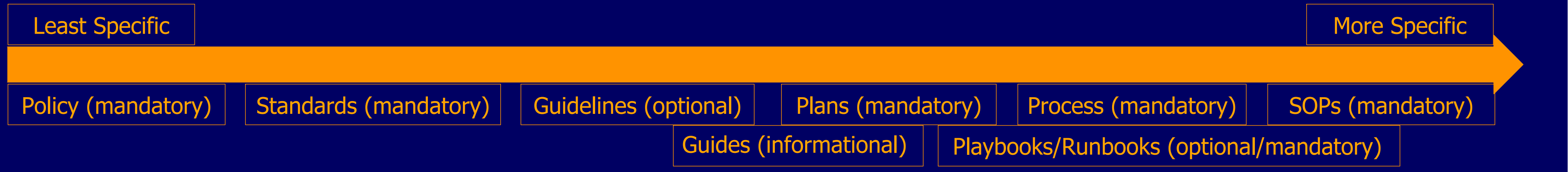
A Policy and Harmonized Control Framework Reference Architecture

Each industry sector has it's own specifics that need to be addressed, whether Retail, Logistics, Healthcare, Banking & Finance, Insurance, or Manufacturing. This policy and harmonized control framework reference architecture cannot legitimately address all relevant specifics. Adapt this accordingly or modify to tailor based on a fit-for-purpose assessment.



A harmonized control framework groups and maps relevant controls across a broader spectrum of laws, standards, and control frameworks to reduce control bloat and duplication in a manner consistent with a company's industry sector and regulatory requirements. Therefore, a single control may be mapped to 2, 4, 6 or more other controls in order to have 1 control and not 2, 4, 6 or more duplicative controls.

Control mapping is seldom perfect and requires taking into account strategic, tactical, and operational controls within additional administrative (people), operational (process), and technical (technology) controls. In this manner, don't include what is not contextually relevant to the organization.

The functional mapping with reduction in controls and duplication provides an audit many, evidence once perspective in addition to a key method for organizaiton and categorization across multiple functional areas.

This reference architecture uses the NIST 800-53 control families as a base to organize controls, policies, standards, guidelines, process, SOPs, etc. As an example it is not a definitive method. There may be a different perspective contextually and logically relevant for different organizations.

This is just one way of looking at it. The key is simplicity, consistency, and the ability maintain relevant categorization from controls to policies to standards to guidelines to process to SOPs, etc.

Organziational policies are generally well understood as the rules of behavior defined in a manner that is enforceable across the orgnization consistently for all personnel and systems. Likewise, LoB Application Policies are understood to be the application or system level policies that support organizational policies, standards, and controls. LoB policies are generally configured within a platform or an application and organizational policies are documents found on an intranet portal.

In this example, Access Control policies do not have to be broken into different on-prem, hybrid, or cloud policies they're all contained in a single Access Control policy. Ensuring content consistency and not duplicating similar content between "different" policies or creating overlapping policies with the same content. A secondary goal is the reduction in effort for maintaining each organizational policy over the long-term.

As a different perspective it means not having different overlapping Access Control policies for Azure, AWS, Google, and systems in an owned datacenter. Focus on commonality as the basis and address uniqueness in separate sections not separate policy documents.

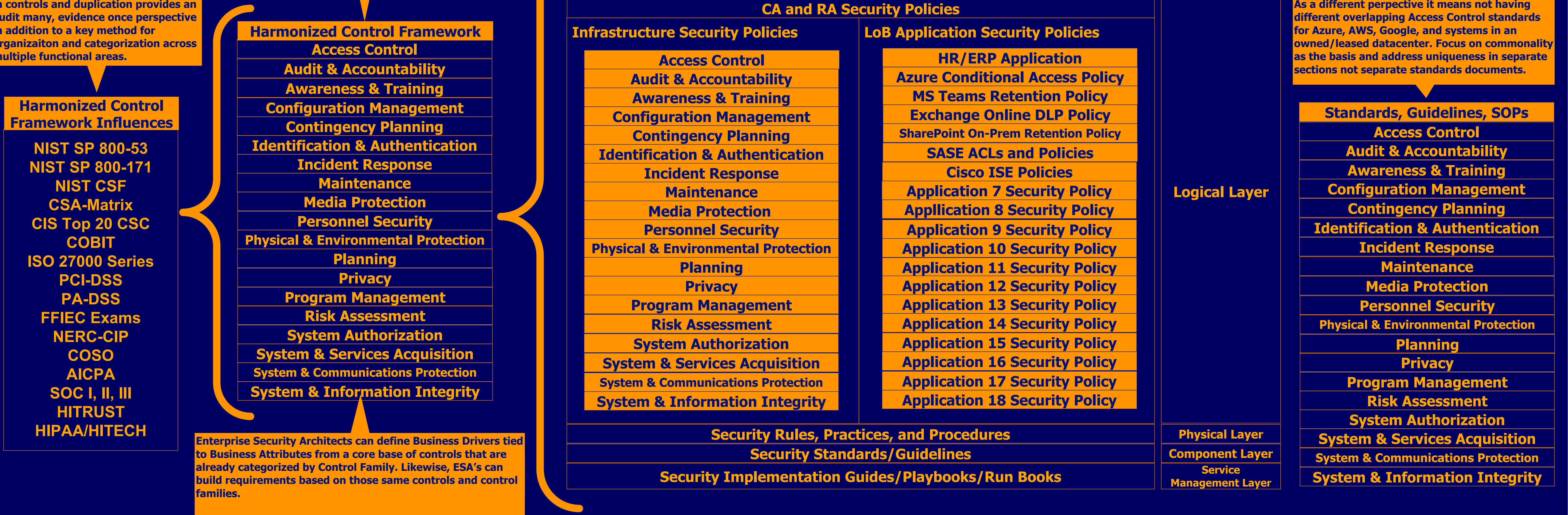
The below block diagram references a SABSA policy architecture modified to consider the control families as logical policy categories.

