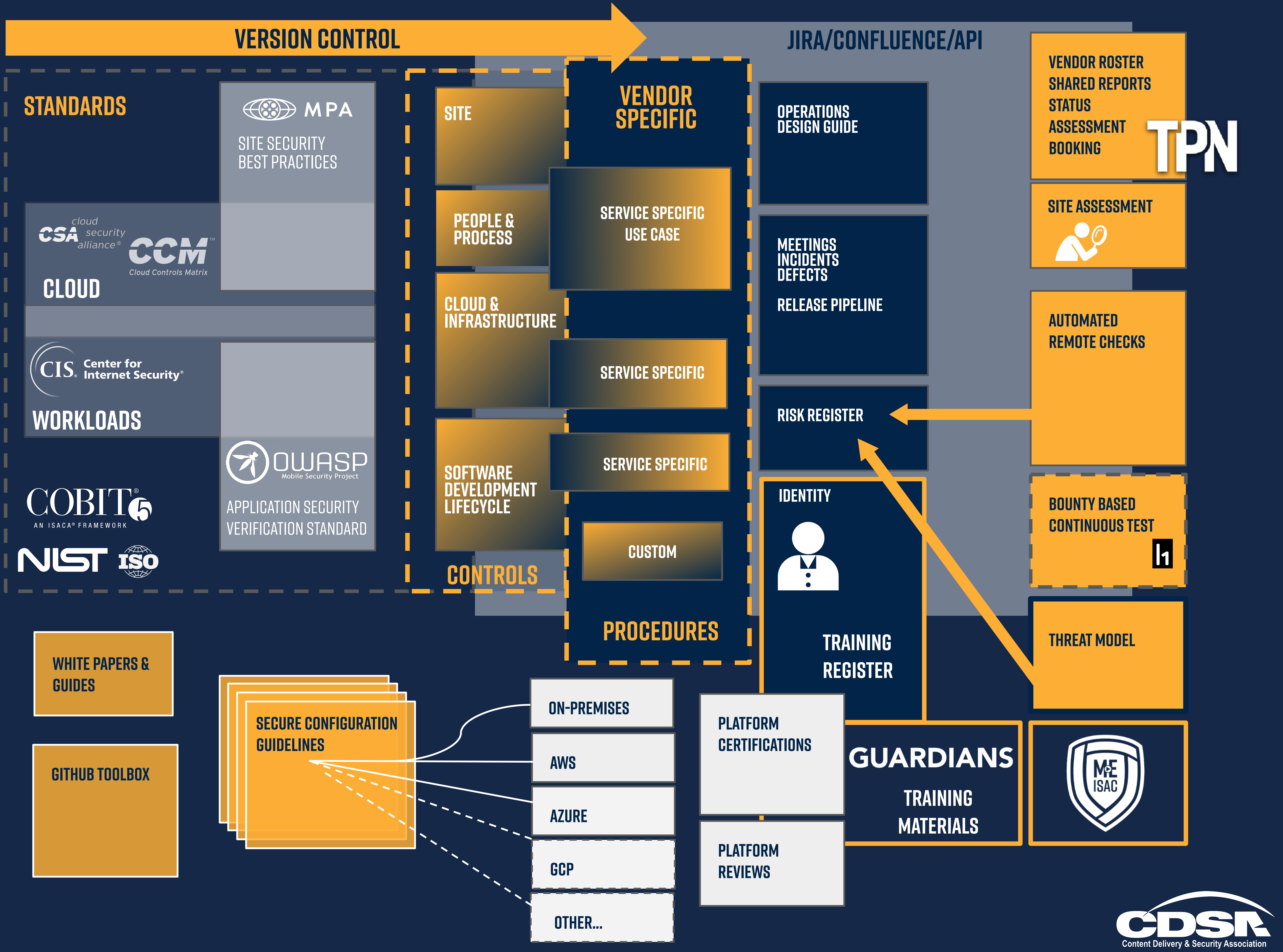
VENDOR PORTAL

ENTERPRISE TOOLS

JupiterOne servicenow zscaler

EVOLUTION: REAL-TIME SECURITY

- REDUCE CONTROLS MAINTENANCE EFFORT
- LEVERAGE CLOUD PLATFORM COLLATERAL
- USABLE DOCUMENTATION, EASY TO ADOPT AN APPROACH
- HIGHLIGHT CONTROL CHANGES AND NEW THREATS/INTEL
- ENABLE SKILLS DEVELOPMENT
- NEW AUDIT SUPPORT



VERSION CONTROL

JIRA/CONFLUENCE/API

STANDARDS

MPA
SITE SECURITY BEST PRACTICES

CSA cloud security alliance
CCM Cloud Controls Matrix
CLOUD

CIS Center for Internet Security
WORKLOADS

OWASP Mobile Security Project
APPLICATION SECURITY VERIFICATION STANDARD

COBIT 5 AN ISACA FRAMEWORK

NIST

ISO

SITE

PEOPLE & PROCESS

CLOUD & INFRASTRUCTURE

SOFTWARE DEVELOPMENT LIFECYCLE

CONTROLS

VENDOR SPECIFIC

SERVICE SPECIFIC USE CASE

SERVICE SPECIFIC

SERVICE SPECIFIC

CUSTOM

PROCEDURES

OPERATIONS DESIGN GUIDE

MEETINGS
INCIDENTS
DEFECTS

RELEASE PIPELINE

RISK REGISTER

IDENTITY

TRAINING REGISTER

VENDOR ROSTER
SHARED REPORTS
STATUS
ASSESSMENT
BOOKING

TPN

SITE ASSESSMENT

AUTOMATED REMOTE CHECKS

BOUNTY BASED CONTINUOUS TEST

THREAT MODEL

WHITE PAPERS & GUIDES

GITHUB TOOLBOX

SECURE CONFIGURATION GUIDELINES

ON-PREMISES

AWS

AZURE

GCP

OTHER...

