GISA Information Security Maturity Model (GISA-ISMM)

Document Version Control

Document Version Control

Version	Date	Author / Editor	Summary of Changes	Approved By
1.0	2025.06.02	GISA Charter Committee	Initial condensed version (modularized)	GISA Executive Committee

GISA Information Security Maturity Model (GISA-ISMM)

Standardizing Public Sector Information Security Resilience in Sri Lanka

The GISA-ISMM is a nationally tailored information security maturity model developed by the GovInfoSec Alliance (GISA) to assess, benchmark, and uplift the security posture of Sri Lanka's public sector institutions. It offers a unified, evidence-based framework to evaluate the maturity of information security governance, operations, compliance, and culture across government organizations.

The GISA-ISMM is informed by and aligned with leading global frameworks, including:

- ISO/IEC 27001 & 27002 – Information Security Management Systems (ISMS) and control implementation
- NIST Cybersecurity Framework (CSF) – Adapted to cover broader information security functions
- NIST SP 800-53 & 800-61 – Controls for information systems and incident response
- CIS Controls v8 – Actionable security recommendations for organizations
- COBIT 2019 – IT governance and enterprise control maturity
- CERT-RMM / C2M2 – Operational resilience and capability models

GISA-ISMM integrates these standards into a practical, contextualized model suitable for Sri Lanka's legal environment, specifically aligning with the Sri Lanka Personal Data Protection Act (PDP Act) and public sector regulatory mandates.

Purpose and Strategic Objectives

- Establish a consistent baseline of information security maturity across ministries and departments
- Promote risk-based planning, control implementation, and capacity development
- Support compliance monitoring under the PDP Act and other sectoral regulations
- Enable inter-agency collaboration and national reporting
- Guide public institutions on the path to becoming resilient, trustworthy digital service providers

Maturity Levels

Level	Level	Description
0	**Nonexistent**	No formal policies, roles, or controls in place
1	**Initial**	Informal or reactive practices; limited documentation
2	**Developing**	Some policies exist; implementation is partial and inconsistent
3	**Managed**	Standardized, documented, enforced, and monitored controls
4	**Optimized**	Integrated with strategic planning; continuously improved based on metrics and threat intelligence

Core Domains Assessed

- Governance & Leadership:
    - Strategic oversight, budget, leadership roles, ISMS program ownership, Governance, Risk & Compliance (GRC)
- Risk Management:
    - Risk register, assessments, mitigation plans, third-party risks, GRC, Infrastructure Security
- Asset & Access Control:
    - Asset inventory, privileged access, MFA, IAM governance Infrastructure Security
- Threat Detection & Incident Response:
    - SIEM, SOAR, IR playbooks, drills, red teaming SecOps, CTI
- Policy & Legal Compliance:
    - Policy completeness, PDP Act, ISO 27001, audit readiness GRC, Policy & Compliance
- Secure Development & AppSec:
    - Secure SDLC, code reviews, CI/CD, vulnerability management AppSec, DevSecOps
- Infrastructure & Cloud Security:
    - Hardening standards, patching, configuration baselines, hybrid cloud posture, Infrastructure Security
- Training, Awareness & Culture:
    - Staff training, phishing simulations, leadership awareness, Cyber Hygiene Index Capacity Building & Awareness
- Threat Intelligence Sharing:
    - Use of MISP, IOC sharing, alerts, inter-agency intel collaboration, CTI
- Business Continuity & Resilience:
    - DR plans, BCP drills, RTO/RPO metrics, ransomware readiness, SecOps, Infra, GR

Assessment Process

- Institutions complete an annual self-assessment using the official GISA-ISMM scorecard
- Results are validated through biannual workshops and, where needed, external or peer review
- GISA consolidates results for national-level benchmarking, strategy refinement, and investment planning

Strategic Role in National Information Security:

The GISA-ISMM will serves as a cornerstone of Sri Lanka's digital governance transformation, contributing to:

- Full implementation of the Personal Data Protection Act (PDP Act)
- Strengthened inter-agency collaboration and crisis coordination
- Development of a Public Sector Information Security Hygiene Index
- Informed allocation of training, technology, and compliance resources
- Global engagement through CERT and regional info-sharing networks

