COSAC 2025

Rob Campbell

WORKSHOP W6

MOVING TOWARDS A FUNCTIONAL SECURITY SERVICES CATALOGUE

From TSI R100 Challenges to Practical SSRM Implementation

www.assuredcontrol.com/rescue

COSAC

Workshop Objectives

Transform security services cataloguing from TSI R100's theoretical challenges into practical, implementable frameworks using SSRM, SABSA methodology, and AI-accelerated development.

01

Understand TSI R100 origins and challenges

02

Validate the Security Services Relationship Model (SSRM) ontology and framework

03

Learn something new

04

Set us up to create practical security service models

05

Leverage AI for accelerated development

06

Decide the future direction of TSI R100

TS R100: Security Services Catalogue

Traditional control frameworks provide requirements but don't describe actual security building blocks that deliver protection.

Where are we today

The Vision

- Standardised security services repository
- Off-the-shelf architectural building blocks
- Common terminology & reference framework
- SABSA + TOGAF integration
- Professional security management approach

The Promise

- Business-driven security alignment
- Standardised architectural building blocks and services repository
- Reusable capability definitions - Common terminology and reference framework
- Common language across teams – EA and ESA integration goals
- Accelerated solution delivery

The Reality

Multiple attempts through working groups, but no real progress.

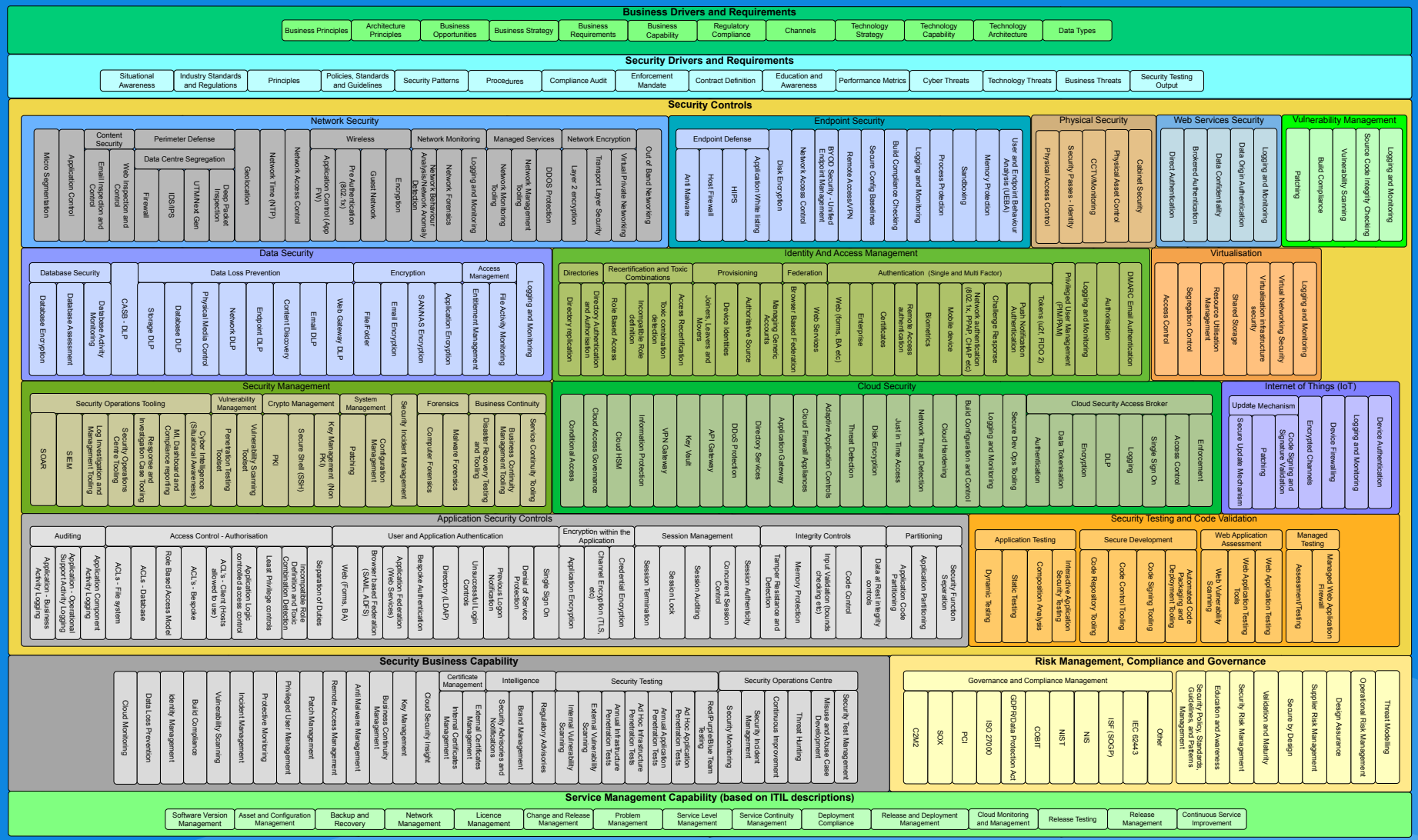
- 7 years later (2018-2025): Core appendices remain empty
- Database schema - marked as "future work" with no completion date
- Catalogue content - reserved appendix with no actual services defined
- Practitioner guidance - promised but never delivered

The Barriers

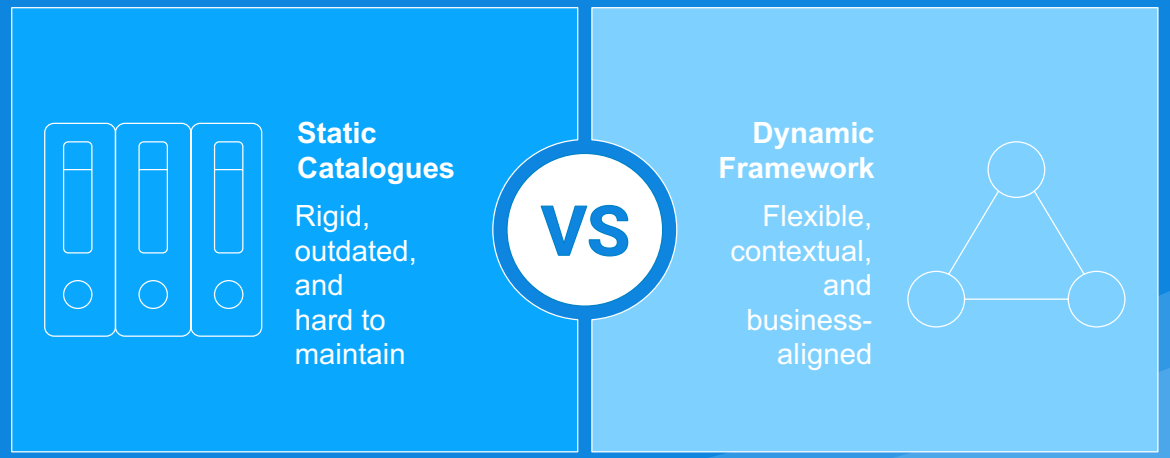
From TSI R100's own assessment:

- Database schema complexity
- Content development bottlenecks
- Lack of practitioner guidance
- Static vs. dynamic requirements
- Maintenance overhead concerns
- Misunderstood definitions

With Ignorance, some naivety and a little arrogance, I thought, **“Surely we are just talking about a better version of this.”**



Down with the Catalogue: Long live the Framework (plus a bit of SABSA method)



The catalogue was right at the time; however, I realised that it would never be finished and would never be quite right.

WHY

Challenge of Static Catalogues

- Rigid tiered taxonomies become outdated
- “One-size-fits-all” lists ignore varying business contexts
- Maintenance nightmares: schema updates for every change

WHAT NOW

The Services Framework - A Dynamic Relationship-Based Framework

- Central graph of Domains → Sub-Domains → Controls → Mechanisms
- Contextual queries yield business-specific catalogues on demand
- Versioned, auditable views lock in consistency per use case

Key Advantages

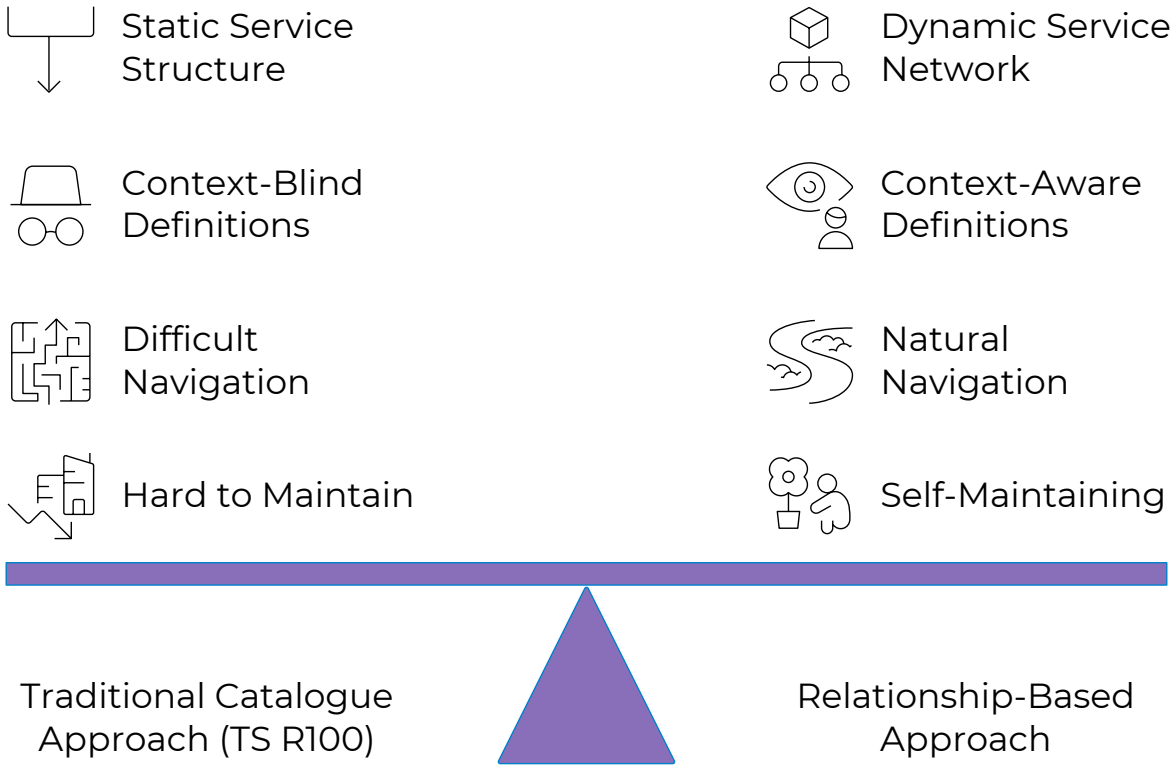
- Business-Driven: Start from business needs, not fixed lists
- Agile Adaptation: Add new services or policies without redesign
- Governance Guardrails: Mandatory relationship rules ensure compliance
- Reusable Artefacts: Slices of the same model serve multiple projects