PLATFORM CERTIFICATIONS

PLATFORM REVIEWS

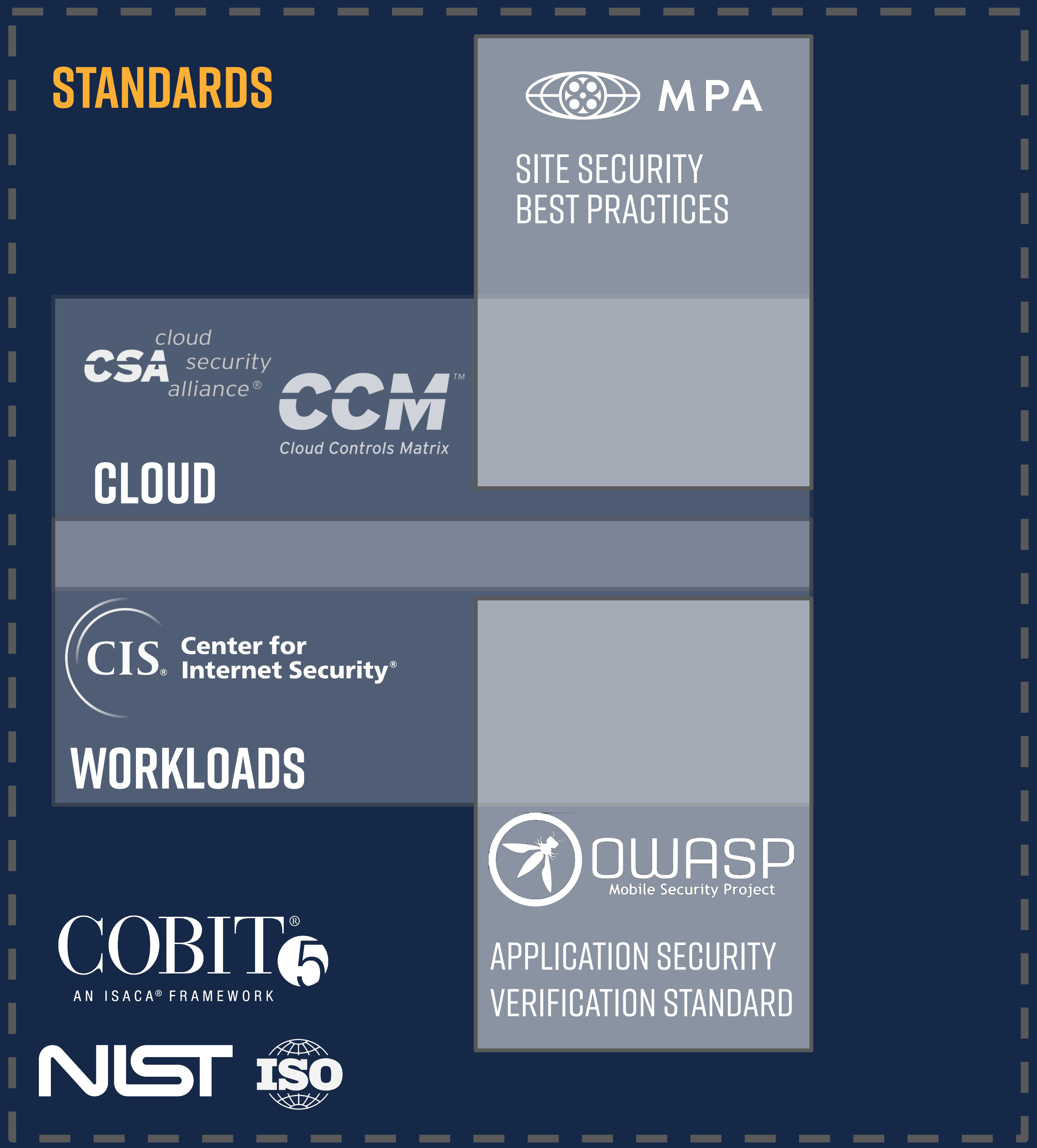
GUARDIANS

TRAINING MATERIALS

ME-ISAC

CDSA
Content Delivery & Security Association

- REDUCE CONTROLS MAINTENANCE EFFORT



STANDARDS

MPA

SITE SECURITY BEST PRACTICES

CSA cloud security alliance®

CCM™ Cloud Controls Matrix

CLOUD

CIS. Center for Internet Security®

WORKLOADS

OWASP Mobile Security Project

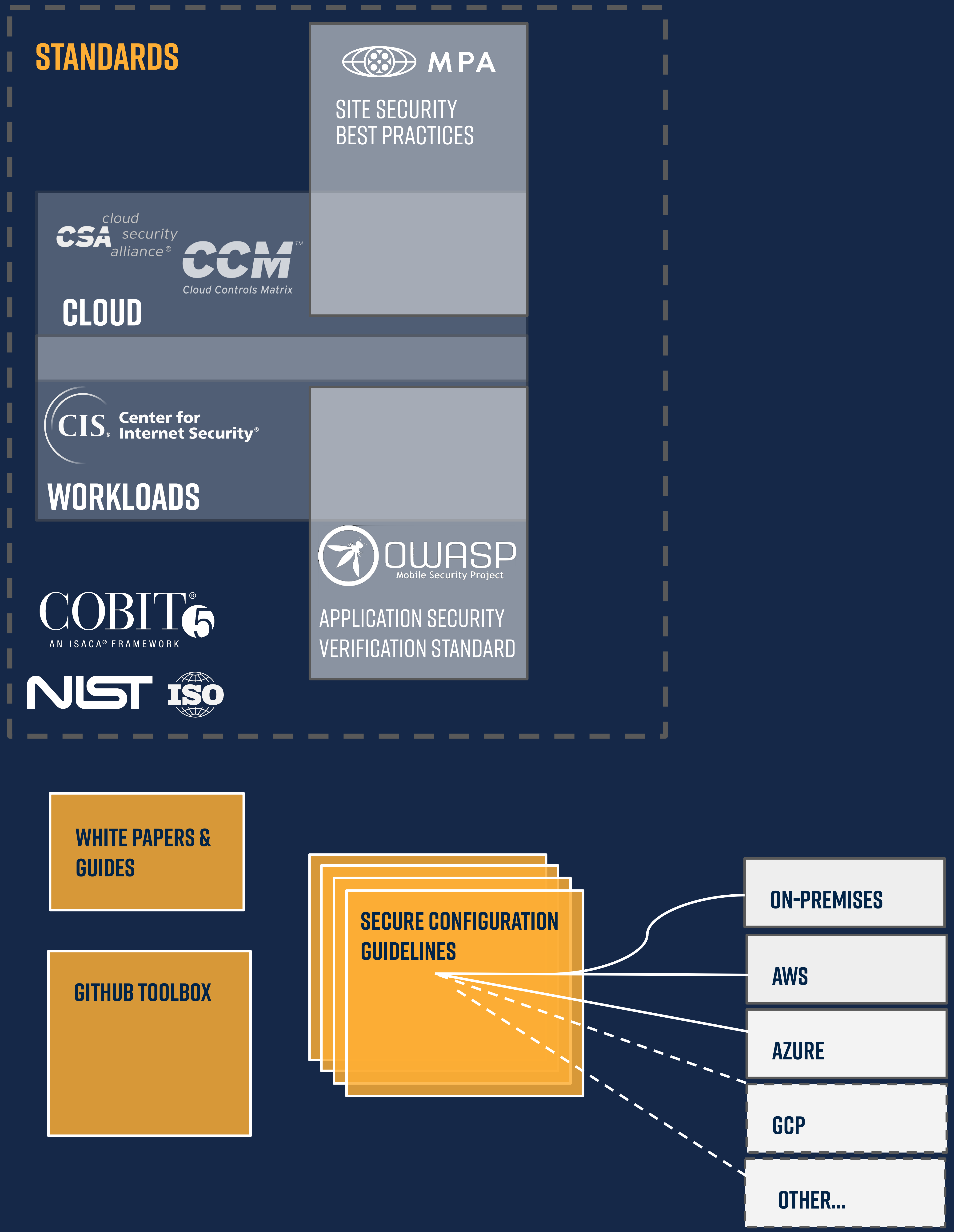
APPLICATION SECURITY VERIFICATION STANDARD

COBIT® 5 AN ISACA® FRAMEWORK

NIST

ISO

- REDUCE CONTROLS MAINTENANCE EFFORT
