

G360 INFORMATION SECURITY

PSGI Implementation Guide

Policies, Standards & Governance Instruments

PUBLIC EDITION | 14 OCTOBER 2026

Scope: five-level governance hierarchy, hierarchical document identification and traceability, Governance Instrument applicability, the PSGI Matrix and registers, exception management, and the PSGI governance/maintenance lifecycle.

Publication and implementation status

This public edition explains the G360 PSGI methodology and its implementation approach. The methodology principles summarized here have been approved for publication by the methodology owner. Example documents, identifiers, approval assignments, control mappings, and corporate adoption are illustrative unless explicitly designated otherwise. Enterprise-specific specifications identified in Section 9 require decisions by the adopting organization.

Control principles adopted for development

- The Governance Model is the top hierarchy level; ISMS describes the overarching management system.
- Policies and Standards are mandatory within their defined scope. Governance Instruments use Mandatory, Customized, or Entity-Specific classifications and a separate individual MANDATORY indicator.
- The PSGI Matrix stays an at-a-glance visual index, supported by separate Document and Exception Registers.
- Unique permanent document identifiers and references to governing documents are mandatory for controlled PSGI documents.
- Exceptions require Entity management endorsement and central enterprise approval; missed solution or re-approval dates require Risk Committee escalation.

Source continuity: adapted from PSGI Implementation Guide Working Draft 6 (13 October 2026), incorporating the methodology owner's PSGI consistency decisions. Section 9 intentionally retains implementation specifications requiring enterprise decisions.

1 Purpose, scope, and status

This guide provides an implementation framework for the G360 Policies, Standards & Governance Instruments (PSGI) methodology. It explains how enterprise security direction is translated into mandatory requirements, supporting governance materials, and operational execution. The methodology is intended to be adaptable to a parent enterprise containing multiple business Entities with differing sectoral, jurisdictional, and operational obligations.

The guide separates (a) approved methodology principles from (b) implementation specifications that still require enterprise decisions. It does not itself assign approval authority to particular executives beyond the approved central-approval model for PSGI exceptions, or establish review intervals, corporate document numbers, or actual control mappings.

2 Governance hierarchy and ISMS relationship

The Information Security Governance Model establishes enterprise security leadership, decision authority, accountability, and oversight. It is the first level of the five-level PSGI hierarchy. The Information Security Management System (ISMS), by contrast, is the coordinated enterprise-wide management system through which security governance requirements are organized, implemented, monitored, maintained, and assessed. The ISMS provides program-wide context for the Governance Model and the documents below it; it is not a sixth document level or a competing name for the Governance Model.

Matrix design rule: The ISMS shall remain a prominent, continuous first column in the PSGI Matrix, visibly spanning each Policy domain and the related Standards, Governance Instruments, and Procedures. It represents their shared management-system context, while the Governance Model establishes authority and oversight. A horizontal Governance Model heading may be used without displacing or collapsing the ISMS column.

Level	Principal purpose	Authority / ownership note
Governance Model	Defines the enterprise governance context, authority, and accountability.	Established by enterprise governing authority.
Policy	Expresses mandatory enterprise security direction.	Mandatory within defined scope.
Standard	Translates Policies into specific mandatory control requirements.	Mandatory within defined scope.
Governance Instrument	Provides official statements, methods, guidance, processes, architectures, registers, metrics, and other support.	Classification and mandatory status determined individually.
Procedure	Directs operational activities and work instructions.	Owned by the responsible business or technical function.

Specificity generally increases toward Procedures, but lower-level documents cannot conflict with or silently override applicable higher-level requirements. A corresponding document is not required at every intervening level.

3 Hierarchical Requirements Traceability

Core principle: Each level of the PSGI hierarchy translates, elaborates upon, and supports requirements established above it, progressing from enterprise direction toward operational execution. Standards are derived from applicable Policies; Governance Instruments support applicable Policies and Standards; Procedures implement requirements relevant to their activities.

3.1 Document identification and required governing references

- Every controlled PSGI document shall have a unique and permanent document identifier; revisions shall use a separate version value.
- Except for the top-level Governance Model, each controlled document shall contain a standardized “Governing and Related PSGI Documents” section citing its applicable higher-level governing documents by their official identifiers.
- The PSGI Document Register shall maintain these references centrally and shall support lookup from higher-level to lower-level materials as well as the reverse.
- Related and supporting references may also appear in the standardized section, clearly distinguished from governing references.
- Operational Procedures may retain a business function’s established numbering convention provided they can be cross-referenced within the PSGI framework.

Document numbering formats such as GOV-001, POL-001, STD-001, GI-001 and PRC-001 are examples only. The official prefix, ranges, and numbering authority remain to be defined.

3.2 Relationship model

Relationships are many-to-many rather than a rigid one-to-one chain. One Policy may support multiple Standards; one Governance Instrument may relate to several Policies or Standards; and one Procedure may implement requirements directly from several levels. Document-level traceability is required. Requirement- or section-level cross-references may be added selectively where regulatory, contractual, audit, or risk considerations justify them.