Relationship-based

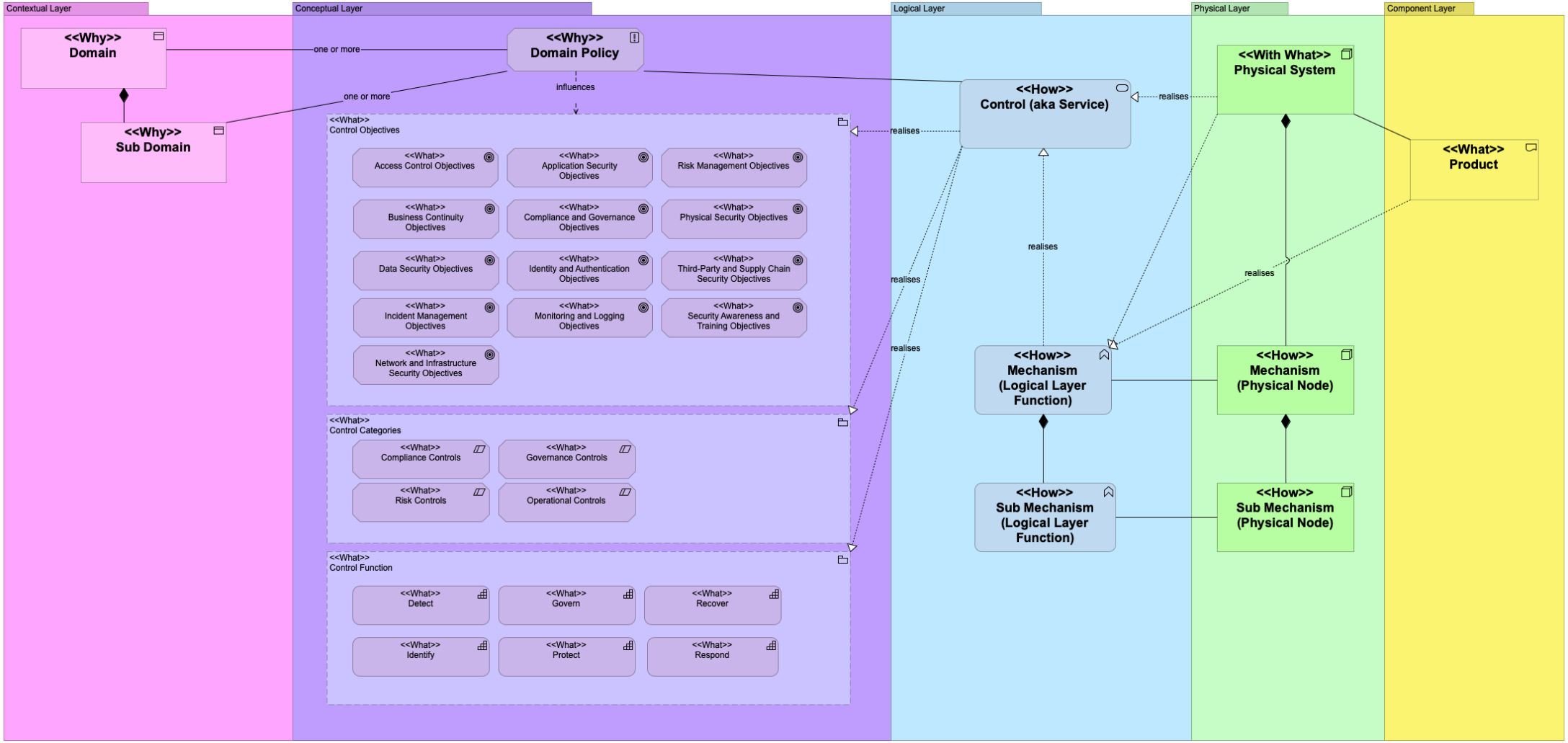
What do I mean when I refer to “relationship-based, not catalogue-based”?

I’m describing a shift in how we conceptualise and organise security services

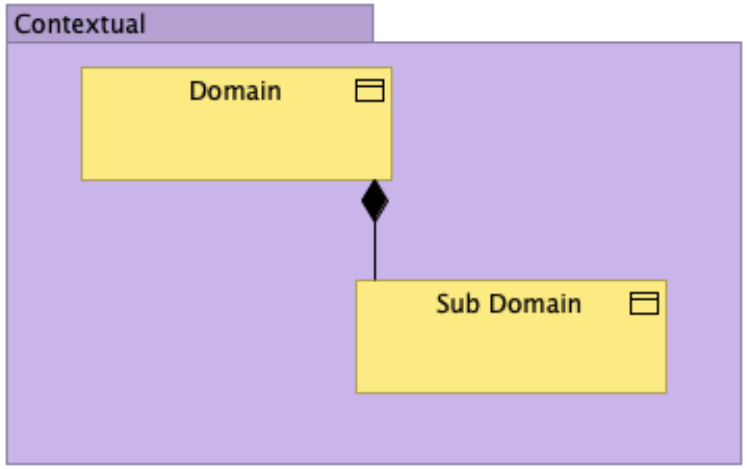
Catalogue vs Relationship Based



A relationship-based approach is preferable because it reflects the dynamic, interconnected nature of modern security services. Unlike static catalogues that are difficult to navigate, lack context, and are hard to maintain, relationship-based models establish a living service network that adapts to organisational needs. They facilitate context-aware definitions, intuitive navigation, and self-maintenance through natural linkages, making them more resilient, scalable, and aligned with how services are actually consumed and delivered. In practice, this means security teams can respond more quickly, reduce complexity, and continuously develop their service model without being hindered by inflexible catalogue structures.



I propose a dynamic, relationship-driven model instead of a monolithic static model



Domain

A Domain defines the broadest scope within the service management architecture. It encompasses an entire area of interest or business concern, providing a high-level view of overarching goals and objectives. A Domain serves as the foundation upon which more specific aspects of the architecture are built, grouping related Sub-Domains and aligning them to strategic requirements.

Key Characteristics

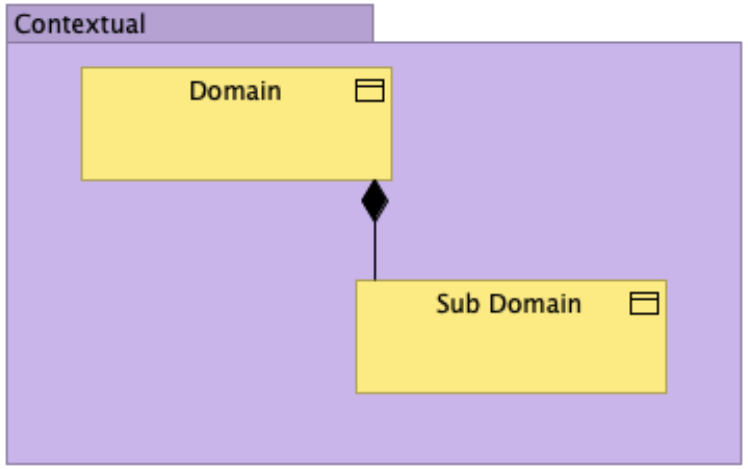
- **Comprehensive Scope:** Spans a major functional area, regulatory domain or business capability.
- **Hierarchical Grouping:** Aggregates multiple Sub-Domains to structure complexity.
- **Strategic Alignment:** Maps directly to high-level business objectives and risk domains.
- **Abstraction Layer:** Presents a consolidated view of related services, controls and mechanisms.

Operational Definition

A Domain acts as the top-level classification unit for organising security services, controls and mechanisms. It provides context for governance, guiding the selection and design of architectural elements by grouping them under a common business-driven category

Also Known As

Architecture Domain (TOGAF / ArchiMate), Service Domain (ITIL / IT4IT), Business Domain (BIZBOK / Business Architecture Guild), Capability Area (ArchiMate Capability Map), Portfolio (SAFe / PMI MoP)



Sub Domain

A Sub-Domain refines a Domain into a focused segment, narrowing the broader concerns into manageable, specialised areas. Each Sub-Domain addresses particular aspects or components of its parent Domain, enabling detailed attention and tailored architectural modelling.

Key Characteristics

- **Targeted Scope:** Isolates distinct facets of the parent Domain for precise control.
- **Detailed Governance:** Facilitates specialised management, monitoring and reporting.
- **Traceability:** Links directly to specific Security Controls and Mechanisms for audit and compliance.
- **Modularity:** Promotes reuse and maintainability by encapsulating related functionality.

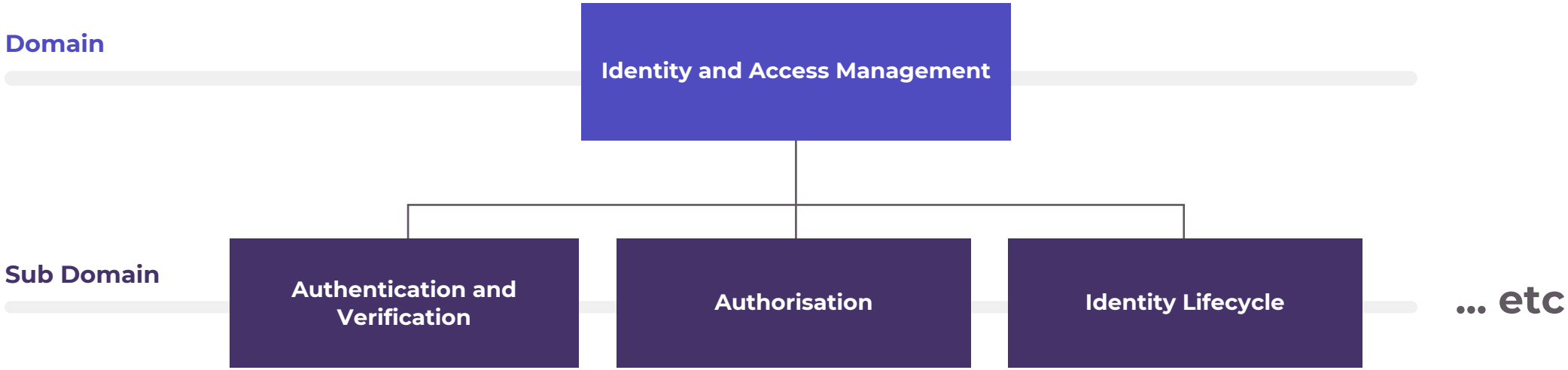
Operational Definition

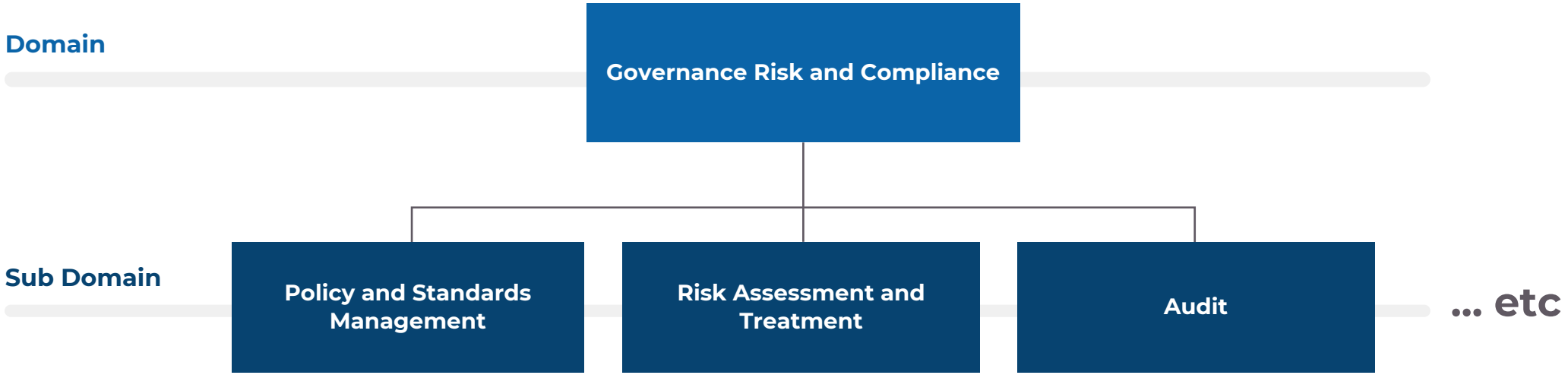
A Sub-Domain serves as an intermediate classification layer, bridging high-level Domains and concrete architectural elements. It guides in decomposing complex business requirements into coherent sets of services, controls and mechanisms that can be implemented and governed effectively