- LEVERAGE CLOUD PLATFORM COLLATERAL



STANDARDS

MPA

SITE SECURITY BEST PRACTICES

CSA cloud security alliance® CCM™ Cloud Controls Matrix

CLOUD

CIS. Center for Internet Security®

WORKLOADS

OWASP Mobile Security Project

APPLICATION SECURITY VERIFICATION STANDARD

COBIT® 5 AN ISACA® FRAMEWORK

NIST ISO

WHITE PAPERS & GUIDES

GITHUB TOOLBOX

SECURE CONFIGURATION GUIDELINES

ON-PREMISES

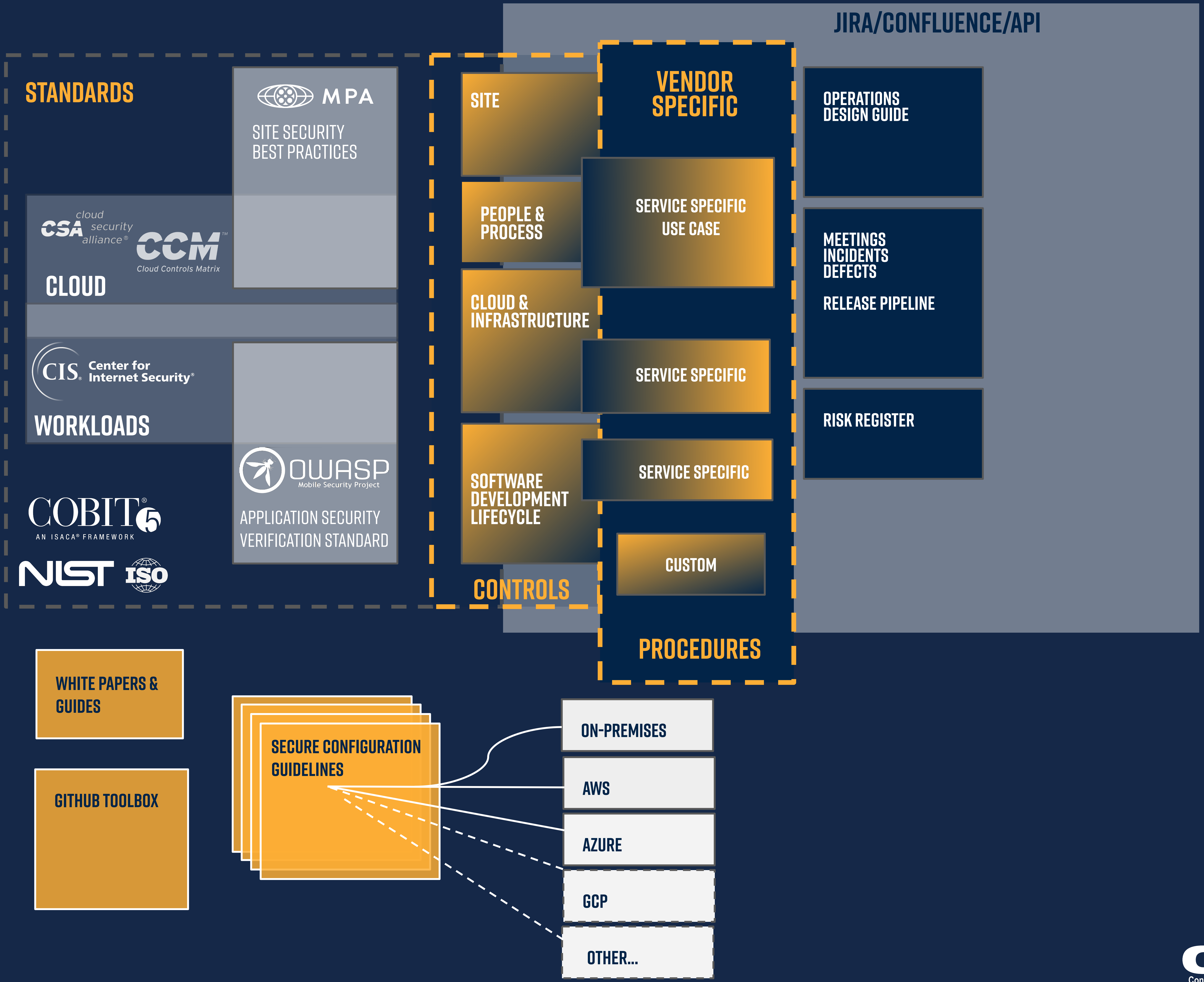
AWS

AZURE

GCP

OTHER...

- REDUCE CONTROLS MAINTENANCE EFFORT
- LEVERAGE CLOUD PLATFORM COLLATERAL
- USABLE DOCUMENTATION, EASY TO ADOPT AN APPROACH



