# Risk Management Frameworks and Security Guides

### The following global is a representative and partial list of risk management frameworks and guides. They provide guidance and best practices for managing risks in cloud security, edge security, cloud-native applications and containers, and public sector defense. The list also includes global frameworks by region although many of the general frameworks are adopted acting as a baseline. Country specific guides extend to meet the needs of local citizens, businesses, and governments.



### Cloud Security Focused Frameworks

##### NIST SP 800-53

* Security and privacy controls catalog for federal information systems and organizations, including controls specific to cloud computing environments. The 800-53 control family forms the baseline for other federal initiatives such as FedRAMP and FISMA.

##### CSA (Cloud Security Alliance) Cloud Control Matrix (CCM)

* A cybersecurity control framework for cloud computing, providing a detailed understanding of security concepts and principles that are aligned with CSA best practices.

##### CIS (Center for Internet Security) Controls

* A set of prioritized actions to protect organizations and data from cyber-attacks, including guidelines specifically for securing cloud environments.

##### ISO/IEC 27017

* A standard that provides guidelines for information security controls applicable to the provision and use of cloud services in addition to ISO/IEC 27002.

##### FedRAMP (Federal Risk and Authorization Management Program)

* A U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Important notes:

* FedRAMP does not apply to on-premise installations, just cloud deployment. On-premise authorization falls under FISMA and the entire stack, and continuous assessment must be addressed.
* FedRAMP considers all security constraints of that environment - everything from physical to application.
* Deploying your application onto a FedRAMP environment does NOT mean your application is FedRAMP certified. Responsibility is shared between the application provider and the infrastructure provider.
* Three levels of authorization exist (low, medium, high) based on data sensitivity.
* Does not hold classified data.

### Edge Security Focused Frameworks

##### ETSI (European Telecommunications Standards Institute) MEC (Multi-access Edge Computing) Security

* A framework providing security guidelines and best practices for deploying edge computing solutions, ensuring secure data processing and transmission at the edge.

##### NIST Cybersecurity Framework (CSF)

* A voluntary framework consisting of standards, guidelines, and best practices to manage and reduce cybersecurity risks, applicable to edge computing environments.

### 

### 

### Cloud-Native Applications, Infrastructure, and Containers Focused Resources

##### NIST SP 800-190 (Application Container Security Guide)

* A guideline that provides recommendations for securing container environments, including risk management practices for containerized applications.

##### Kubernetes Security Best Practices (CNCF)

* Guidelines and best practices published by the Cloud Native Computing Foundation for securing Kubernetes environments and containerized applications.

##### Kubernetes STIG (Security Technical Implementation Guide)

* The Kubernetes STIG provides security guidelines and best practices for configuring and securing Kubernetes clusters. Developed by the Defense Information Systems Agency (DISA), it includes requirements for securing the Kubernetes environment, including nodes, network configurations, and container security, to ensure compliance with Department of Defense (DoD) security policies.

Used across the DoD, US Federal government, and beyond as the de facto. Released MarCH 2023

##### Rancher STIG (Security Technical Implementation Guide)

* The Rancher STIG offers security configuration guidelines for Rancher, an open-source container management platform. It provides recommendations and requirements for securing Rancher deployments, including access control, logging, monitoring, and network security, to help organizations manage their containerized applications securely and in compliance with DoD standards. This STIG was approved in April 2023 and is the first multi-cluster management software to hold a DISA STIG.

##### SLE Micro STIG (Security Technical Implementation Guide)

* The SLE Micro STIG provides security guidelines and best practices specifically for the SUSE Linux Enterprise (SLE) Micro, which is a lightweight, purpose-built operating system designed for containerized and edge environments. Developed by the Defense Information Systems Agency (DISA), the STIG ensures that SLE Micro installations adhere to stringent security requirements, making them suitable for deployment in high-security environments, including those within the Department of Defense (DoD). This STIG was approved in June 2024.

#### Common Criteria (EAL4+)

* Common Criteria (EAL4+) defines a common set of tests regarding the process of the design, testing, verification, and shipping of new security products. Common Criteria enables customers to assess a level of trust in how a product has been designed, tested, built, and shipped.

### 

### 

### Public Sector Defense Focused Frameworks

#### DoD Cloud Computing Security Requirements Guide (SRG)

* A set of guidelines and requirements issued by the U.S. Department of Defense for securing cloud computing solutions used by defense agencies.