Also Known As

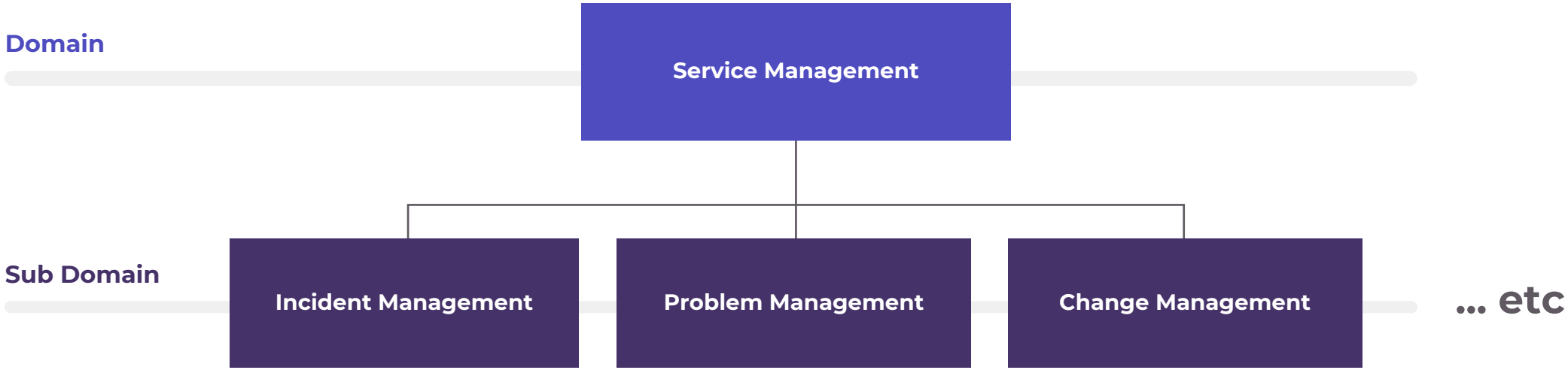
Service Category (ITIL / ServiceNow), Functional Area (Enterprise-Architecture), Capability Cluster (ArchiMate Capability Map), Security Domain (ISO 27002 Control Families), Technology Domain Segment (TOGAF Technology Architecture)

