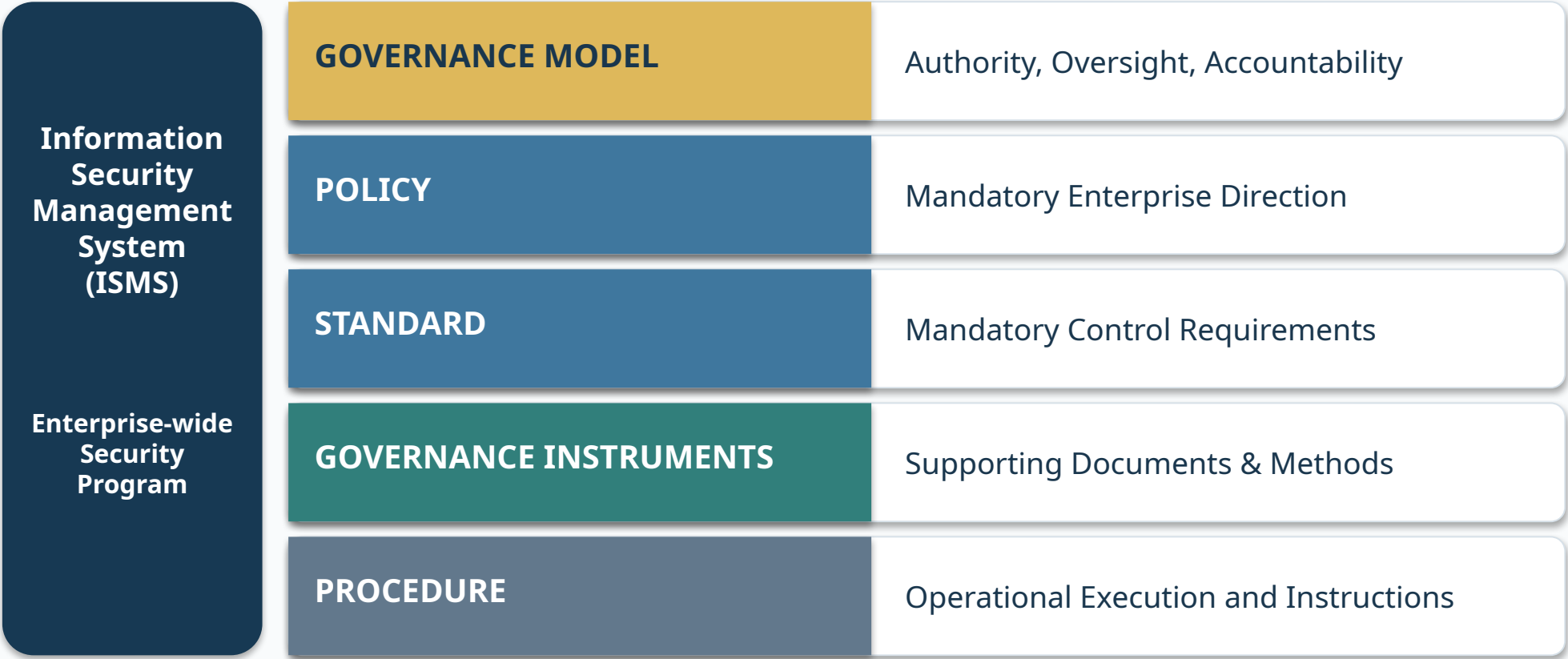


Information Security Governance

Policies, Standards & Governance Instruments (PSGI)

Governance Model • ISMS program context • PSGI Matrix
Hierarchical traceability • Controlled exceptions • Maintenance

One Hierarchy • One Enterprise Information Security Program



The ISMS is not an additional PSGI document level. Document approval roles must be defined separately.

PSGI Matrix — the ISMS column remains foundational

Illustrative excerpt of the approved Forward Matrix design; actual workbook retains nine Policy domains and all original entries.