Maturity Level Definition

- 0 – Nonexistent:
    - No awareness or action, no policies, roles, or controls exist
- 1 - Initial / Ad Hoc:
    - Reactive, informal practices, Security handled case-by-case; no consistent approach
- 2 - Developing / Defined:
    - Documented, partial implementation, Basic policies/processes exist; some implementation but no metrics
- 3 - Managed / Institutionalized:
    - Standardized and enforced Controls are applied consistently; measured and reviewed
- 4 - Advanced / Adaptive:
    - Proactive and optimized, fully integrated with risk, data, and threat intelligence; continuous improvement cycle in place

Maturity Bands:
Based on total Score.

- 0–10: Basic (At Risk)
- 11–20: Developing (Needs Support)
- 21–30: Intermediate (Growing Capability)
- 31–36: Proficient (Sector Ready)
- 37–40: Leading (National Model)

Assessment Cycle

- Every 12 months:
    - Each institution completes GISA-CMM Scorecard
- Every 24 months:
    - Peer-reviewed cross-institutional validation by GRC WG
- Mid-cycle check-ins:
    - Optional reviews via GISA Regional Hubs or Sector Champions

GISA-ISMM Domain Guidance Manual

Governance & Leadership

- Maturity Levels:
  - Level 0 – Nonexistent: No awareness, no defined roles or ISMS
  - Level 1 – Initial: No formal cybersecurity leadership
  - Level 2 – Developing: CISO role informally assigned
  - Level 3 – Managed: CISO with clear mandate and budget
  - Level 4 – Optimized: InfoSec integrated into executive governance
- Best Practices: Assign a CISO, establish ISMS, secure cybersecurity budget.
- Evidence: Org chart, cybersecurity budget, IS strategy
- Guidance: Elevate security leadership role, align ISMS with national policy.

Risk Management

- Maturity Levels:
  - Level 0: No risk awareness or documented assessments
  - Level 1: Risks handled informally
  - Level 2: Basic risk register maintained
  - Level 3: Periodic, formal risk assessments
  - Level 4: Continuous risk monitoring integrated with decision-making
- Best Practices: Use ISO 31000 or NIST RMF for structured risk assessment and mitigation.
- Evidence: Risk Register, Risk Assessment Reports
- Guidance: Institutionalize a regular risk review cycle.

Asset & Access Control

- Maturity Levels:
  - Level 0: No asset inventory or access control
  - Level 1: No asset register; unmanaged access
  - Level 2: Partial inventory, manual access reviews
  - Level 3: Centralized inventory, IAM with MFA
  - Level 4: Continuous access monitoring and adaptive control
- Best Practices: Maintain up-to-date asset inventories and enforce MFA
- Evidence: Asset list, IAM policy, access logs
- Guidance: Move from manual reviews to automated IAM tools.

Threat Detection & Incident Response

- Maturity Levels:
  - Level 0: No defined response process
  - Level 1: Ad hoc, undocumented response
  - Level 2: Documented but untested playbooks
  - Level 3: Validated playbooks; SIEM/SOAR in use
  - Level 4: Real-time detection; drills; red-teaming integration
- Best Practices: Establish IR Playbooks, SIEM/SOAR solutions, conduct red teaming
- Evidence: IR plans, drill logs, SIEM screenshots
- Guidance: Run regular tabletop and technical exercises.

Policy & Legal Compliance

- Maturity Levels:
  - Level 0: No policy or legal awareness
  - Level 1: No compliance mapping
  - Level 2: Partial alignment with legal/policy mandates
  - Level 3: Full PDP Act alignment; periodic audits
  - Level 4: Continuous compliance review and legal updates
- Best Practices: Align with PDP Act, ISO 27001, NIST CSF.
- Evidence: Policy register, compliance audits
- Guidance: Conduct biannual gap assessments.