JIRA/CONFLUENCE/API

STANDARDS

MPA
SITE SECURITY BEST PRACTICES

CSA cloud security alliance®
CCM™ Cloud Controls Matrix
CLOUD

CIS® Center for Internet Security®
WORKLOADS

OWASP Mobile Security Project
APPLICATION SECURITY VERIFICATION STANDARD

COBIT® 5
AN ISACA® FRAMEWORK

NIST ISO

CONTROLS

SITE

PEOPLE & PROCESS

CLOUD & INFRASTRUCTURE

SOFTWARE DEVELOPMENT LIFECYCLE

VENDOR SPECIFIC

SERVICE SPECIFIC USE CASE

SERVICE SPECIFIC

SERVICE SPECIFIC

CUSTOM

PROCEDURES

OPERATIONS DESIGN GUIDE

MEETINGS
INCIDENTS
DEFECTS

RELEASE PIPELINE

RISK REGISTER

WHITE PAPERS & GUIDES

GITHUB TOOLBOX

SECURE CONFIGURATION GUIDELINES

ON-PREMISES

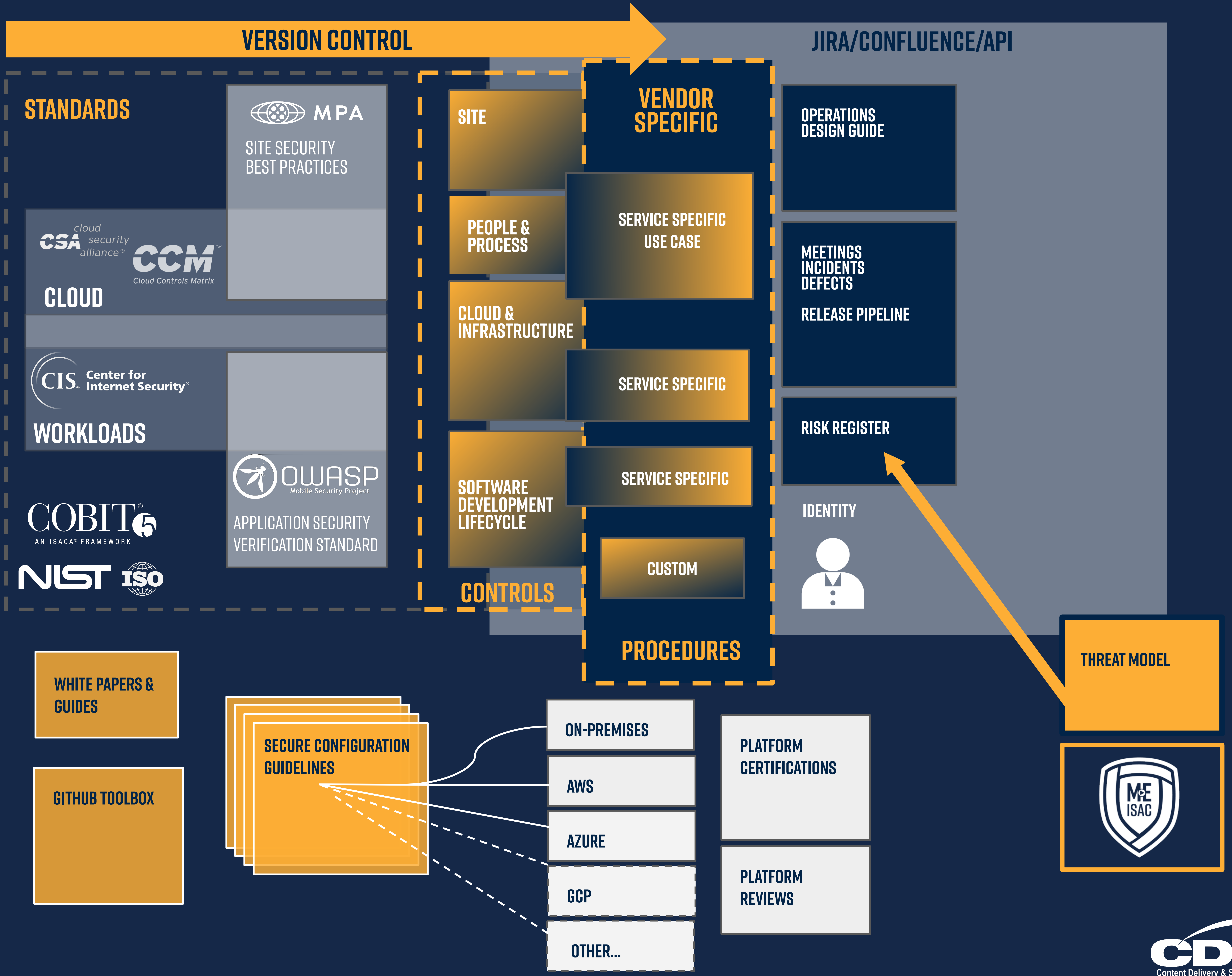
AWS

AZURE

GCP

OTHER...

- REDUCE CONTROLS MAINTENANCE EFFORT
- LEVERAGE CLOUD PLATFORM COLLATERAL
- USABLE DOCUMENTATION, EASY TO ADOPT AN APPROACH