ISMS	POLICY	STANDARDS	GOVERNANCE INSTRUMENTS	PROCEDURES
Enterprise-wide program Context Spans all Policy domains	Security Governance	Risk Mgmt · Metrics & KPIs	Policy & Standards Mgmt	Function owned
	Data Security	Classification · Cryptography	Employee Data Handling	Function owned
	Access Security	Account Lifecycle · MFA	User Responsibilities	Function owned
	Technology Security	Vulnerability · Endpoint	Acceptable Use	Function owned
	Personnel Security	Training · Awareness	Information Dept Ethics	Function owned
	Relationship Security	Vendor · Cloud Services	Outsourcing Services	Function owned
	Physical Security	Secure Areas · Monitoring	—	Function owned
	Resiliency (DR & BC)	Disaster Recovery · Continuity	Resiliency Overview	Function owned
	Compliance & Privacy	Compliance · Security Reviews	—	Function owned

Matrix = practical navigation • Document Register = control system of record • Exception Register = deviations and enforcement

Complementary Views and Controlled Records

GOVERNANCE TRIANGLE

Explains each level’s purpose, authority, and increasing operational specificity.

PSGI MATRIX

Visual working reference with the ISMS first column across all nine Policy domains.

Permanent document identifiers • Mandatory upward governing references • Many-to-many relationships

DOCUMENT REGISTER

Controls document identity, ownership, versions, approvals, mandatory status, applicability, and cross-references.

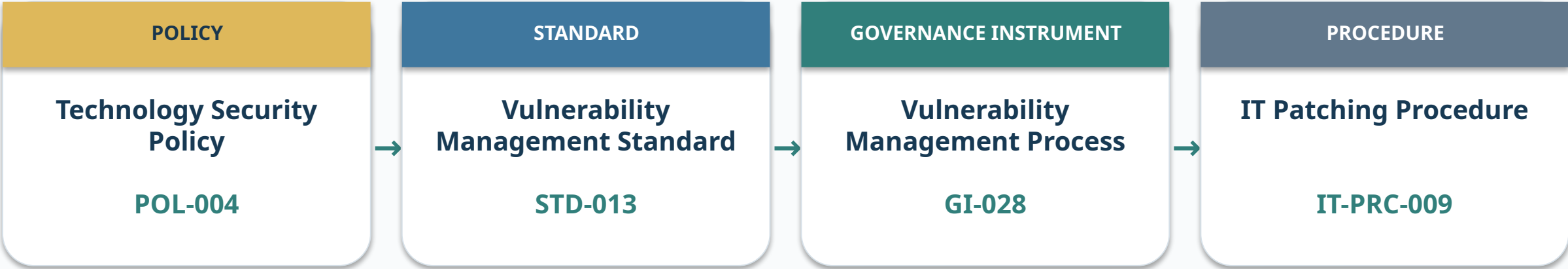
EXCEPTION REGISTER

Controls Entity requests, central decisions, risk assessments, deadlines, reviews, and Risk Committee dispositions.

The Matrix remains intentionally simple; the Registers supply the detailed records.

Hierarchical Requirements Traceability

Each controlled document cites its governing PSGI document identifier(s); version is recorded separately.



An Instrument may support multiple Standards; a Procedure may reference several higher-level documents. An intervening document is not required at every level.

ILLUSTRATIVE ONLY: Reference numbers and titles are examples, not actual approved corporate assignments.

Entity Applicability and Enforceable Exceptions

GOVERNANCE INSTRUMENT CLASSIFICATIONS

Mandatory
Customized
Entity-Specific

Each Instrument also carries a separate mandatory designation and defined Entity applicability.

APPROVAL AUTHORITY

Entity management endorses an exception request.

Enterprise CISO or designated central enterprise authority approves, rejects, or formally re-approves it.