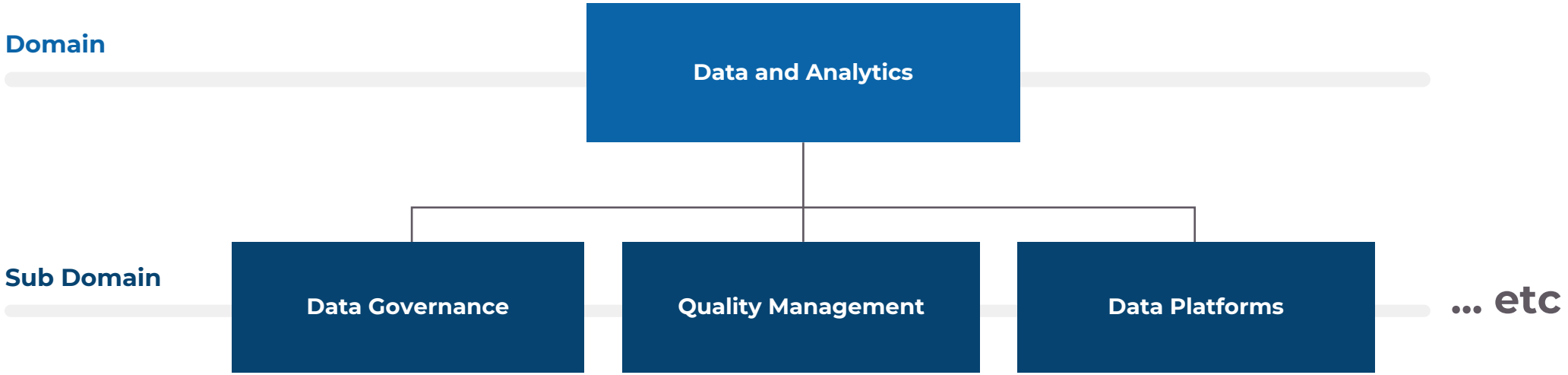
Examples- Security Domains



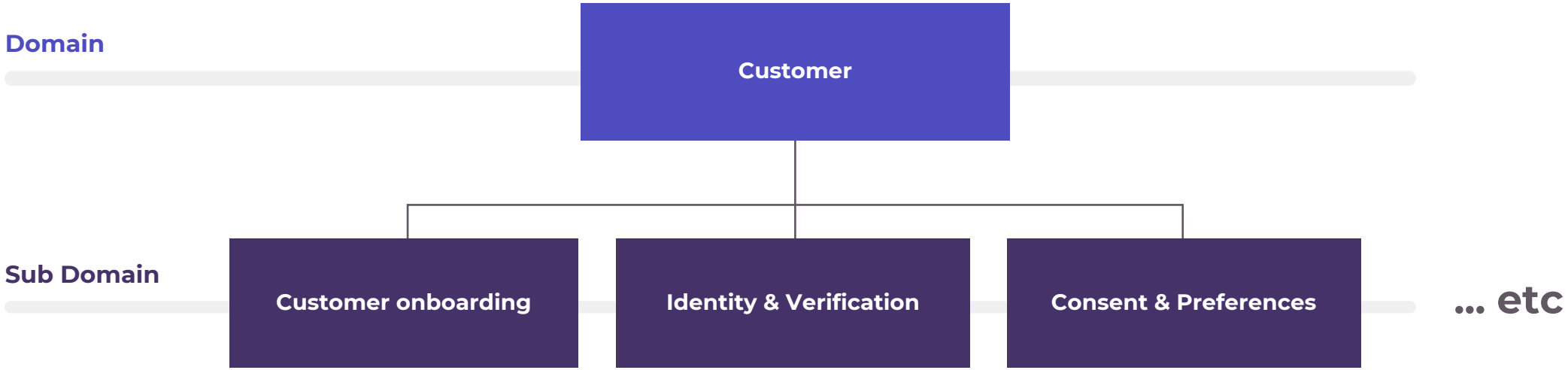


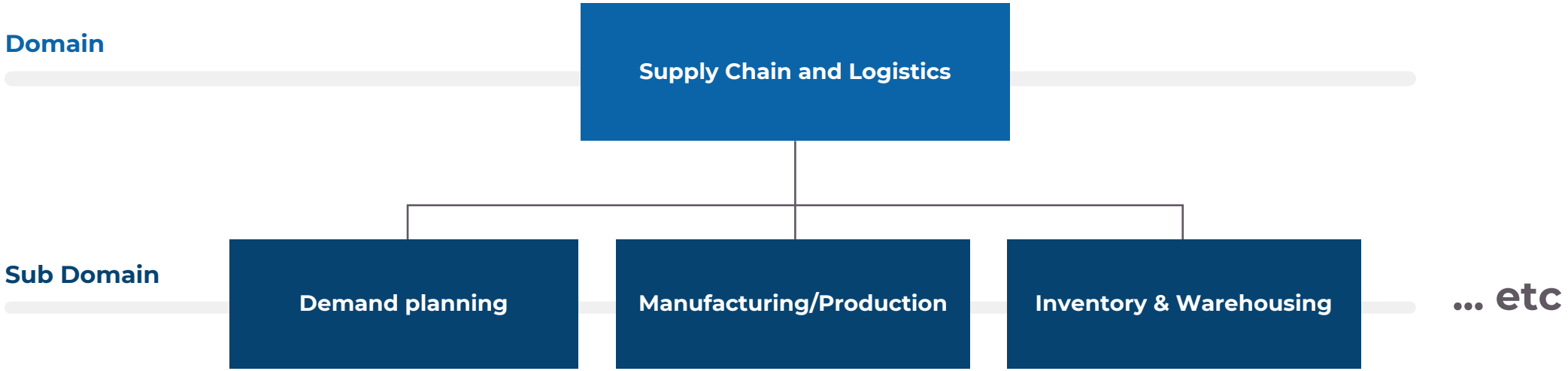
Examples- Technology Domains



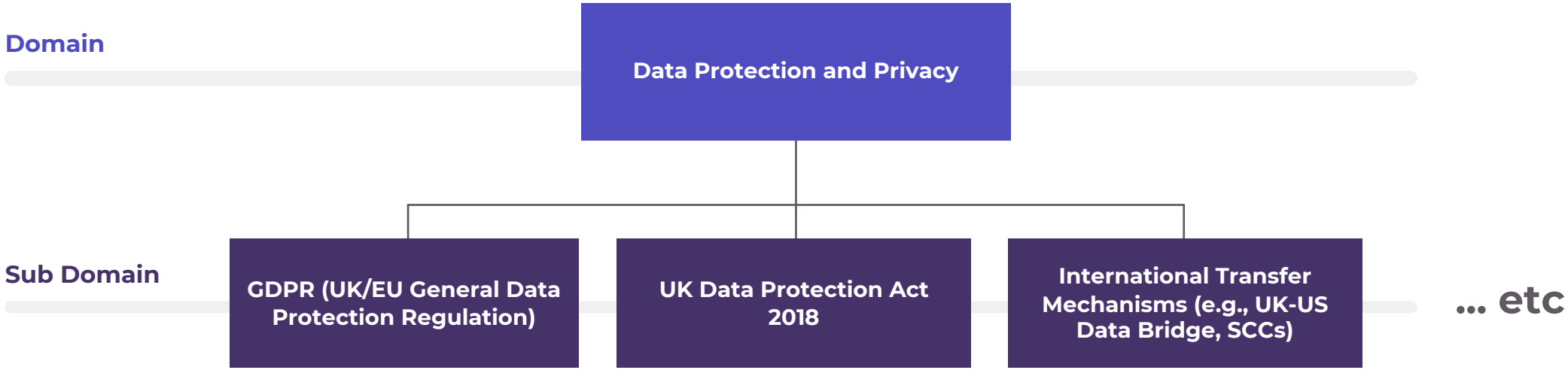


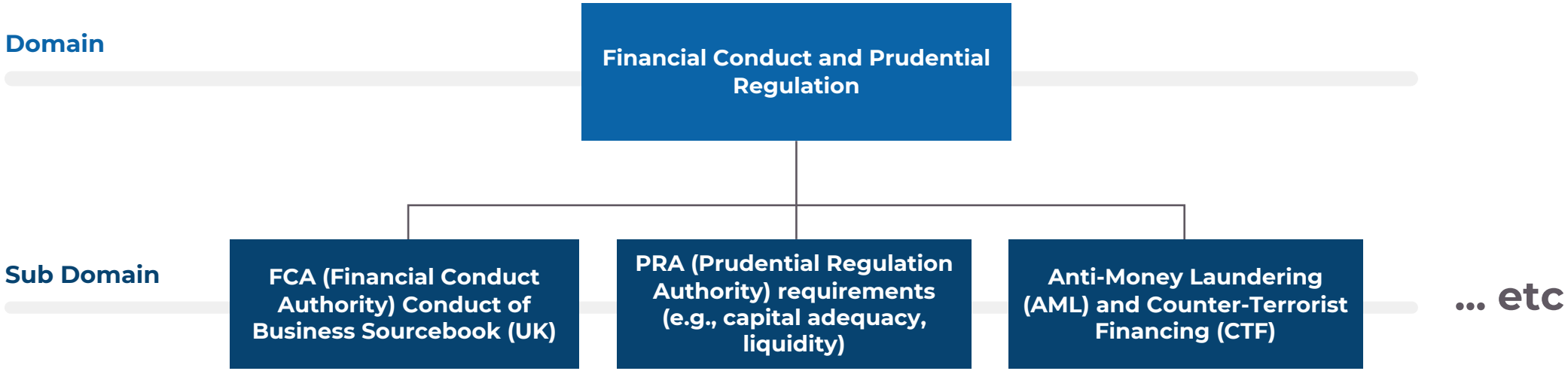
Examples – Business Domains





Examples – Regulatory Domains

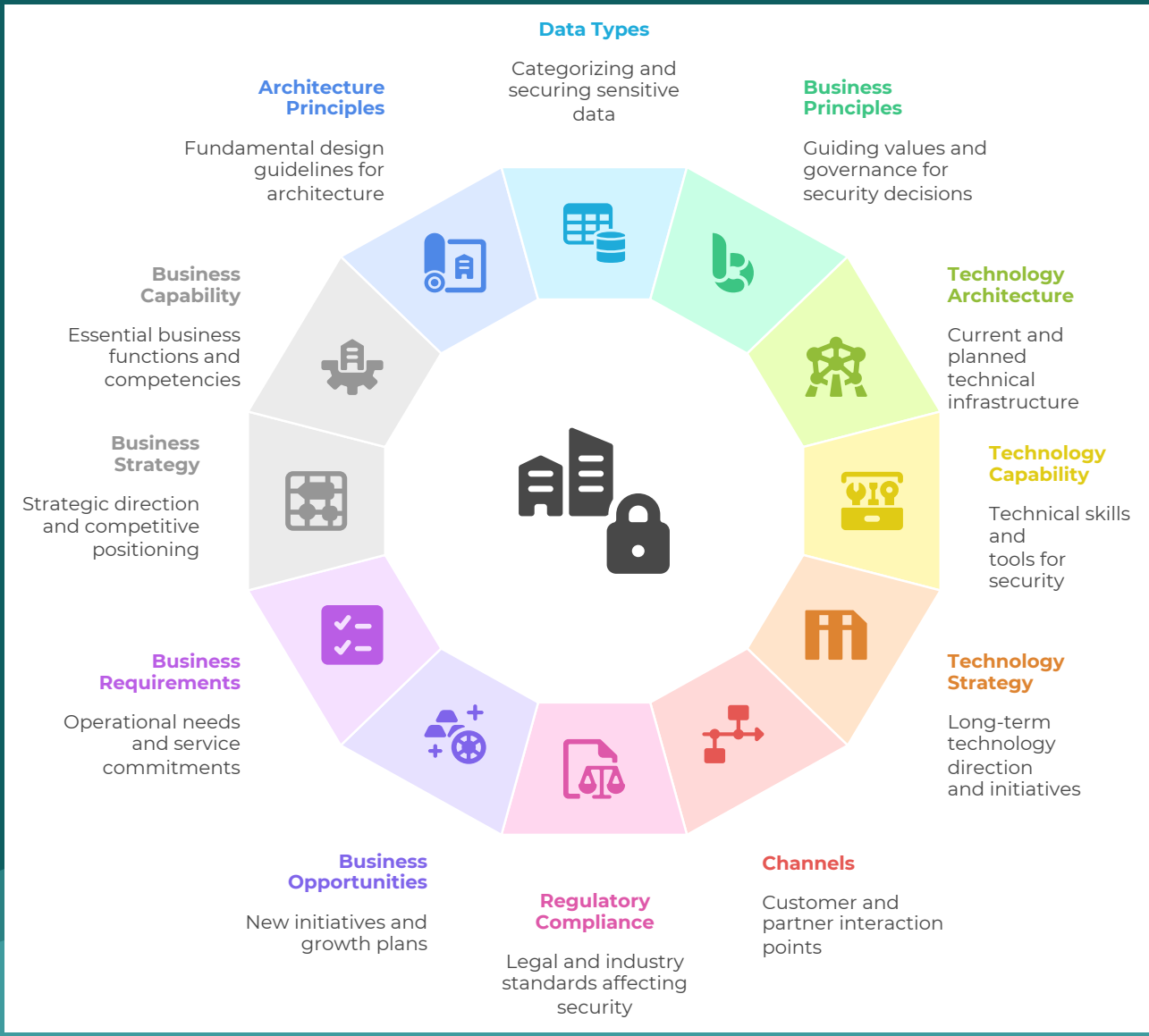




Pro Tip

Applying Context

What Do I need to think about when defining a Domain or Sub Domain



These form the Domain requirements.

Focus	Description	Long Description	Questions to consider
Data Types	Security needs based on the types of data the organisation handles, such as personal, sensitive, or proprietary data.	Understanding the types of data the organisation handles is crucial for implementing appropriate security measures. Different data types have varying levels of sensitivity and legal requirements. Ensuring that personal, sensitive, and proprietary data are adequately protected helps prevent data breaches, ensures compliance with data protection regulations, and maintains the trust of customers and stakeholders.	· What types of data does the organisation handle? · Which data is considered personal, sensitive, or proprietary? · What legal requirements apply to the data we manage? · How should different data types be classified and protected? · Are there specific encryption or access control measures required for certain data types?
Business Principles	Fundamental statements that reflect the organisation's values and guide the overall corporate direction regarding security.	Business principles provide a strategic foundation for security measures by aligning them with the organisation's core values and ethical standards. These principles guide decision-making processes and ensure that security practices support the overall business objectives. Adhering to business principles in security ensures consistency, integrity, and a strong ethical stance, which are essential for maintaining a positive organisational reputation and achieving long-term success.	· What are the fundamental values that guide our organisation? · How do our business principles influence our approach to security? · What ethical standards must our security measures uphold? · How can we ensure that security policies align with our business principles? · How do these principles impact decision-making in security implementations?
Technology Architecture	The structure and organisation of the technology systems within the organisation, including hardware, software, and networks.	Technology architecture defines the framework for the organisation's IT infrastructure. Considering security within this architecture ensures that all technology components are protected against threats and vulnerabilities. A well-secured technology architecture enables seamless integration and operation of systems, reduces the risk of cyber attacks, and supports the organisation's technological and business goals effectively.	· What are the components of our current technology architecture? · How do we secure each layer of our technology stack (hardware, software, network)? · What are the potential vulnerabilities within our architecture? · How do we ensure secure integration of new technologies? · What standards and best practices should we follow for our technology architecture?
Technology Capability	The security needs associated with maintaining and developing the technological capabilities of the organisation.	Maintaining and enhancing technological capabilities requires robust security measures to protect against evolving threats. Ensuring that these capabilities are secure allows the organisation to leverage technology for competitive advantage, operational efficiency, and innovation while safeguarding critical assets and information from potential cyber threats.	· What are our key technological capabilities that need protection? · How do we ensure the security of our development and operational environments? · What measures are in place to protect against technology-specific threats? · How do we maintain and enhance our technology capabilities securely? · What are the security implications of adopting new technologies?
Technology Strategy	Security requirements guided by the overall plan for technology and how it supports business objectives.	A technology strategy outlines the roadmap for technology adoption and utilisation within the organisation. Integrating security requirements into this strategy ensures that all technological initiatives are designed with security in mind, aligning with business objectives and mitigating risks associated with technology implementations and advancements. This proactive approach supports sustainable growth and resilience.	· What is our overall technology strategy, and how does it support business objectives? · How do we integrate security into our technology roadmap? · What are the key security goals within our technology strategy? · How do we align technology investments with security requirements? · How does our technology strategy address emerging threats and vulnerabilities?
Channels	Security requirements that arise from the different distribution and communication channels the business uses.	Different distribution and communication channels present unique security challenges. Ensuring the security of these channels is essential to protect sensitive information, maintain the integrity of communications, and prevent unauthorised access. Secure channels enable reliable and trustworthy interactions with customers, partners, and internal stakeholders, supporting the organisation's operational effectiveness and reputation.	· What distribution and communication channels does our business use? · What security risks are associated with each channel? · How do we protect data transmitted through these channels? · What measures are in place to secure both digital and physical channels? · How do we ensure secure communication with customers, partners, and employees?

Focus	Description	Long Description	Questions to consider
Regulatory Compliance	Requirements derived from legal and regulatory mandates that the organisation must adhere to.	Regulatory compliance is critical for avoiding legal penalties, maintaining market access, and ensuring ethical operations. Adhering to regulatory requirements ensures that the organisation's security measures meet established standards, protecting sensitive data and maintaining trust with regulators, customers, and partners. Compliance also demonstrates the organisation's commitment to responsible business practices.	• What legal and regulatory requirements must we comply with? • How do these regulations impact our security measures? • What steps do we need to take to ensure compliance? • How often do we need to conduct compliance audits? • What are the consequences of non-compliance, and how can we mitigate these risks?
Business Opportunities	Security needs identified through new business opportunities, influencing how these opportunities are pursued.	Identifying and addressing security needs associated with new business opportunities ensures that these ventures are pursued safely and responsibly. This approach helps mitigate risks, protect assets, and support sustainable growth. By considering security early in the exploration of new opportunities, the organisation can innovate and expand while maintaining a strong security posture.	• What new business opportunities are we exploring? • How do these opportunities impact our security posture? • What specific security requirements are needed to support new business ventures? • How do we assess and mitigate risks associated with new opportunities? • What are the potential benefits and security trade-offs of pursuing these opportunities?
Business Requirements	Specific security needs derived from the business strategy and operations.	Business requirements outline the security needs necessary to support the organisation's strategic goals and day-to-day operations. Addressing these requirements ensures that security measures are tailored to the specific needs of the business, enhancing operational efficiency, protecting assets, and supporting overall business success. This alignment ensures that security is an enabler of business objectives rather than a barrier.	• What are the specific security needs derived from our business strategy and operations? • How do these requirements support our overall business objectives? • What are the key business processes that require protection? • How do we ensure that security measures are tailored to our operational needs? • What are the potential security risks associated with our business activities?
Business Strategy	Long-term plans and strategic objectives that determine security priorities and investments.	Integrating security into the business strategy ensures that long-term goals are achieved securely. Strategic objectives guide security priorities and investments, ensuring that resources are allocated effectively to protect against risks and support business growth. This alignment helps build a resilient organisation capable of adapting to changing environments and emerging threats.	• What are our long-term business goals and strategic objectives? • How do these goals influence our security priorities? • What security investments are needed to support our business strategy? • How do we align security initiatives with strategic business plans? • What are the key risks to achieving our strategic objectives, and how can we mitigate them?
Business Capability	Security requirements sourced from the capabilities that the business must maintain or achieve.	Business capabilities represent the competencies and processes critical to the organisation's success. Ensuring these capabilities are secure protects the organisation's core functions and enables it to operate effectively and competitively. Addressing security at the capability level ensures that the organisation can meet its strategic objectives and maintain operational excellence.	• What core capabilities does our business need to maintain or achieve? • How do these capabilities influence our security requirements? • What measures are in place to protect our critical business functions? • How do we ensure that our capabilities are resilient against security threats? • What are the potential vulnerabilities within our business capabilities?
Architecture Principles	Core principles that govern the approach to the enterprise architecture, ensuring that business and IT are aligned for security.	Architecture principles guide the design and implementation of the enterprise architecture, ensuring that business and IT strategies are aligned and secure. These principles ensure that security considerations are integrated into all architectural decisions, supporting a cohesive and secure organisational framework that enables efficient and effective operations.	• What are the core principles guiding our enterprise architecture? • How do we ensure that security is integrated into our architectural decisions? • What alignment is needed between business and IT for security? • How do these principles influence our approach to system design and development? • What are the potential security risks in our architectural framework?

Pro Tip

The Domain is the cornerstone of a comprehensive and relevant Services Catalogue. Understanding the Business is crucial in establishing that cornerstone.

Business motivations are fundamental to developing security measures that align with the organisation’s core values, strategic goals, and operational needs. These drivers ensure that security measures are not only compliant with regulations but also support the organisation’s mission and long-term success. By integrating security into business principles, strategies, and capabilities, the organisation can protect its assets, reputation, and continuity against a wide range of threats, thereby enabling a secure and resilient business environment.

Note : This is not the entire Value Stream.

Identity and Access Management

Example Value Stream representing the Domain

Identity Lifecycle Management

Covers the end-to-end processes of identity creation, modification, and deletion for human and non-human actors (e.g., employees, contractors, service accounts, APIs, bots). Encompasses onboarding, transfers, offboarding, access provisioning, deprovisioning, and periodic access reviews. This sub-domain maintains the integrity of identity data, ensures timely changes in response to business events, and supports regulatory requirements for user lifecycle management.

Identity Provisioning Service

Automates and enforces standardised creation of new identities and initial access rights consistent with business rules, HR triggers, and role profiles.

Access Certification Service

Orchestrates regular access reviews, requiring business/IT owners to attest to the correctness of assigned access rights and automating revocation workflows for violations.

Identity Deprovisioning Service

Ensures prompt and complete removal or disabling of identities and associated access on termination or system change events.

Identity Data Synchronization Service

Maintains consistency and accuracy of identity attributes across all connected systems, reconciling authoritative sources and downstream directories.

Do you need to go to the next level?

Note : This is not the entire Value Stream.