- HIGHLIGHT CONTROL CHANGES AND NEW THREATS/INTEL



VERSION CONTROL

JIRA/CONFLUENCE/API

STANDARDS

MPA SITE SECURITY BEST PRACTICES

CSA cloud security alliance® CCM™ Cloud Controls Matrix

CLOUD

CIS. Center for Internet Security®

WORKLOADS

OWASP Mobile Security Project

APPLICATION SECURITY VERIFICATION STANDARD

COBIT®5 AN ISACA® FRAMEWORK

NIST ISO

SITE

PEOPLE & PROCESS

CLOUD & INFRASTRUCTURE

SOFTWARE DEVELOPMENT LIFECYCLE

CONTROLS

VENDOR SPECIFIC

SERVICE SPECIFIC USE CASE

SERVICE SPECIFIC

SERVICE SPECIFIC

CUSTOM

PROCEDURES

OPERATIONS DESIGN GUIDE

MEETINGS
INCIDENTS
DEFECTS

RELEASE PIPELINE

RISK REGISTER

IDENTITY

THREAT MODEL

ME ISAC

WHITE PAPERS & GUIDES

GITHUB TOOLBOX

SECURE CONFIGURATION GUIDELINES

ON-PREMISES

AWS

AZURE

GCP

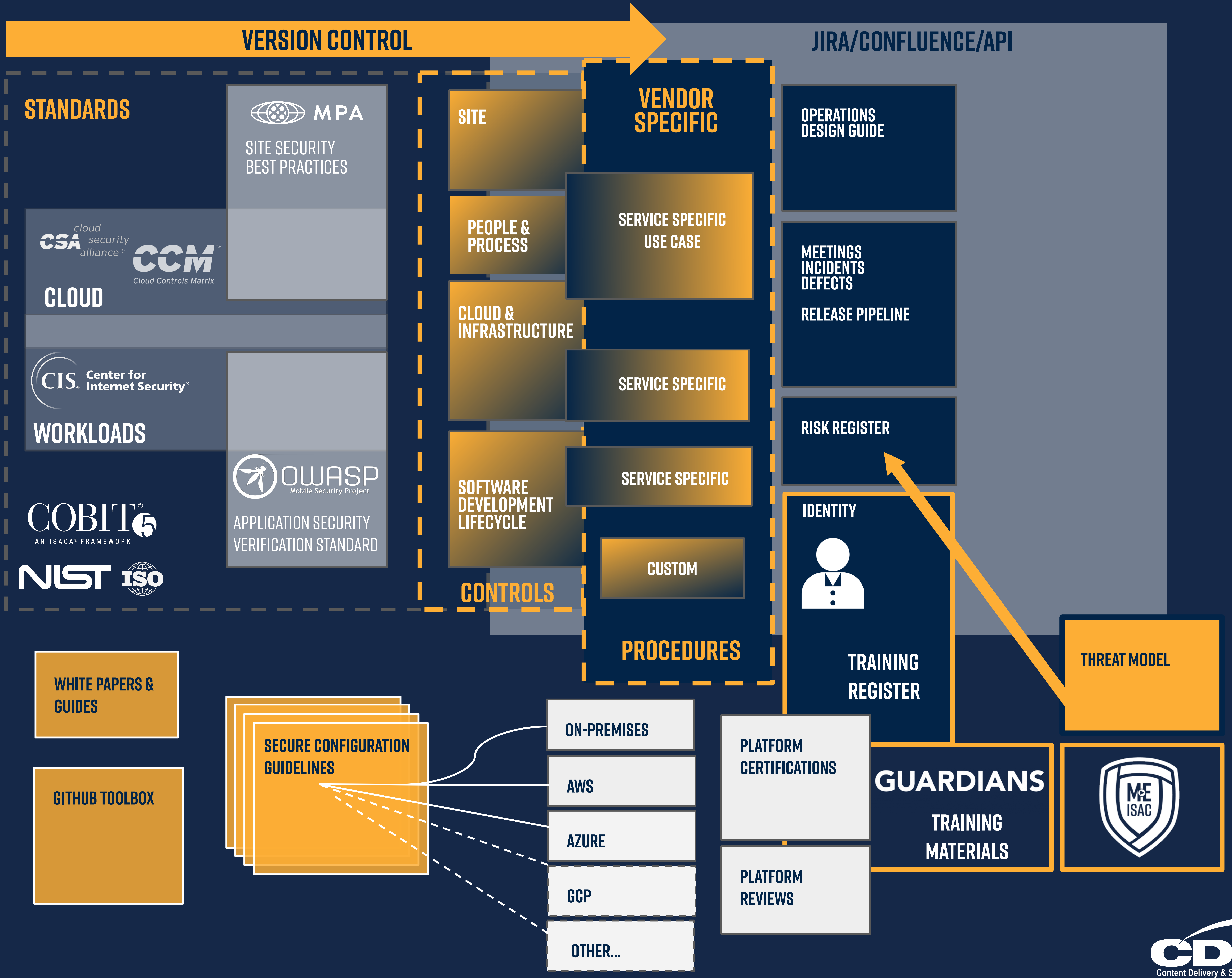
OTHER...