Utilizing the control families from the harmonized control framework allows for categorization logically to group simular items. This delivers built-in organization for standards, guidelines, process, SOPs, playbooks, and runbooks.

Each can be grouped logically into similar relevant areas. It's a simple method for maintaining organizational relevance and consistency within the overall capability of knowledge management and replication.

In this example, Access Control standards do not have to be broken into different on-prem, hybrid, or cloud standards they're all contained in a single Access Control standard. Ensuring content consistency and not duplicating similar content between "different" standards or creating overlapping standards with the same content. A secondary goal is the reduction in effort for maintain standards, guidelines, process, and SOPs, etc. over the long-term.

As a different perpective it means not having different overlapping Access Control standards for Azure, AWS, Google, and systems in an owned/leased datacenter. Focus on commonality as the basis and address uniqueness in separate sections not separate standards documents.



Harmonized Control Framework Influences

NIST SP 800-53
NIST SP 800-171
NIST CSF
CSA-Matrix
CIS Top 20 CSC
COBIT
ISO 27000 Series
PCI-DSS
PA-DSS
FFIEC Exams
NERC-CIP
COSO
AICPA
SOC I, II, III
HITRUST
HIPAA/HITECH

Harmonized Control Framework

Access Control
Audit & Accountability
Awareness & Training
Configuration Management
Contingency Planning
Identification & Authentication
Incident Response
Maintenance
Media Protection
Personnel Security
Physical & Environmental Protection
Planning
Privacy
Program Management
Risk Assessment
System Authorization
System & Services Acquisition
System & Communications Protection
System & Information Integrity

Organizational Policies/Line of Business Application Security Policies

Overaching Operational Risk Management Policy

Enterprise Security Policy | Acceptable Use Policy | Business Continuity Policy

CA and RA Security Policies

Infrastructure Security Policies

Access Control
Audit & Accountability
Awareness & Training
Configuration Management
Contingency Planning
Identification & Authentication
Incident Response
Maintenance
Media Protection
Personnel Security
Physical & Environmental Protection
Planning
Privacy
Program Management
Risk Assessment
System Authorization
System & Services Acquisition
System & Communications Protection
System & Information Integrity

LoB Application Security Policies

HR/ERP Application
Azure Conditional Access Policy
MS Teams Retention Policy
Exchange Online DLP Policy
SharePoint On-Prem Retention Policy
SASE ACLs and Policies
Cisco ISE Policies
Application 7 Security Policy
Appllication 8 Security Policy
Application 9 Security Policy
Application 10 Security Policy
Application 11 Security Policy
Application 12 Security Policy
Application 13 Security Policy
Application 14 Security Policy
Application 15 Security Policy
Application 16 Security Policy
Application 17 Security Policy
Application 18 Security Policy

Security Rules, Practices, and Procedures
Security Standards/Guidelines
Security Implementation Guides/Playbooks/Run Books

SABSA Layers

Logical Layer
Physical Layer
Component Layer
Service Management Layer

Standards, Guidelines, SOPs

Access Control
Audit & Accountability
Awareness & Training
Configuration Management
Contingency Planning
Identification & Authentication
Incident Response
Maintenance
Media Protection
Personnel Security
Physical & Environmental Protection
Planning
Privacy
Program Management
Risk Assessment
System Authorization
System & Services Acquisition
System & Communications Protection
System & Information Integrity

Enterprise Security Architects can define Business Drivers tied to Business Attributes from a core base of controls that are already categorized by Control Family. Likewise, ESA's can build requirements based on those same controls and control families.

Because the control families tie to policies and standards they're defensible when someone asks to show where this is required.