Human Resources

Example Value Stream representing the Domain

Employee Lifecycle Management

This foundational sub-domain manages the comprehensive journey from talent attraction through employee separation, ensuring consistent security controls and employee experience delivery throughout all transitional milestones. Key services include automated recruitment and selection processes, structured onboarding programmes, continuous performance management aligned to business objectives, and secure employee separation procedures that maintain compliance obligations

Workforce Data Governance

Establishing comprehensive governance over employee data assets, this sub-domain ensures regulatory compliance, data protection, and authorised access across all HR systems. Critical services encompass data classification and protection mechanisms, GDPR compliance management including data subject rights fulfilment, governance of HR analytics ensuring ethical use of employee data, and data retention and disposal aligned to legal and business requirements

HR Service Delivery

Providing structured, multi-tiered service models that balance employee accessibility with operational efficiency, this sub-domain implements shared service centres, business partner consultancy, and self-service capabilities. Core services include employee self-service portals for routine transactions, centralised HR service desks with defined service levels, strategic HR business partner support for complex organisational needs, and shared services centres for transactional operations

People Risk Management

Focusing on workforce-related security risks including insider threats, compliance violations, and reputational risks, this sub-domain implements proactive risk identification and mitigation controls throughout the employee lifecycle. Essential services encompass comprehensive background verification aligned to role risk levels, insider threat detection respecting privacy rights, structured incident response for employment-related security matters, and workforce risk assessment supporting strategic planning

WS1: Define Your Domains

Workshop Activity

1. In small groups, select your domain and define its purpose.
2. Draft the high-level value stream on a whiteboard or flipchart.
3. Decompose each stage into sub-domains and detail key elements.
4. Share back for group feedback and alignment.

Map the Domain and Sub Domains

From your Domain identify the activities within that Domain – these become the sub domains

- Do you need to go a level deeper?

Pick and Define

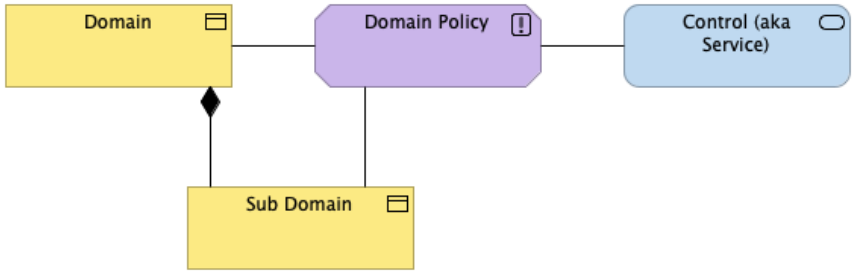
Pick one domain and write its purpose in one sentence.

- Use the Business Context slides as a prompt to consider the business context and then identify the key activities that make up that domain.

Choose whether your Domain is;

- Business Capability focused
- Technology Capability focused
- Security Capability focused
- Regulatory focused
- Some other focus

I would like each group to choose a different focus in order to test the logic.



Domain Policy

A Domain Policy specifies the authoritative set of security principles, rules and governance directives for a defined Domain. It translates high-level business objectives and risk appetites into a cohesive policy that applies uniformly across all Sub-Domains, Controls and Mechanisms governed by that Domain.

Key Characteristics

- **Conceptual Governance:** Defines what must be enforced before any logical or physical design is undertaken
- **Scope-Constrained:** Applies to a specific Domain and all its constituent Sub-Domains
- **Rule-Based:** Captures mandatory requirements (e.g. data classification levels, authentication standards, compliance mandates)
- **Traceable:** Mapped bidirectionally to business drivers (Contextual Layer) and to Controls/Mechanisms (Logical & Physical Layers)

Operational Definition

A Domain Policy is a self-contained governance artefact that, when invoked, guides the consistent application of security requirements across its Domain. It is realised by Security Controls and Mechanisms at lower layers, ensuring all architectural elements comply with the defined mandates and performance criteria.

Also Known As

Security Policy (ISO/IEC 27001), Policy Set (OASIS XACML / Zero-Trust Frameworks), Control Objective (COBIT / ISACA), Domain Standard (NIST / CIS Benchmarks), Architecture Principle (TOGAF)

,

Data Protection and Privacy (example)

Policy 1	Policy 2	Policy 3	Policy 4
All personal and sensitive data must be classified and processed in line with GDPR and the UK Data Protection Act 2018.	All personal data must have a clearly documented lawful basis for collection, processing, and retention.	International transfers of personal data must use approved safeguards (e.g., SCCs, UK–US Data Bridge) with risk assessments maintained.	Data subjects' rights (access, rectification, erasure, portability) must be supported and fulfilled within statutory timelines.
Driver: Legal compliance, customer trust	**Driver**: Transparency, accountability	**Driver**: Global business enablement, lawful operations	**Driver**: Customer empowerment, regulatory compliance
Data Classification and Handling	**Lawful Basis for Processing**	**Cross-Border Transfers**	**Data Subject Rights**
Risk Mitigated: Data breaches, regulatory fines	**Risk Mitigated:** Unlawful processing, reputational damage	**Risk Mitigated:** Invalid transfers, loss of compliance certifications	**Risk Mitigated**: Complaints, legal challenges, fines

Top Tips

Keep Policies Principle-Based, Not Technical

Policies should set rules or expectations, not implementation details.

Link Every Policy to a Business Driver

If you can't explain why the business cares, it's probably not a policy.

Drivers are often: compliance, trust, resilience, efficiency, transparency.

Make Them Risk-Responsive

Policies should explicitly reduce a risk.

A quick check: "If this policy didn't exist, what could go wrong?"

Be Clear, Concise, and Enforceable

Use direct language: "must," "shall," "will."

Avoid vague statements like "should be considered" or "where appropriate."

Scope Them to the Domain

Don't drift into enterprise-wide catch-alls — stay in the lane of the domain.

E.g., in Data & Analytics: "All data must have an owner" is valid; "All suppliers must sign NDAs" belongs elsewhere.

Service Management (example)

Policy 1	Policy 2	Policy 3	Policy 4
All incidents must be logged, categorised, and prioritised within agreed SLAs, with escalation paths clearly defined.	Major incidents must undergo problem management with root cause analysis completed and preventative actions tracked to closure.	All changes to production systems must follow a formal change management process with risk assessment and approval before implementation.	Critical services must maintain defined recovery time (RTO) and recovery point objectives (RPO), tested at least annually.
Driver: Operational resilience, customer satisfaction	**Driver**: Continuous improvement, service stability	**Driver**: Compliance, stability of critical services	**Driver**: Business continuity, resilience commitments
Incident Response	**Root Cause Analysis**	**Change Approval**	**Service Availability**
Risk Mitigated: Extended outages, loss of service trust	**Risk Mitigated:** Repeat failures, unmanaged technical debt	**Risk Mitigated:** Service disruption from unauthorised or untested changes	**Risk Mitigated**: Inability to recover from outages

Top Tips

Keep Policies Principle-Based, Not Technical

Policies should set rules or expectations, not implementation details.

Link Every Policy to a Business Driver

If you can't explain why the business cares, it's probably not a policy.

Drivers are often: compliance, trust, resilience, efficiency, transparency.

Make Them Risk-Responsive

Policies should explicitly reduce a risk.

A quick check: "If this policy didn't exist, what could go wrong?"

Be Clear, Concise, and Enforceable

Use direct language: "must," "shall," "will."

Avoid vague statements like "should be considered" or "where appropriate."

Scope Them to the Domain

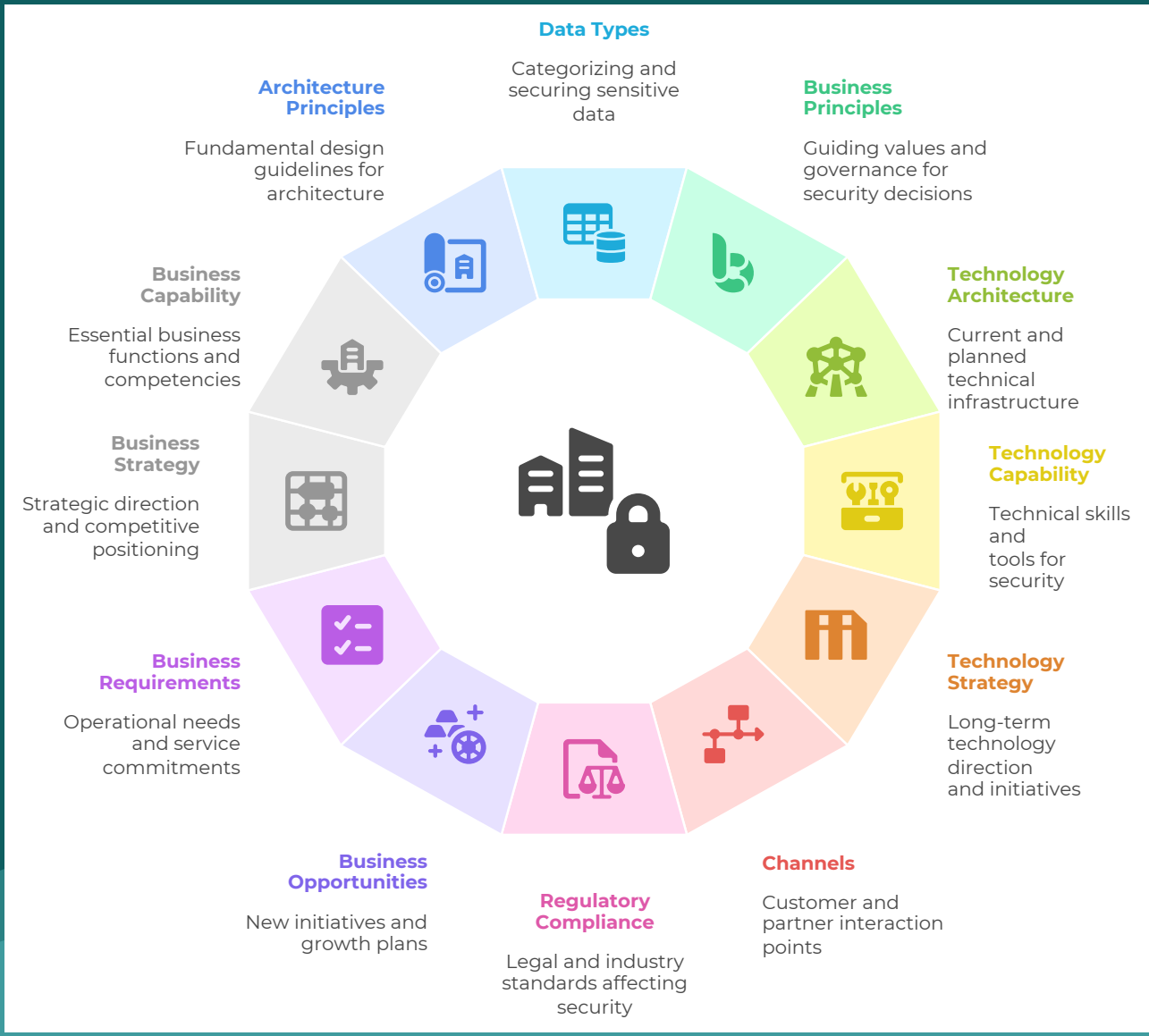
Don't drift into enterprise-wide catch-alls — stay in the lane of the domain.

E.g., in Data & Analytics: "All data must have an owner" is valid; "All suppliers must sign NDAs" belongs elsewhere.

Pro Tip

Applying Context

What Do I need to think about when defining a Domain or Sub Domain



These form the Domain requirements.

WS2: Define Your Domains Policies

Workshop Activity

1. In small groups, using your domain define a set of policy statements.
2. Draft the policies for domains and sub-domains.
3. Share back for group feedback and alignment.

Step One

Start With Business Drivers and Obligations

Ask: "What does the business need from this domain?"

- Compliance requirements (e.g. GDPR, FCA, ISO 27001).
- Strategic goals (trust, resilience, cost optimisation).
- Risk appetite (e.g. zero tolerance for unauthorised access).

These define the why behind the policy.

Step Two

Map to Domain Scope

Check your domain definition and sub-domains.

- Policies must directly govern those areas — nothing outside.

Example: Service Management Domain → policies should govern incident/problem/change management, not HR policies.

Step Three

Identify Key Risks and Dependencies

Ask: "What could go wrong in this domain if left unmanaged?"

- In Data & Analytics: poor data quality, unauthorised access, biased models.
- In Service Management: uncontrolled changes, recurring incidents, missed SLAs.