PLATFORM CERTIFICATIONS

PLATFORM REVIEWS

CDSA Content Delivery & Security Association

- REDUCE CONTROLS MAINTENANCE EFFORT
- LEVERAGE CLOUD PLATFORM COLLATERAL
- USABLE DOCUMENTATION, EASY TO ADOPT AN APPROACH
- HIGHLIGHT CONTROL CHANGES AND NEW THREATS/INTEL
- ENABLE SKILLS DEVELOPMENT



VERSION CONTROL

JIRA/CONFLUENCE/API

STANDARDS

MPA
SITE SECURITY
BEST PRACTICES

CSA cloud security alliance®
CCM™ Cloud Controls Matrix
CLOUD

CIS Center for Internet Security®
WORKLOADS

OWASP Mobile Security Project
APPLICATION SECURITY
VERIFICATION STANDARD

COBIT 5
AN ISACA® FRAMEWORK

NIST

ISO

SITE

PEOPLE & PROCESS

CLOUD & INFRASTRUCTURE

SOFTWARE DEVELOPMENT LIFECYCLE

CONTROLS

VENDOR SPECIFIC

SERVICE SPECIFIC USE CASE

SERVICE SPECIFIC

SERVICE SPECIFIC

CUSTOM

PROCEDURES

OPERATIONS DESIGN GUIDE

MEETINGS
INCIDENTS
DEFECTS

RELEASE PIPELINE

RISK REGISTER

IDENTITY

TRAINING REGISTER

THREAT MODEL

WHITE PAPERS & GUIDES

GITHUB TOOLBOX

SECURE CONFIGURATION GUIDELINES

ON-PREMISES

AWS

AZURE

GCP

OTHER...