3.3 Illustrative traceability path

Illustrative item	Example identifier	Governing reference
Technology Security Policy	POL-004	Governance Model
Vulnerability Management Standard	STD-013	POL-004
Vulnerability Management Process	GI-028	STD-013; POL-004 (if applicable)
IT Patching Procedure	IT-PRC-009	STD-013; GI-028

Illustrative titles and identifiers, not approved G360 corporate documents or verified requirement-to-requirement mappings. The Vulnerability Management progression follows the source presentation’s use case.

4 Governance Instrument classification and Entity applicability

Governance Instruments are a family of supporting materials, including official security statements, guidelines and good practices, methods, overviews, processes, centralized functions, architectures, minimum contractual security language, registers, reports, and metrics. Their document type alone does not establish whether they are mandatory.

Classification	Working definition
Mandatory	An instrument category intended to express a required common governance direction within its approved scope; individual enforceability must still be explicitly designated.
Customized	An instrument intended to accommodate formally authorized adaptation to differing operating conditions while respecting governing Policies and Standards.

Classification	Working definition
Entity-Specific	An instrument addressing needs or additional obligations of a defined business Entity, sector, jurisdiction, or specialized operation that differ from or are not covered by general enterprise Standards.

An instrument shall also have a separate visible MANDATORY indicator and an applicability designation. A Customized or Entity-Specific classification does not by itself mean optional; likewise, a title or category does not itself establish a mandatory designation. Individual mandatory assignments and the detailed applicability/approval criteria remain subject to the methodology owner's determination.

Illustrative Entity-Specific contexts include casinos and gaming, law enforcement, aviation, and maritime operations (including SOLAS-related obligations). These are examples of sectors with distinct requirements, not assertions that any specific obligation is satisfied by a named PSGI document.

An Entity may seek an exception to an applicable Governance Instrument, but shall not treat it as waived merely because that Entity is specialized. An approved internal exception cannot excuse noncompliance with applicable laws or regulations or automatically waive mandatory Policies or Standards.

5 PSGI working artifacts and their boundaries

Artifact	Role	Not its purpose
PSGI Governance Triangle	Conceptual five-level view, purposes and progressive specificity.	An exhaustive document inventory.
PSGI Matrix	Visual, everyday placemat/index with a continuous ISMS first column spanning Policy domains; displays Policies, Standards, Governance Instruments and departmental Procedures.	The detailed system of record for every document, approval, or exception.
PSGI Document Register	Controlled record of documents, versions, ownership, approvals, mandatory flags, scope and hierarchical references.	A substitute for the readable, visual Matrix.
PSGI Exception Register	Controlled record of requests, risks, approvals, dates, enforcement, and closure.	Authority to approve or extend exceptions automatically.

The approved Forward Matrix retains a continuous leftmost ISMS column extending across all Policy domains; its additional columns present Policies, Standards, Governance Instruments, and departmental Procedures. The Matrix is a visual reference, not the system of record for document approval or exceptions. Detailed control attributes, hierarchical references, and exceptions belong in the separate Document and Exception Registers. The current illustrative matrix entries must not be presented as proof of formally approved document numbers, mandatory designations, or implemented document hyperlinks.

5.1 Minimum proposed PSGI Document Register fields

Document identifier; title; hierarchy level; owner; responsible approval authority; approval status and dates; version and effective date; next review date; authoritative document link; mandatory designation (for Governance Instruments); Instrument classification (where relevant); Entity applicability; higher-level governing document IDs; related document IDs; and archival/supersession status. Priority may be included if formally used.

6 PSGI Exception Management and enforcement

Exceptions are controlled, time-bounded authorizations for an identified Entity to deviate from a specified Governance Instrument or provision. The requesting Entity must endorse the exception. The Enterprise CISO or other designated central enterprise authority approves, rejects, or renews it. The Risk Committee provides enforcement oversight for missed commitments; referral to that committee does not itself constitute approval or extension.

6.1 Required exception lifecycle

Step	Control expectation
1. Request	Identify Entity, affected Instrument/provision, reason for deviation, proposed duration, and accountable business owner.
2. Assess	Evaluate risk, regulatory/contractual obligations, alternatives, compensating controls, and proposed solution/remediation date.
3. Endorse and decide	Obtain Entity management endorsement followed by central enterprise approval or rejection. Record evidence and conditions.
4. Register and monitor	Record approved scope, effective/expiration dates, re-approval date, review milestones, accountable owners, and evidence of controls.
5. Review and re-approve	Reassess changes and residual risk. Continuing deviations require affirmative central re-approval; no automatic renewal.
6. Close / revoke / escalate	Close when resolved; revoke when no longer justified; escalate missed solution or re-approval deadlines to Risk Committee.

6.2 Mandatory Risk Committee escalation

ENFORCEMENT RULE: Any and all exceptions that miss either their designated solution/remediation deadline OR formal re-approval date shall be brought to the Enterprise Risk Committee, regardless of Entity, justification, or risk rating.