Each risk points to a potential policy.

Step Four

Look for Non-Negotiables

Policies should capture rules that always apply — not "nice to haves."

- If a rule can be waived casually, it's probably a guideline, not a policy.

Example: "All incidents must be logged" (policy) vs. "Log incidents where practical" (guideline).

Step Five

Balance Between Too Broad and Too Detailed

Too broad: "We must manage data properly" → unhelpful.
Too detailed: "Use SQL stored procedures to cleanse data" → too technical.
Right level: "All data must have an identified owner and steward responsible for quality and access decisions."

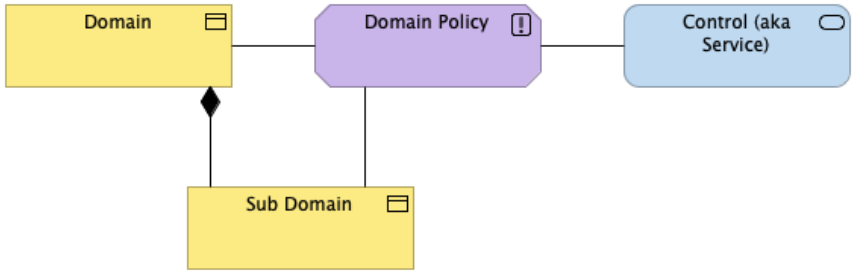
Step Six

Test with Three Questions

For each draft policy, ask:

1. Does it tie back to a business driver or obligation?
2. Does it mitigate a clear risk in the domain?
3. Can it be enforced and measured consistently?

If you can answer yes to all three, it's a good candidate.



Control (Service)

A Control (Service) is a logical security service, defined at the logical layer of the SABSA architecture, that delivers specific functionality to satisfy business-driven security requirements. Each Control Service operates on information, not raw data, and abstracts from implementation details to provide a consistent and reusable service interface. It is fully traceable to business attributes and forms part of the chain of accountability from business drivers to technical implementation.

Key Characteristics

- **Logical Abstraction:** Specifies what security capability is required, independent of how it is implemented.
- **Service Interface:** Exposes defined inputs, outputs and performance criteria through a clear service contract.
- **Business Traceability:** Maps directly to business attributes and strategic objectives, ensuring alignment with governance, risk management and compliance needs.
- **Self-Contained:** Encapsulates all necessary functional logic, allowing controls to be reused across multiple solutions without modification.
- **Information-Centric:** Acts on and manipulates structured information, preserving the integrity and confidentiality of business data flows.

Operational Definition

A Security Control is a self-contained logical service unit that, when invoked, orchestrates the required security processes. It receives information inputs, applies business-driven security logic, and produces information outputs in accordance with its service level agreement, while remaining agnostic of the physical hosts or technologies that ultimately execute its functions.

Also Known As

Logical Control Service (SABSA), Security Service (ISO 27001, NIST CSF), Control Objective Implementation (COBIT), Capability Service (ArchiMate / IT4IT),

Translate Policies into Services/Controls (Logical Layer)

Each Domain Policy implies a set of services (logical security capabilities) that enforce it!

Purpose: Define the logical services that deliver the control functions required to make policies enforceable.

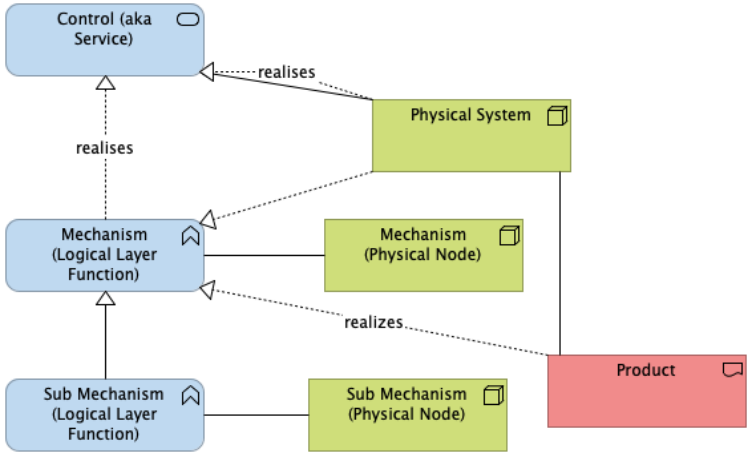
Domain	Policy	Service (Control)
Service Management	All incidents must be logged and categorised within SLA.	Incident Management Service (control for intake, categorisation, escalation).
Service Management	All production changes must follow a formal approval process.	Change Management Service (workflow, risk assessment, CAB integration).
Data & Analytics	All data must have an identified owner and steward.	Data Governance Service (control for metadata, stewardship roles, accountability).
Data & Analytics	Data must meet defined quality metrics.	Data Quality Monitoring Service (profiling, validation, remediation workflow).
Data Protection	International transfers must use approved safeguards.	Cross-Border Data Transfer Control Service (enforces SCCs, logs transfers).

WS3: Define Your Services

Workshop Activity

1. In small groups, using your domain policies define a set of services.
2. Pick one Domain Policy and run with that.
3. Identify one or more services which reflect the intent of the policy.
4. Share back for group feedback and alignment.

- **Domain Policies** → mapped to one or more **Security Services**.
- Shared understanding of how logical controls operationalise policies.



Logical Mechanism

A Mechanism, as a Logical Function, defines the logical process or workflow required to implement one or more Security Controls (services). It specifies the sequence of tasks, decision points, and information transformations necessary to deliver the control's capabilities, acting at the logical layer independent of physical hosts.

Key Characteristics

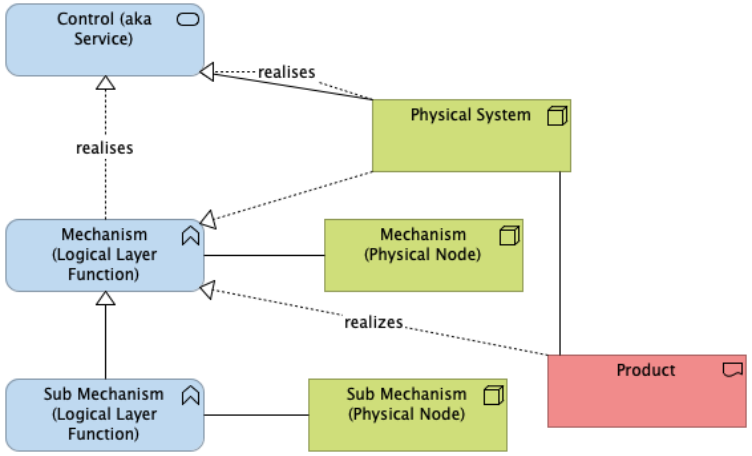
- **Process-oriented:** Captures the end-to-end workflow, including branching logic and information handling.
- **Technology-agnostic:** Specifies only what must occur, not how or where it is executed.
- **Modular:** Can be decomposed into Sub-Mechanisms for granular control.
- **Reusable:** Standardised functions that can realise multiple controls or services.

Operational Definition

A Mechanism is a self-contained logical component with well-defined inputs, outputs, and performance criteria. Invoked by the control's service interface, it orchestrates process flows that downstream physical nodes will execute.

Also Known As

Security Process Function (SABSA Logical Layer), Logical Workflow (TOGAF / ArchiMate), Control Realisation Function (COBIT / ISACA), Implementation Process (NIST SP 800-53 / NIST CSF), Process Activity (ISO/IEC 27001 / CIS Controls), Service Process Function (ITIL / Service Modelling), Logical Execution Flow (IT4IT / Architecture Modelling)



Logical Sub Mechanism

A Sub-Mechanism, as a Logical Layer Function, is a finer-grained logical component of a broader Mechanism. It encapsulates a specific subset of the workflow—such as approval checks, data sanitisation, or audit log formatting—operating at the logical layer to realise part of a control.

Key Characteristics

- **Granular:** Defines a single, focused process element within a larger workflow.
- **Defined Interfaces:** Has explicit inputs, outputs, and success criteria.
- **Composable:** Can be combined or reordered within the parent mechanism.
- **Traceable:** Mapped back to specific control requirements for audit and testing.

Operational Definition

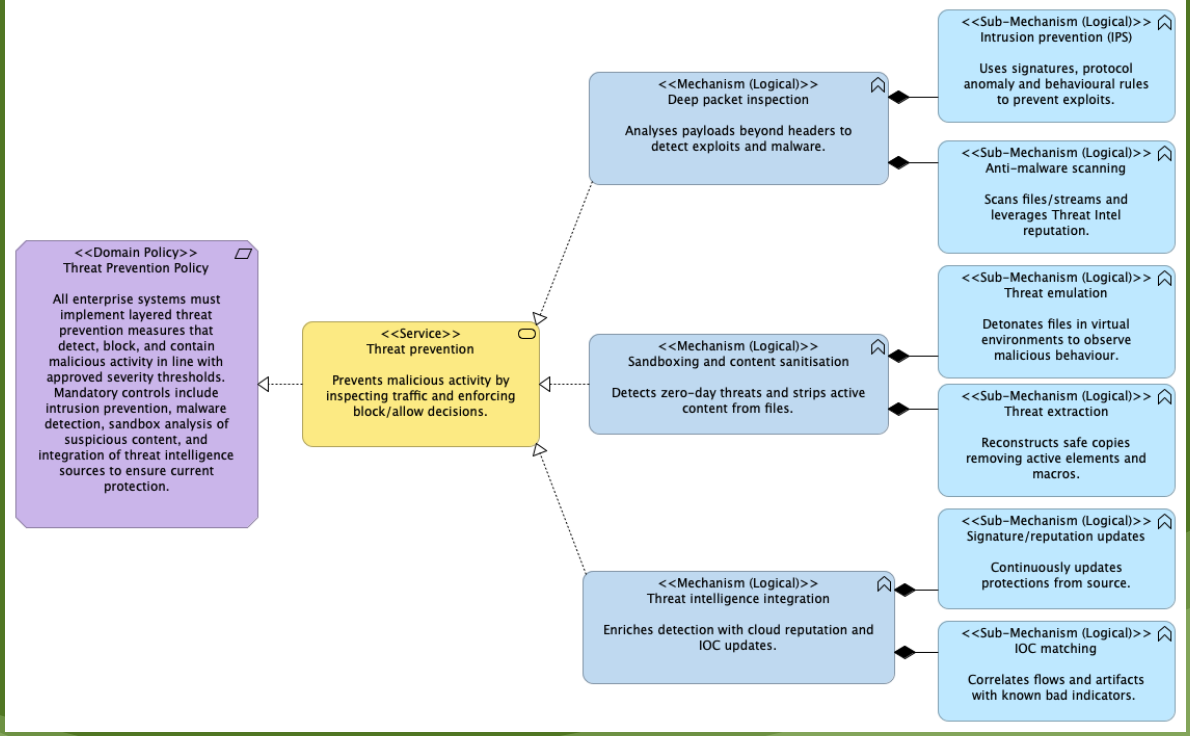
A Sub-Mechanism is a self-contained logical function invoked by the parent mechanism. It organises a discrete set of decision points or information transformations that contribute to the overall security process.

Also Known As

Logical Task Element (SABSA), Process Step Function (TOGAF / ArchiMate), Control Sub-Function (COBIT / ISACA), Implementation Activity (NIST SP 800-53 / NIST CSF), Configuration Item Activity (ITIL / CMDB practice),Technical Control Step (ISO/IEC 27001 / CIS Controls), Logical Node Sub-Process (IT4IT / Service Modelling)

Example : Security Technology

Logical Mechanisms and Sub Mechanisms



Rule of Thumb for definition

+ Keep mechanisms technology-agnostic (describe what must be done, not how).
+ Sub-mechanisms should be single-purpose and reusable.
+ If a logical piece has independent failure modes, monitoring needs, or scaling characteristics, model it as a sub-mechanism.
+ Don’t over-decompose: stop when decomposition no longer adds clarity or testability.
+ Prefer deterministic I/O: every mechanism should have defined inputs, outputs and success/failure states.