PLATFORM CERTIFICATIONS

PLATFORM REVIEWS

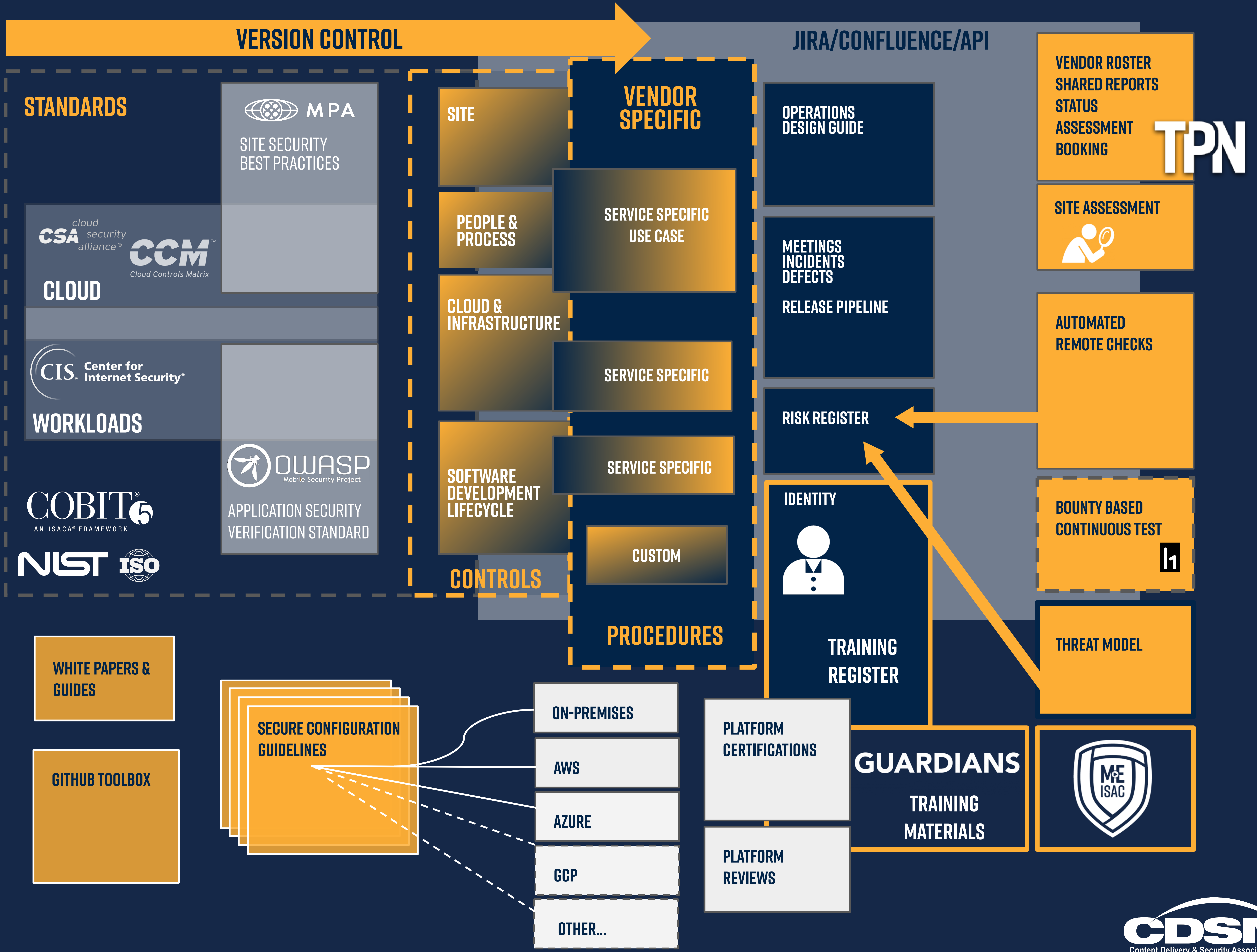
GUARDIANS

TRAINING MATERIALS

ME ISAC

CDSA
Content Delivery & Security Association

- REDUCE CONTROLS MAINTENANCE EFFORT
- LEVERAGE CLOUD PLATFORM COLLATERAL
- USABLE DOCUMENTATION, EASY TO ADOPT AN APPROACH
- HIGHLIGHT CONTROL CHANGES AND NEW THREATS/INTEL
- ENABLE SKILLS DEVELOPMENT
- NEW AUDIT SUPPORT



VERSION CONTROL

JIRA/CONFLUENCE/API

STANDARDS

MPA
SITE SECURITY BEST PRACTICES

CSA cloud security alliance
CCM Cloud Controls Matrix
CLOUD

CIS Center for Internet Security
WORKLOADS

OWASP Mobile Security Project
APPLICATION SECURITY VERIFICATION STANDARD

COBIT 5 AN ISACA FRAMEWORK

NIST ISO

SITE

PEOPLE & PROCESS

CLOUD & INFRASTRUCTURE

SOFTWARE DEVELOPMENT LIFECYCLE

CONTROLS

VENDOR SPECIFIC

SERVICE SPECIFIC USE CASE

SERVICE SPECIFIC

SERVICE SPECIFIC

CUSTOM

PROCEDURES

OPERATIONS DESIGN GUIDE

MEETINGS
INCIDENTS
DEFECTS

RELEASE PIPELINE

RISK REGISTER

IDENTITY

TRAINING REGISTER

VENDOR ROSTER
SHARED REPORTS
STATUS
ASSESSMENT
BOOKING

TPN

SITE ASSESSMENT

AUTOMATED REMOTE CHECKS

BOUNTY BASED CONTINUOUS TEST

THREAT MODEL

WHITE PAPERS & GUIDES

GITHUB TOOLBOX

SECURE CONFIGURATION GUIDELINES

ON-PREMISES

AWS

AZURE

GCP

OTHER...