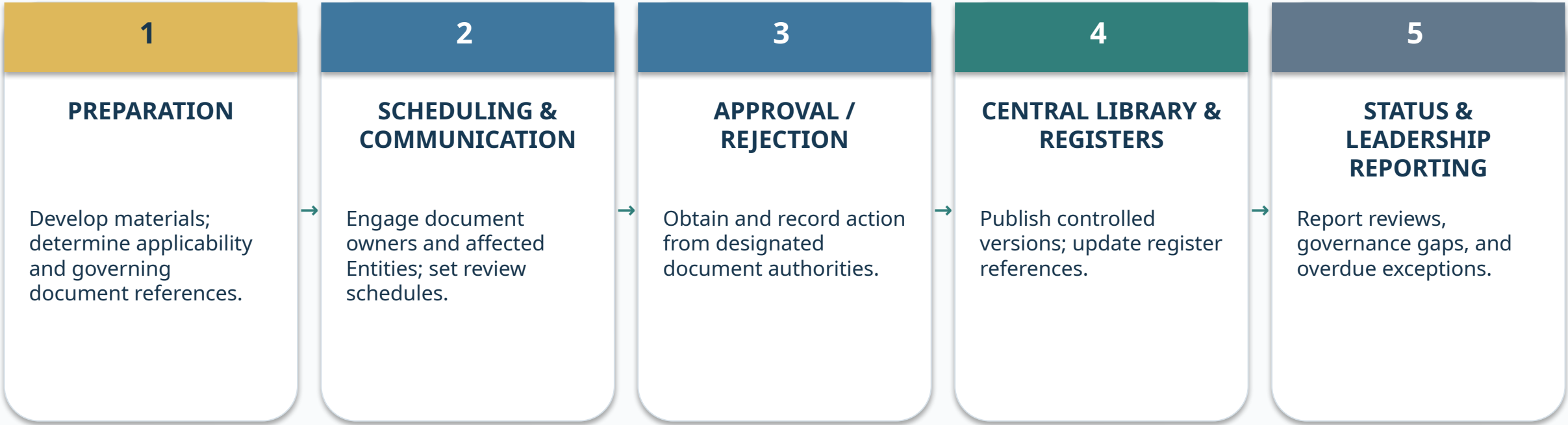
MANDATORY RISK COMMITTEE ESCALATION

Any exception missing its solution / remediation date or formal re-approval date must be escalated, regardless of risk rating or requesting Entity.

Exceptions are documented, time-limited, monitored and re-approved affirmatively. They do not waive applicable law or regulation.

Five-stage PSGI Governance and Maintenance Process

The original recurring governance lifecycle is retained, with document control, Entity applicability, and risk enforcement.



Ownership of business or technology Procedures stays with the responsible operational functions.

Governance ownership and control boundaries

Enterprise governing authority	Establishes Governance Model, authority and oversight
Enterprise Information Security	Administers PSGI; coordinates Policy and Standard governance
PSGI document owner	Maintains its assigned controlled document and reviews
Designated document approver	Approves controlled documents under formally designated authority
Entity management	Endorses exception requests; remains accountable for Entity actions
Enterprise CISO / designee	Central decision authority for PSGI exceptions
Enterprise Risk Committee	Receives mandatory escalations of missed exception deadlines
Operational functions	Own and maintain their Procedures

Specific document-approval authorities and routine review intervals remain implementation decisions.

Practical Value of the Coordinated PSGI Methodology

The distinctive value is not the existence of Policies and Standards: it is the way they are organized, connected, governed, and enforced.

EXECUTIVES

Understand governance coverage, accountability, Entity applicability and exceptions without navigating a library of individual files.

DIRECTORS & MANAGERS

Find related governance materials, identify document owners, confirm controlling references, and monitor maintenance.

ANALYSTS & ENGINEERS

Use the visual Matrix as a day-to-day reference; follow document identifiers to controlled sources and relevant procedures.

Methodology scope: five-level hierarchy, ISMS context, Matrix + Registers, traceability, exception enforcement, and five-stage governance maintenance.