The Risk Committee shall be provided the missed obligation, aging, residual risk, relevant Entity accountability, interim controls, proposed corrective action and owner, and next action date. Its disposition, required follow-up, and closure evidence shall be entered into the Exception Register. An expired or overdue exception does not renew automatically; committee review does not displace the designated central exception-approval authority.

Exceptions with material or urgent exposure may require immediate notification through enterprise escalation channels rather than waiting for a scheduled committee meeting. The notification channel and timing thresholds are implementation decisions to be established.

6.3 Proposed Exception Register fields

Identity & authority	Risk, dates & enforcement
Exception ID; Entity; affected PSGI document ID and section; justification; Entity sponsor/endorser; central approving authority; decision and evidence.	Risk and regulatory assessment; compensating controls; business owner; committed solution date; effective and expiration dates; next review and formal re-approval dates.
Status; approval history; renewals; supporting artifacts and audit trail.	Overdue flags; Risk Committee referral date; committee disposition; corrective-action owner; revised commitments; verification of final closure.

7 PSGI Governance and Maintenance Process

The original recurring five-stage PSGI Governance and Maintenance Process is retained, with the following controls added. Specific document approval authorities are not inferred from document ownership and must be defined by the enterprise.

Stage	Required work products / control activities
1. Preparation	Prepare or revise material; assign/document ID; identify governing references and scope; verify classification and legal/regulatory considerations; identify owner and proposed approver.
2. Scheduling & Communication	Notify affected stakeholders and Entities; set review and consultation schedule; capture feedback and decisions; trigger reviews for material changes.
3. Presentation & Approval / Rejection	Submit for designated approval; record approvals, rejections, and deferrals; prevent unapproved content from being represented as authoritative.
4. Updating Central Library	Publish approved version; update Document Register, Matrix pointers and applicable exception references; retain superseded versions and archive metadata.
5. Status & Progress Reporting	Report approvals, overdue document reviews, coverage gaps, register completeness, Entity applicability, and overdue exceptions and Risk Committee escalation.

7.1 Scheduled and event-driven maintenance

Each controlled document shall have an accountable owner and a recorded next review date. Material changes in regulatory obligations, business structure, operating conditions, technology, threat/risk profile, or governing requirements should trigger additional reviews. A defined versioning and supersession scheme must preserve previous approved editions for evidence and audit purposes. The review cadence and approval/delegation matrix remain open for determination.

8 Governance ownership and reporting

Accountability	Default methodology assignment
Enterprise governing authority	Establishes the overarching Governance Model and oversight architecture.
Enterprise Information Security	Administers the PSGI framework, coordinates Policies/Standards governance and maintains central document administration.
Document owner	Develops, maintains, and reviews assigned controlled documents, coordinating with affected Entities.
Designated document approver	Approves or rejects individual controlled PSGI documents under authority to be defined.
Entity management	Endorses exceptions requested for its Entity and remains accountable for corrective actions.
CISO / designated central enterprise authority	Approves, rejects, or formally re-approves PSGI exceptions.
Enterprise Risk Committee	Reviews every escalated missed solution or re-approval commitment; directs and monitors enforcement follow-up.

Accountability	Default methodology assignment
Business / technology operational owner	Authors and maintains its own Procedures and ensures relevant governing PSGI references are maintained.

Central PSGI governance responsibility must not be interpreted as an assumption of responsibility for all Procedures. Information Security owns only the Procedures within its own operational remit; other departments remain accountable for their respective work instructions.

9 Implementation specifications still requiring owner decisions

The following matters are intentionally not presented as approved rules. They should be resolved before a corporate adoption or public presentation of the detailed operational model:

- Official document numbering format, issuing authority, naming conventions, and integration with existing departmental Procedure IDs.
- Individual Governance Instrument MANDATORY designations and exact Entity-applicability determination/approval rules.
- Document approval matrix, authority/delegation thresholds, and procedures for rejected or contested documents.
- Routine review intervals and event-driven review triggers for each controlled document class.
- Exception request/endorsement templates, risk acceptance thresholds, compensating control evidence standards, and renewal limits.
- Risk Committee submission frequency, escalation notification service levels, and disposition/closure protocols.
- Actual approved Policy/Standard/Instrument inventories, detailed document links, and any optional requirement-level mappings.
- Publication permissions and treatment of sensitive content in material shared with external auditors or clients.

Appendix A Example standardized reference section

Template for insertion near the beginning of a controlled PSGI document. All sample IDs below are illustrative.

Field	Example / instructions
Document ID and version	GI-028 Version 1.0 (format subject to final numbering convention)
Owner and status	Owning function; approved / pending / retired as appropriate
Governance Instrument attributes	Classification: [Mandatory / Customized / Entity-Specific]; MANDATORY: [approved Yes / No / pending]; Applicability: [Entities]
Governing PSGI Documents	STD-013 Vulnerability Management Standard; POL-004 Technology Security Policy (if applicable)
Related PSGI Documents	IT-PRC-009 IT Patching Procedure (related lower-level reference)
Approved exceptions	Exception Register references (if applicable); do not insert confidential exception details in broadly shared documents