PLATFORM CERTIFICATIONS

PLATFORM REVIEWS

GUARDIANS

TRAINING MATERIALS

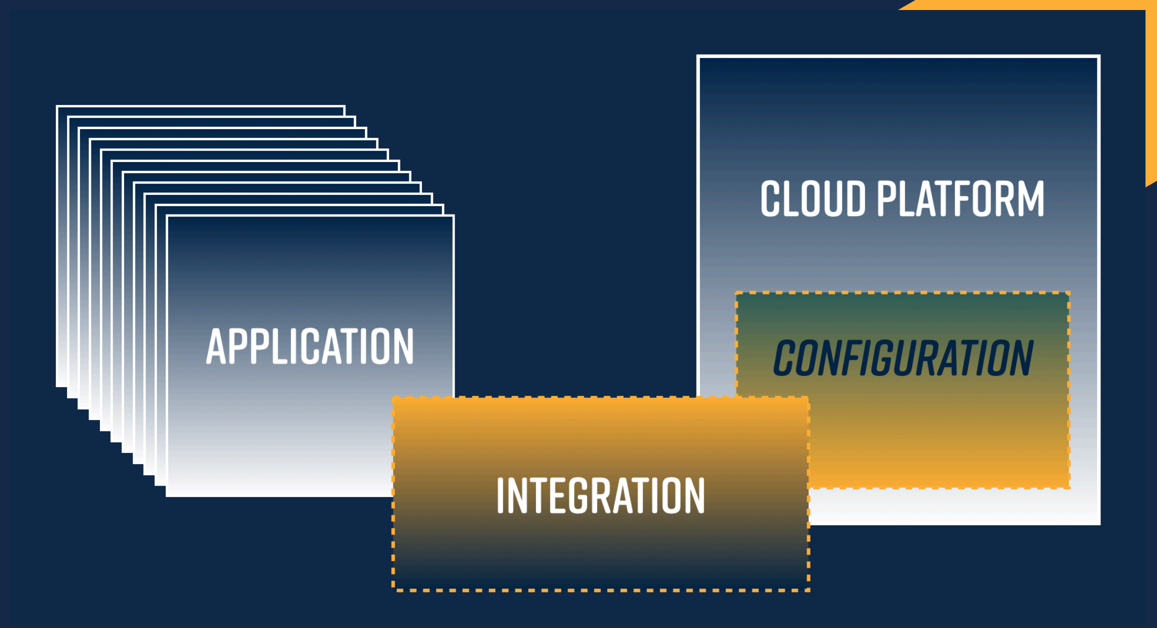
ME-ISAC

CDSA Content Delivery & Security Association

WHERE WE ARE GOING...

ROADMAP

IDENTIFY TARGETS



CONFIRM STANDARDS FRAMEWORK

ISO

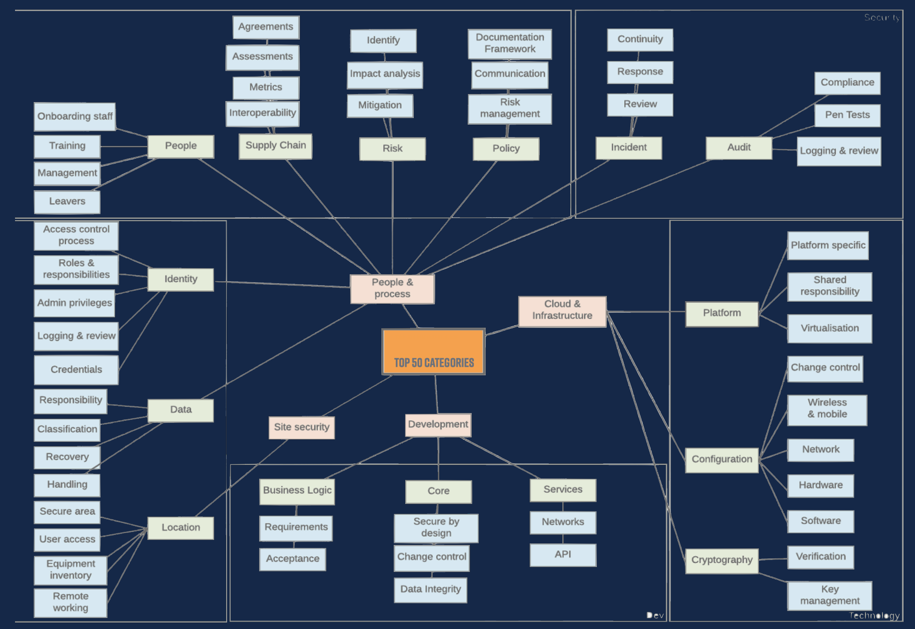
CSA cloud security alliance®

CIS. Center for Internet Security®

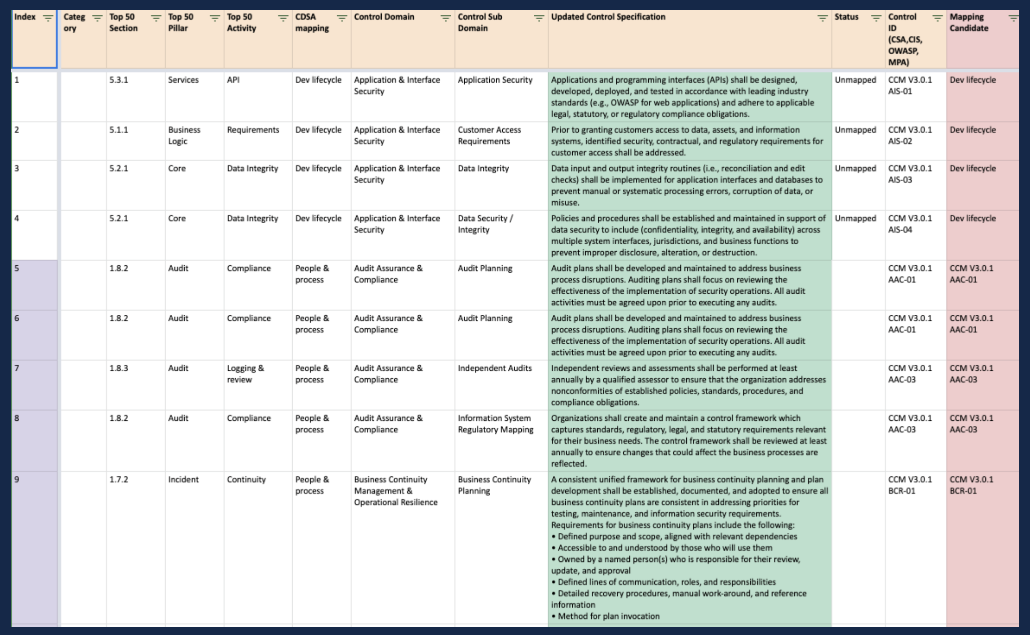
OWASP Mobile Security Project

BEST PRACTICES

HIGH LEVEL ORIENTATION



DETAILED ROADMAP



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

PUBLISH CONTROL FRAMEWORK

We are here

ROAD-TEST USE CASES

VENDOR BETA

CDSA
Content Delivery & Security Association

QUESTIONS, IDEAS OR COMMENTS?

Contact: bschofield@CDSAonline.org

CDSA
Content Delivery & Security Association