Secure Development & AppSec

- Maturity Levels:
  - Level 0: No consideration of security in development
  - Level 1: No secure coding policy
  - Level 2: Guidelines exist, but ad hoc use
  - Level 3: Code reviews, SDLC, CI/CD controls enforced
  - Level 4: DevSecOps culture with bug bounty or automation
- Best Practices: Enforce secure coding, run vulnerability scans, integrate DevSecOps.
- Evidence: Dev policies, scan reports, CI/CD pipeline configs
- Guidance: Train developers and mandate SDLC compliance.

Infrastructure & Cloud Security

- Maturity Levels:
  - Level 0: Infrastructure is unmanaged or undocumented
  - Level 1: No baselines; ad hoc control application
  - Level 2: Manual hardening; basic patching
  - Level 3: Defined baselines; automation in place
  - Level 4: Continuous posture monitoring (CSPM, SIEM)
- Best Practices: Apply hardening standards, monitor cloud workloads, implement patch SLAs.
- Evidence: Hardening guides, patch logs
- Guidance: Automate vulnerability and config management.

Training, Awareness & Culture

- Maturity Levels:
  - Level 0: No awareness or InfoSec messaging
  - Level 1: Occasional campaigns only
  - Level 2: Mandatory training for IT staff
  - Level 3: Full coverage of end-users; LMS tracking
  - Level 4: Personalized, risk-based training and simulations
- Best Practices: Run annual training, phishing simulations, Cyber Hygiene Index.
- Evidence: LMS reports, awareness posters
- Guidance: Use KPIs to drive awareness outcomes.

Threat Intelligence Sharing

- Maturity Levels:
  - Level 0: No visibility or threat data consumption
  - Level 1: Limited awareness; passive consumption
  - Level 2: Consumes feeds (e.g., from CERT|LK)
  - Level 3: Issues alerts; participates in intel forums
  - Level 4: Automated threat sharing; threat ops integration
- Best Practices: Subscribe to MISP, share IOCs, issue alerts.
- Evidence: IOC feed, threat bulletins
- Guidance: Standardize formats and automate sharing.

Business Continuity & Resilience

- Maturity Levels:
  - Level 0: No plans or recovery strategies
  - Level 1: Awareness of BCP need only
  - Level 2: Draft BCP/DRP exists but untested
  - Level 3: Plans tested annually; RTO/RPO defined
  - Level 4: Inter-agency BCP collaboration; adaptive resilience plans
- Best Practices: Maintain tested DRP/BCP with defined RTO/RPO.
- Evidence: DRP docs, test reports
- Guidance: Annual drills and impact analysis.

Sample Information Security Maturity Model Assessment

Step 1: Each domain gets a score from 0 to 4, based on the institution's current maturity.

Domain	Maturity Level	Score
Governance & Leadership	Level 3	3
Risk Management	Level 2	2
Asset & Access Control	Level 2	2
Threat Detection & Incident Response	Level 1	1
Policy & Legal Compliance	Level 3	3
Secure Development & AppSec	Level 2	2
Infrastructure & Cloud Security	Level 1	1
Training, Awareness & Culture	Level 3	3
Threat Intelligence Sharing	Level 2	2
Business Continuity & Resilience	Level 2	2

Step 2: Total the Scores

`3 + 2 + 2 + 1 + 3 + 2 + 1 + 3 + 2 + 2 = 21`

Step 3: Map Score to Maturity Band

Band	Score Range	Status
Basic (At Risk)	0–10	☐
Developing	11–20	☐
Intermediate	21–30	☐
Proficient	31–36	☐
Leading	37–40	☐

Result**:** Intermediate (Growing Capability)

Step 4: Apply Assessment Cycle Logic

- This scorecard would be submitted during the annual cycle.
- A peer-reviewed validation would occur every 24 months.
- A mid-cycle check-in can optionally be requested via the GISA Executive Committee or Sector Champion if the institution wants to re-assess progress before the next formal cycle.

Step 05: Summary of Sample Institution

- Overall Maturity Score: 21/40
- Maturity Band: Intermediate
- Implications:
    - Solid foundation in governance, policy, and awareness.
    - Needs improvement in threat detection, cloud security, and AppSec maturity.
    - Eligible for targeted GISA support to reach Proficient status in the next cycle.