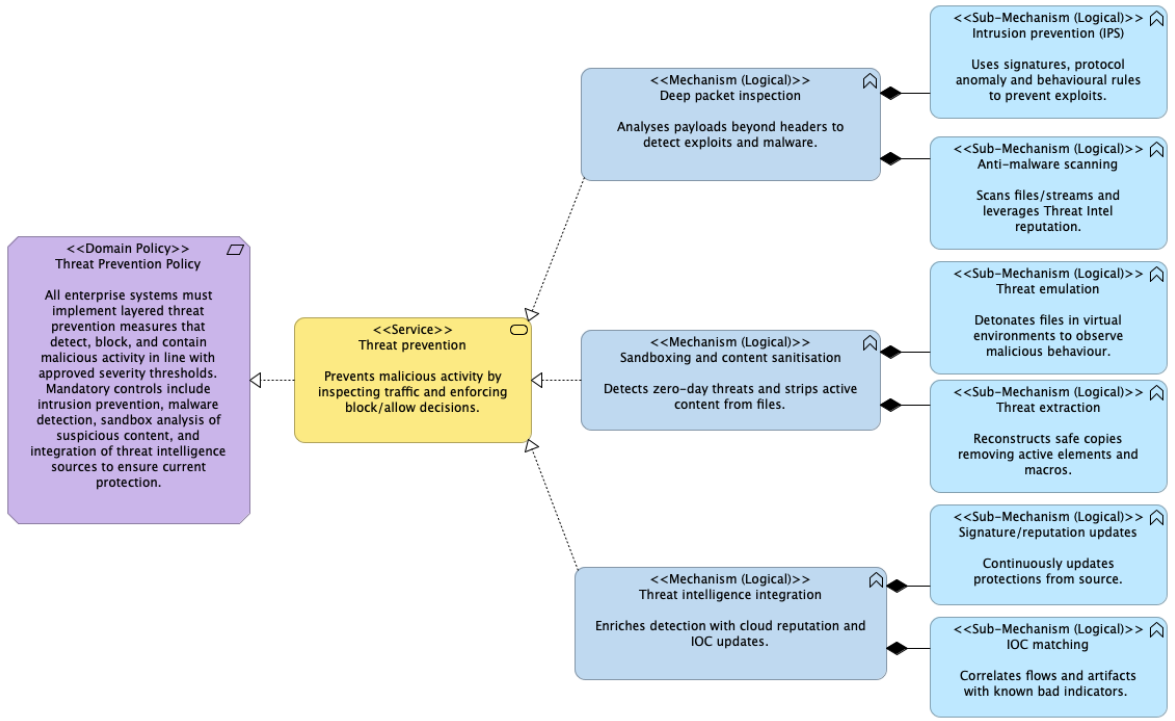
What details do I need to capture?

Logical Mechanisms and Sub-Mechanisms are where things start to transition from concept to the physical world.

The services are logical and extremely useful in high-level discussions, but it is here that the design becomes useful to the developers and engineers.

Modelling tools make this work easier.

1. ID / Name
2. Short purpose (one sentence)
3. Inputs (data/events with format)
4. Outputs (data/events with format)
5. Pre-conditions (what must be present)
6. Post-conditions / Success criteria (measurable)
7. Policy / Control mapping (policy IDs, ISO/NIST control references)
8. Non-functional requirements (latency, throughput, resilience, data residency)
9. Dependencies (other mechanisms, services, external feeds)
10. Ownership (team / role)
11. Audit evidence (logs, test reports, alerts)
12. Test cases (positive/negative; measurement thresholds)
13. Suggested physical node types (e.g. network sensor, sandbox cluster, cloud API)



WS4: Identify Your Logical Mechanisms and Sub Mechanisms

Workshop Activity

1. In small groups, using your selected Service.
2. Identify the Logical Mechanisms and Sub Mechanisms.
3. Share back for group feedback and alignment.

Define the Mechanism

Ask: “What logical process or workflow delivers this service?”

- Write down one Mechanism that represents the end-to-end logical flow.
- Give it a name (e.g., Incident Logging & Categorisation Workflow).
- Define its inputs/outputs (what it takes in, what it produces).
- Clarify the success criteria (what does ‘done’ look like?).

Break into Sub-Mechanisms

- Decompose the Mechanism into smaller, reusable steps.
- Capture 2–3 Sub-Mechanisms that handle specific parts of the workflow.

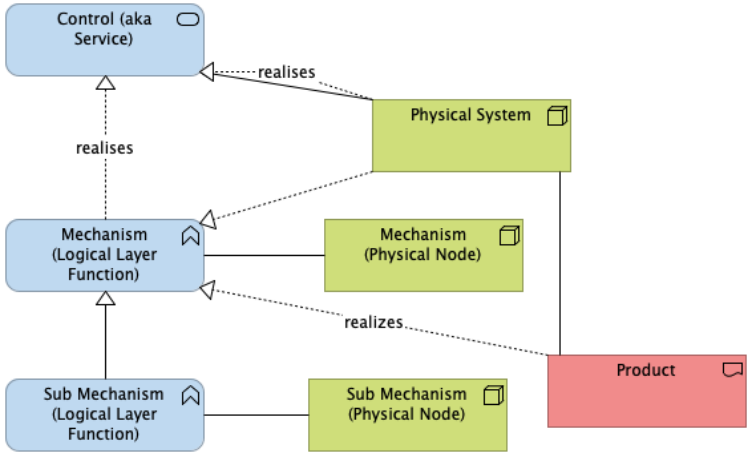
Examples: Log Intake Validation, Priority Assignment, Escalation Trigger.

Ensure each has:

- A clear purpose (single-function, reusable).
- Defined inputs/outputs.
- Traceability back to the Service & Policy.

Output

- A simple **Service → Mechanism → Sub-Mechanism** breakdown, showing how logical workflows deliver policy intent.
- A common understanding of when to stop decomposing (don’t over-complicate, but ensure testable steps).



Physical Mechanism

A Security Mechanism, as a Node, represents the concrete execution environment—servers, network devices, software modules, or human-run procedures—that realises the logical workflow defined by the Application Function. It embodies the physical instantiation of a mechanism, acting on data at the SABSA physical layer.

Key Characteristics

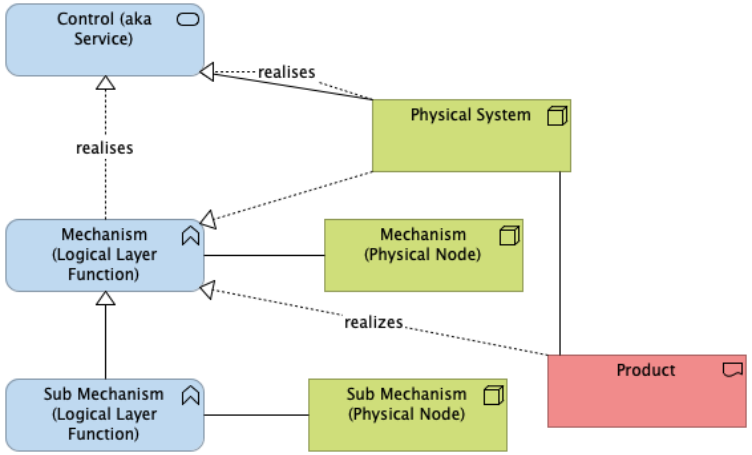
- **Execution Environment:** Hosts software, hardware, or procedural resources.
- **Data-Centric:** Operates on and transforms data to fulfil the logical mechanism's tasks.
- **Implementation-Specific:** Varies by technology choice and operational context.
- **Multi-Hosting:** A single Node may execute multiple mechanisms or sub-mechanisms.

Operational Definition

A Security Mechanism is a tangible resource or procedure that carries out the steps of the logical mechanism, processing data through encryption, validation, logging, or other technical means.

Also Known As

Physical Security Node (SABSA), Technology Component (TOGAF / ArchiMate), Configuration Item (ITIL / CMDB), Security Component (NIST CSF / NIST SP 800-53), Implementation Mechanism (COBIT / ISACA), Technical Control (ISO/IEC 27001 / CIS Controls), Resource Node (IT4IT / Service Modelling), Operational Technology Component (ISA/IEC 62443)



Physical Sub Mechanism

A Sub-Mechanism as a Node is the physical or procedural component that executes the logical sub-process defined by its Application Function. Examples include a specific encryption library, a microservice container or a manual approval desk handling review tasks.

Key Characteristics

- **Focused Functionality:** Executes a narrow, well-defined technical task.
- **Component-Level Execution:** Exists as part of a broader host environment.
- **Composable:** Multiple sub-mechanisms combine to fulfil a complete mechanism.
- **Technology-Bound:** Defined by the particular hardware, software, or procedural technology chosen.

Operational Definition

A Physical Sub-Mechanism is the lowest-level execution element. It performs a discrete technical action—such as applying a cryptographic algorithm, transforming a data field, or generating a system alert—that contributes directly to the parent mechanism's outcome.

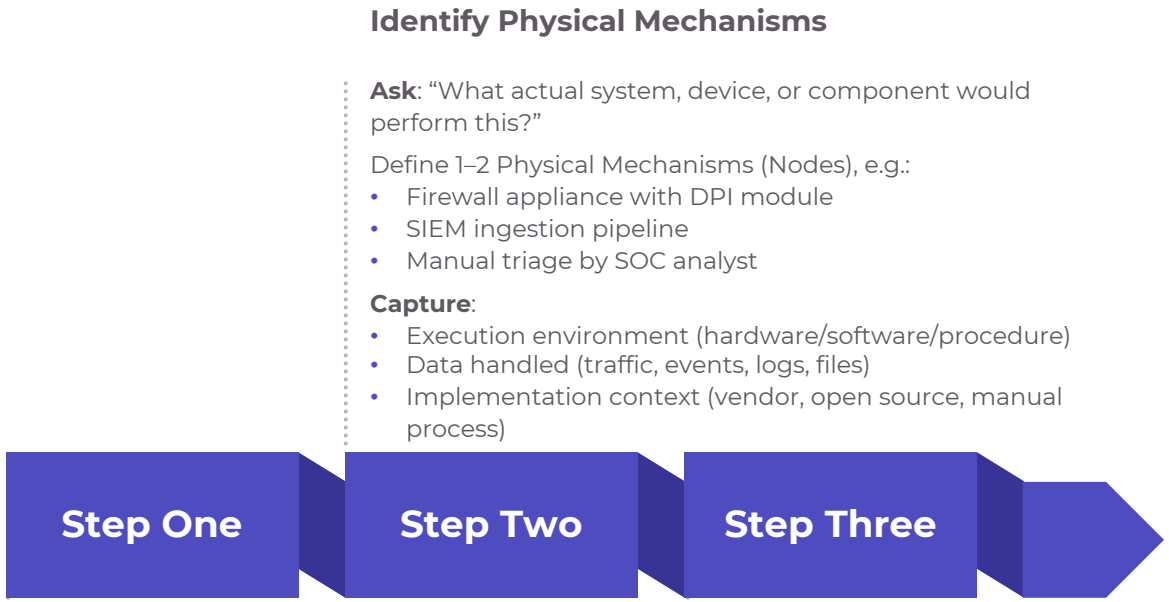
Also Known As

Physical Component Function (TOGAF / ArchiMate), Control Execution Step (COBIT / ISACA), Implementation Step (NIST SP 800-53 / NIST CSF), Configuration Item Activity (ITIL / CMDB practice), Technical Control Element (ISO/IEC 27001 / CIS Controls), Node Sub-Process (IT4IT / Service Modelling), Procedural Sub-Task (ISA/IEC 62443 for OT contexts)

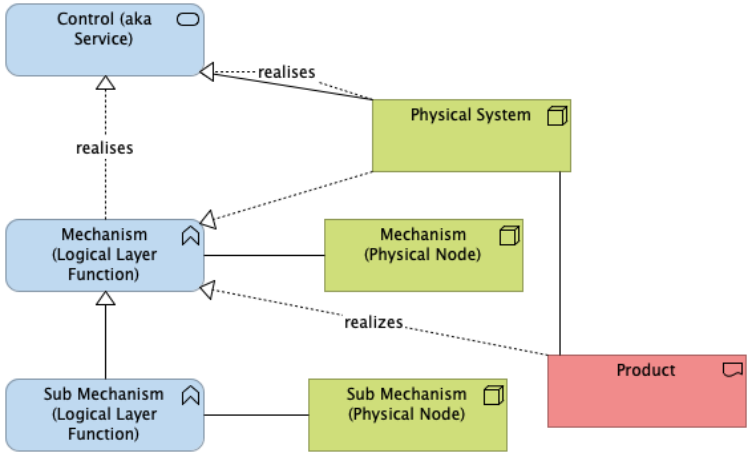
WS5: Define Your Physical Mechanisms and Sub Mechanisms

Workshop Activity

1. In small groups, select a Logical Mechanism.
2. Ask what is going to deliver this in practical terms.
3. Map the physical system to the mechanism.
4. Share back for group feedback and alignment.