#### UK NCSC Cloud Security Principles

* A set of security principles published by the UK National Cyber Security Centre to help organizations assess the security of cloud services.

#### ISO/IEC 27001

* An international standard for managing information security, with applicability to cloud computing and public sector organizations.

#### C5 (Cloud Computing Compliance Controls Catalogue)

* A framework developed by the German Federal Office for Information Security (BSI) that outlines security requirements for cloud computing.

### 

### Industry Focused Frameworks and Guides

#### PCI DSS (Payment Card Industry Data Security Standard)

* PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It is intended to protect cardholder data from breaches and fraud. The standard includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

#### HIPAA (Health Insurance Portability and Accountability Act)

* HIPAA is a U.S. law that sets national standards for the protection of sensitive patient health information. The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI), while the HIPAA Security Rule establishes standards for safeguarding electronic PHI (ePHI). Compliance ensures that healthcare organizations, as well as their business associates, protect patient data from unauthorized access and breaches.

#### SOC 2 (System and Organization Controls 2)

* SOC 2 is a framework developed by the American Institute of CPAs (AICPA) for managing and securing customer data based on five "trust service criteria": security, availability, processing integrity, confidentiality, and privacy. It is commonly used by service organizations to demonstrate their commitment to data protection and risk management practices.

### 

### General and Frameworks and Guidelines

#### GDPR (General Data Protection Regulation)

* GDPR is a comprehensive data protection regulation enacted by the European Union to protect the privacy and personal data of EU citizens. It applies to all organizations that process personal data of individuals residing in the EU, regardless of the organization's location. The regulation mandates strict data protection practices, including obtaining consent, data minimization, and providing individuals with rights over their data.

#### NIS2 (Network and Information Systems Directive 2)

* NIS2 is an updated directive from the European Union aimed at improving the cybersecurity and resilience of network and information systems across the EU. It expands the scope of the original NIS Directive to cover more sectors and introduces stricter security and incident reporting requirements for critical and important entities in areas such as energy, transport, health, and digital infrastructure.

##### CORA (Cloud Operating Reference Architecture)

* CORA is a framework that provides a standardized approach for cloud architecture and operations, ensuring best practices for security, compliance, and operational efficiency. It is designed to help organizations manage their cloud environments effectively and securely, aligning cloud operations with business goals and regulatory requirements.

### 

### Asia-Pacific Regional Frameworks and Guides

#### APRA CPS 234 (Australian Prudential Regulation Authority - Prudential Standard CPS 234)

* A framework for information security management for financial institutions in Australia. It mandates that regulated entities maintain information security capabilities commensurate with the size and extent of threats to their information assets.

#### MAS TRM (Monetary Authority of Singapore - Technology Risk Management Guidelines)

* Guidelines to manage technology risks faced by financial institutions in Singapore. It covers governance, risk assessment, security controls, and incident management to ensure the robustness of IT systems.

#### PDPA (Personal Data Protection Act - Singapore)

* A law governing the collection, use, disclosure, and care of personal data in Singapore. It aims to protect individual privacy while enabling organizations to responsibly use data.

#### Japan's Cybersecurity Management Guidelines

* Guidelines issued by Japan's Ministry of Economy, Trade, and Industry (METI) and the Information-Technology Promotion Agency (IPA) to help organizations manage cybersecurity risks effectively.

#### CCPA (Cybersecurity Classified Protection Act - China)

* Regulations for the protection of information systems in China, establishing security measures based on the classification of information systems and the sensitivity of the data they process.

#### India's National Cyber Security Policy

* A framework to protect public and private infrastructure from cyber-attacks, safeguard data, and build a secure and resilient cyberspace for Indian citizens, businesses, and the government.

#### K-ISMS (Korean Information Security Management System)

* A certification standard for information security management in South Korea, ensuring that organizations implement appropriate security controls to protect information assets.

#### NDB Scheme (Notifiable Data Breaches Scheme - Australia)

* Part of the Australian Privacy Act, it mandates organizations to notify individuals and the Office of the Australian Information Commissioner (OAIC) about data breaches likely to result in serious harm.

#### OJK Regulation (Financial Services Authority - Indonesia)

* Regulations issued by Indonesia's OJK to enhance cybersecurity and information technology risk management in the financial services sector.

#### HKMA Supervisory Policy Manual (Hong Kong Monetary Authority)

* Guidelines and best practices for risk management and cybersecurity for financial institutions in Hong Kong, including technology risk management, outsourcing, and business continuity planning.

#### CSA Singapore Cybersecurity Code of Practice for Critical Information Infrastructure

* A code of practice issued by the Cyber Security Agency of Singapore (CSA) outlining the mandatory cybersecurity measures for operators of critical information infrastructure (CII) to protect against cyber threats.

#### ASEAN Framework on Personal Data Protection

* A regional initiative to harmonize data protection laws across ASEAN member states, promoting cross-border data flows while protecting personal data.

### 

### Middle Eastern Cloud Security Guidelines and Frameworks

#### UAE National Cybersecurity Strategy

* A comprehensive strategy to enhance cybersecurity in the UAE, addressing threats to critical information infrastructure and promoting cybersecurity awareness and resilience.

#### NESA (National Electronic Security Authority) IAS (Information Assurance Standards) - UAE

* Guidelines issued by NESA for ensuring the security of information systems in critical national infrastructure, including aspects related to cloud security.

#### SAMA Cybersecurity Framework - Saudi Arabia

* A framework issued by the Saudi Arabian Monetary Authority to strengthen the cybersecurity posture of financial institutions, including guidelines for securing cloud environments.

#### NCSC (National Cyber Security Center) Cloud Security Guidelines - Saudi Arabia

* Guidelines developed by the Saudi NCSC to help organizations implement secure cloud services, focusing on data protection, access control, and compliance.

#### Qatar National Information Assurance Policy

* A policy framework by the Ministry of Transport and Communications in Qatar, providing guidelines for securing information systems, including cloud security measures.

#### Oman National Cybersecurity Strategy

* A strategy aimed at enhancing the cybersecurity capabilities of Oman, including guidelines for securing cloud services and protecting critical information infrastructure.

### 

### African Cloud Security Guidelines and Frameworks

#### NIST-DT (National Information Technology Development Agency) Guidelines - Nigeria

* Guidelines issued by NIST-DT for securing government data in cloud environments, promoting best practices for data protection and cybersecurity.

#### South African Protection of Personal Information Act (POPIA)

* A comprehensive data protection law that includes guidelines for processing personal data in cloud environments, ensuring data privacy and security.

#### Kenya Information and Communications Act - Data Protection Guidelines

* Regulations under the Kenya Information and Communications Act, providing guidelines for data protection and cybersecurity in cloud services.

#### Morocco Law No. 09-08 on the Protection of Individuals with regard to the Processing of Personal Data

* A law that outlines the protection of personal data, including guidelines for secure data processing in cloud environments.

#### Rwanda Data Protection and Privacy Law

* Legislation aimed at protecting personal data, with provisions for securing data in cloud services and ensuring compliance with data protection standards.

### 

### South American Cybersecurity and Cloud Security Frameworks

#### LGPD (Lei Geral de Proteção de Dados) - Brazil

* Brazil's General Data Protection Law, similar to the GDPR, which sets out guidelines for the protection of personal data. It includes provisions for data security, privacy, and management, affecting cloud service providers and users.

#### National Cybersecurity Strategy - Brazil

* A strategic framework developed by the Brazilian government to enhance the country's cybersecurity posture, including measures to protect cloud infrastructure and critical information systems.

#### Argentinian Data Protection Law (Ley de Protección de los Datos Personales)

* Argentina's data protection law that sets out requirements for the processing and protection of personal data, including guidelines for secure data storage and processing in cloud environments.

#### Chile's Personal Data Protection Law (Ley de Protección de la Vida Privada)

* Chile's data protection law that provides guidelines for the protection of personal data, impacting how cloud service providers manage and secure data.

#### Colombian Data Protection Law (Ley Estatutaria 1581 de 2012)

* Colombia's data protection framework that establishes guidelines for data processing, protection, and privacy, including measures for cloud-based data security.

#### Uruguayan Personal Data Protection Law (Ley No. 18.331)

* Uruguay's legislation for personal data protection, providing guidelines for secure data management practices, including those relevant to cloud computing.

#### Peruvian Law on Personal Data Protection (Ley de Protección de Datos Personales)

* Peru's framework for personal data protection, which includes guidelines for data security and privacy, affecting cloud service providers and users.