- A mapping from Logical Mechanism → Physical Mechanism(s)/Nodes.
- Examples of concrete environments (devices, software, procedures).
- A clearer view of where accountability and implementation dependencies sit.



Physical System

The Physical System represents tangible components including hardware, software, infrastructure, and procedural elements that implement Security Mechanisms at the physical layer of the SABSA architecture framework. These systems enable the practical execution of security objectives by providing the concrete implementation foundation that supports Security Controls (Services) operating at the logical layer.

Key Characteristics

- **Mechanism Implementation:** Physical Systems host and execute the security mechanisms that deliver the functionality specified by Security Controls at the logical layer
- **Data Processing:** Unlike Security Controls which act on information, Physical Systems operate on and manipulate data through technological processes and human procedures
- **Tangible Infrastructure:** Encompasses servers, networks, applications, databases, physical facilities, and the human actors who carry out security procedures
- **Implementation Agnostic:** The same Security Control may be supported by different Physical System configurations depending on enterprise requirements, technology choices, and operational constraints

---

Operational Definition

Physical Systems provide the technological and procedural infrastructure necessary to transform logical security requirements into operational security capabilities. They represent the “how” of security implementation, whilst Security Controls define the “what” of security functionality required by the business.

Also Known As

Technology Component (TOGAF / ArchiMate), Configuration Item (ITIL), Asset (ISO/IEC 27001), Implementation Mechanism (COBIT), System Component (NIST CSF / NIST SP 800-53), Resource Node (IT4IT), Operational Technology Asset (ISA/IEC 62443)

WS6: From Physical Mechanisms to Physical Systems

Workshop Activity

1. In small groups, select a Physical Mechanism.
2. Ask yourself what is the mechanism going to run on.
3. Map the physical system to the mechanism.
4. Share back for group feedback and alignment.

Identify Physical System

Ask: "What concrete infrastructure or resource actually runs this?"

Define 1–2 Physical Systems that host or support the mechanism, e.g.:

- Firewall appliance or virtual firewall cluster
- Elastic SIEM storage and analytics platform
- SOC L1 analyst with incident triage playbook

Capture:

- Type (hardware, software, infra, or human)
- Core function (what it processes or executes)
- Key dependencies (e.g., OS, network, vendor stack)

Pick a Physical Mechanism

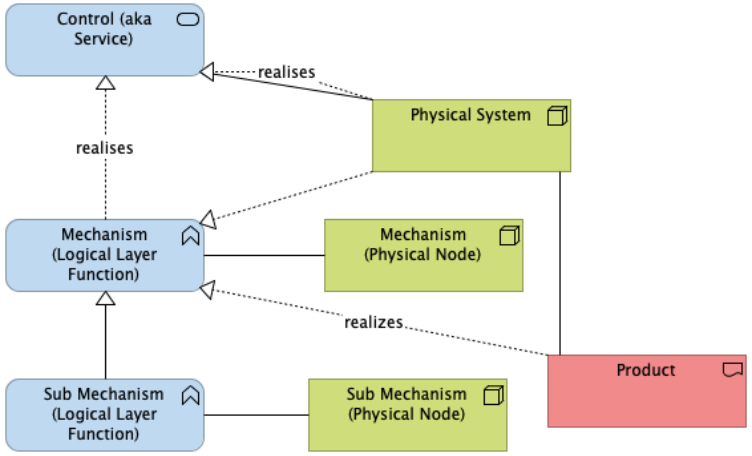
Select one Physical Mechanism (e.g., Firewall DPI Node, SIEM Event Collector, SOC Analyst Procedure).

Review what the mechanism does, its inputs/outputs, and role in the security service.

Align to Mechanisms

- Map each Physical System clearly back to the Physical Mechanism(s) it supports.
- Discuss whether one system can host multiple mechanisms or needs separation.
- Consider diversity of implementation (appliance vs cloud-native vs manual process).

- A clear mapping from Physical Mechanism → Physical System(s).
- Visibility of the concrete execution environment for security capabilities.
- Basis for asset inventory, architecture modelling, and operations planning.



Product

A Product is a tangible component—such as a hardware appliance, software package, tool, standard or reference implementation—packaged by a vendor or developed in-house to provide the technological foundation for executing Security Mechanisms and Sub-Mechanisms. It resides at the component layer of the SABSA framework, translating conceptual and logical designs into procurable solution artefacts.

Key Characteristics

- **Vendor-specific:** Identified by product name, version and vendor, encapsulating defined feature sets and supported protocols.
- **Standards-compliant:** Conforms to industry standards, regulatory requirements and enterprise policies.
- **Deployable artefact:** Delivered as physical appliances, software installations, cloud services or documented procedures.
- **Configurable and extensible:** Supports parameterisation, integration and customisation to meet organisational requirements.
- **Managed lifecycle:** Governed by procurement, deployment, patching, upgrade, support and retirement processes.

Operational Definition

A Product represents the concrete solution offering that is procured, configured and maintained to realise security functionality. It defines interface specifications, operational constraints and support agreements, and forms the basis for deploying mechanisms, sub-mechanisms and ultimately delivering technical Security Controls.

Also Known As

Product / Solution Artefact (SABSA Component Layer), Technology Product (TOGAF / ArchiMate), Configuration Item – Product Type (ITIL / CMDB), Security Tool or Technology (ISO/IEC 27001 / CIS Controls), Solution Enabler (COBIT / ISACA), Information System Component (NIST CSF / NIST SP 800-53), Vendor Package / COTS Solution (Procurement Standards / IT4IT), Security Technology Product (ISA/IEC 62443 for OT contexts)

Can we do it in reverse?

Yes—reversing the process from "product" back up to Sub-Domain and Domain is both feasible and often desirable, because it proves traceability, validates value, and supports impact/risk analysis across the SABSA stack and adjacent frameworks.

What reverse means

Start with a product or control implementation, enumerate its delivered security services and control objectives, and then map those upward to the Business Attribute Profile, risk treatments, and the parent Sub-Domain/Domain scope.

This is backward traceability: linking solution components and features to their originating requirements and business drivers so each item has a clear "why."

Why do it

- Assurance and value proof: Backward links show each deployed tool or feature is justified by a business attribute and risk objective, avoiding shelf-ware and "gold-plating."
- Change and impact analysis: When a product setting changes or a licence is removed, upward links show which control objectives, risks, and business outcomes are affected.
- Audit and compliance: Many standards expect demonstrable traceability from controls to requirements and business needs; maintaining reverse links simplifies audits and reduces remediation churn.
- Rationalisation and cost control: Product-to-Domain maps reveal overlaps and gaps across tools, enabling consolidation decisions tied to explicit attributes and services.
- Product-led operating model: Treating security capabilities as products benefits from "reverse-engineering" strategy from what is actually used, ensuring product backlogs align to enterprise outcomes.

How to Execute

- Catalogue product capabilities as security services, then link each service to specific control objectives and risks in the SABSA Matrix using the Business Attribute Profile as the normalising lens.
- Maintain a two-way traceability matrix: forward (Domain→Component) for design and reverse (Product→Domain) for assurance and operations; automate where possible in tooling.
- Use domain modelling to scope inheritance, so mappings remain meaningful across organisational and lifecycle views without being constrained by predefined scopes.

When it's most useful

- During tool renewals or consolidations to evidence coverage and avoid weakening key attributes like availability or integrity.
- After incidents or regulatory updates to quickly identify which products and settings realise the affected requirements.
- When integrating SABSA with enterprise architecture methods to preserve end-to-end traceability across strategy, design, implementation, and run.

Demo Time

Using a tool to do this quickly.

This is work in progress and not a finished product so please be kind.

Business Context

Each LLM model will produce varying outputs and levels of detail

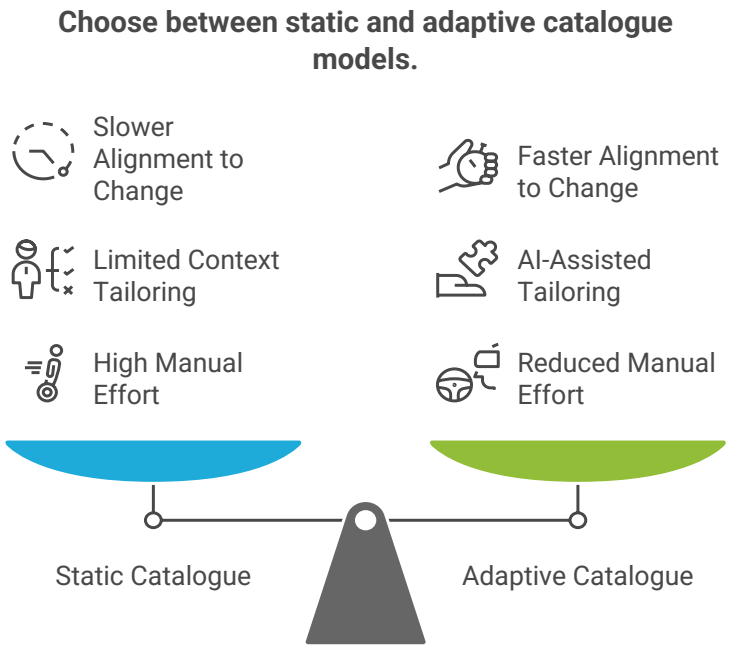
Generate a detailed business context for a fictional organisation in the [INSERT BUSINESS TYPE OR INDUSTRY HERE]. The output should cover the following categories, providing realistic, cohesive, and in-depth descriptions that highlight the business's objectives, competitive challenges, market context, operational priorities, and motivations. The viewpoint should be business-led, referencing security only where it is specifically called out. Each section should read like a plausible summary for a real company and facilitate the identification of SABSA domains and sub-domains for further analysis.

Sections:
+ - Business Drivers and Requirements
+ - Data Types
+ - Business Principles
+ - Technology Architecture
+ - Technology Capability
+ - Technology Strategy
+ - Channels
+ - Regulatory Compliance
+ - Business Opportunities
+ - Business Requirements
+ - Business Strategy
+ - Business Capability
+ - Architecture Principles

For each category, explain in detail:
+ - The core motivations and objectives of the business as they relate to the category
+ - The typical challenges faced and approaches taken
+ - How the business context influences key priorities, strategies, and relationships (internal and external)
+ - Any relevant opportunities, risks, or constraints unique to the business type or industry

Format responses to ensure they are suitable for SABSA business context modelling and can be used directly to derive domains and sub-domains.

TSI R100: Stay Static or Go Adaptive?



The question

Is the original TSI R100 scope still relevant, or should we pivot to a relationship-based model that uses AI to generate and curate security service catalogues on demand, tailored to context?

Why consider a pivot

- Relationship-first: tie services to business outcomes, risks, threat intel, compliance obligations, and measures, so the catalogue flexes with change.
- AI-assisted generation: use LLMs and graph queries to assemble “just-in-time” service views for scenarios (e.g., M&A, new regs, cloud migrations), with human governance.
- Faster alignment: reduce time from strategy change to catalog updates; improve traceability and auditability of rationale and control choices.

What stays, what changes

- Keep: TSI R100’s taxonomy, service definitions, and control patterns as the canonical knowledge base.
- Change: delivery as dynamic views generated via relationships (graph model) plus AI tooling, not static slides or fixed lists.

Proposed decision statement

Approve a strategic pivot: maintain R100 as authoritative content, delivered through a relationship-based metamodel with AI-supported, on-demand catalogue generation and lifecycle governance.