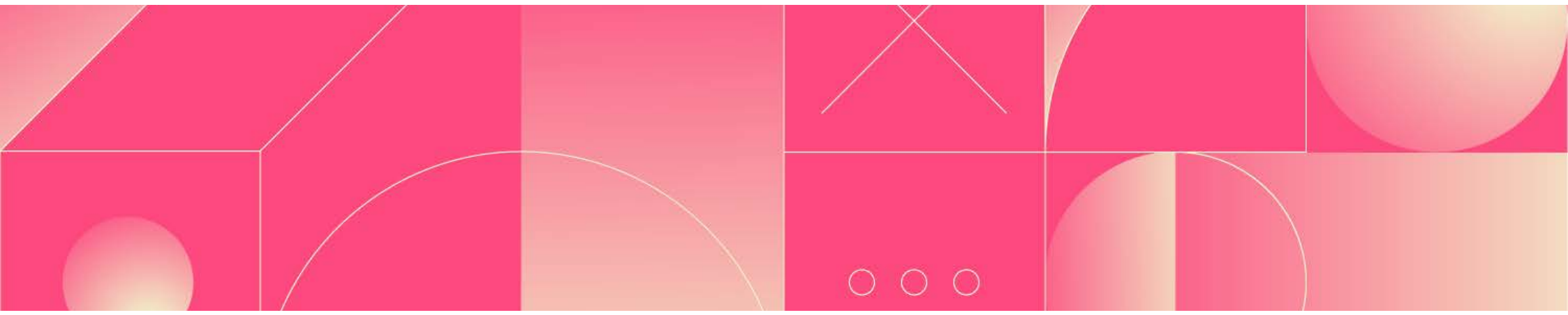
HORANGI
CYBER SECURITY

13 Compliance Frameworks For Cloud-Based Organizations

The need for cloud compliance begins as soon as you build on the cloud. Considering the shared responsibility of cloud security, which are the regulatory frameworks that you need to be aware of?



Organizations that use public cloud Infrastructure-as-a-Service (IaaS) can uniquely take advantage of how easy the cloud is to deploy and manage. With this incredible speed and power comes its own set of challenges, one of which is security — of which compliance is a subset.

Fortunately, as an organization that reaps the benefits of cloud, the shared responsibility of security in the cloud also means you are responsible only for managing data, classifying assets, managing access, and cloud configurations — all while the Cloud Service Provider (CSP) manages the hardware and operations ancillary to their data centers.

Choosing the right cybersecurity framework from the litany of available frameworks requires an intimate understanding of your business areas of jurisdiction and business requirements. From the three broad categories of framework...

- Industry & Location-Specific Regulations
- Security-Centric Frameworks
- Cloud Well-Architected Frameworks

... we dive into the 13 most significant compliance frameworks for the cloud today and which your organization is most suited for.

Industry & Location-Specific Regulations

At the top of an organization's compliance priority list ought to be the laws within their geographical jurisdiction and the industries they operate in. Non-compliance with these laws can have serious consequences, including reputation loss, hefty fines, and revocation of business licenses.

1. Credit Card Payments: PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards covering all merchants processing credit or debit card payments. This set of standards aim to protect card users against credit card fraud and identity theft.

Some of the things merchants need to do for be compliant with PCI DSS include:

- Use of antivirus software
- Installation of firewalls
- Regular vulnerability testing

If your organization stores and manages such sensitive credit card information in the cloud, it is your duty to equip your IT team with the specialized cloud expertise to securely design and maintain your cloud environment. Failure to comply with the PCI DSS Cloud Computing Guidelines could lose your organization the ability to process credit card payments.

2. Healthcare: HIPAA

The United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to protect individuals' health-related information, among which are sections that directly pertain to information security.

Organizations regulated under HIPAA are required to conduct risk analyses and establish risk management policies to manage threats to the confidentiality, integrity, and availability of critical health data they manage. If your organization uses cloud-based services (SaaS, IaaS, PaaS) to manage and transmit this data, it is your duty to ensure that the service provider is HIPAA-compliant, and you have adopted best practices in managing your cloud configurations.

3. Singapore: MAS-TRM

The Monetary Authority of Singapore (MAS) first published the MAS-TRM (Technology Risk Management) guidelines in 2013 to regulate IT systems within Financial Institutions (FIs) in Singapore.

In 2019, MAS released a consultation paper detailing changes to better reflect the state of IT systems used in FIs operating within Singapore. Some of these changes include:

- Specific guidelines for Agile development and DevOps
- Support for emerging technologies like the Internet of Things (IoT)
- More emphasis on cyber resilience and security monitoring

While most of the MAS-TRM guidelines themselves are not legally-binding, MAS subsequently released a legally-binding subset of the guidelines called the MAS Cyber Hygiene Notices that govern the gamut of FIs on cloud control items such as password policies, Multi-Factor Authentication (MFA), and access controls.

4. Malaysia: BNM-RMiT

Bank Negara Malaysia (BNM) Risk Management in Technology (RMiT) guidelines officially took effect from January 1, 2020. The guidelines impact companies operating in Malaysia that fall under these categories:

- Licensed banks
- Licensed investment banks
- Licensed Islamic banks
- Licensed insurers including professional reinsurers
- Licensed takaful operators including professional retakaful operators
- Prescribed development financial institutions
- Approved issuers of electronic money
- Operators of a designated payment system

If there were no clear regulations in Malaysia before governing secure cloud operations, BNM-RMiT now provides a mix of legally-binding regulations and best practices that include (not limited to the following):

- Emphasis on the inherent risk of using cloud computing technology
- Conducting a risk assessment prior to migrating all infrastructure and assets to the cloud
- Specific usage requirements on cloud services

5. Australia: APRA Prudential Practice Guide CPG 234

The Australian Prudential Regulation Authority's (APRA) Prudential Practice Guide identifies Information Security weaknesses within Australian FIs. They aim to help organizations in Australia become resilient against various threats.

CPG 234 operates on a zero-trust assumption on *emerging technologies* such as cloud computing. To quote APRA, services falling under *emerging technologies* should only be used when:

"The technology has matured to a state where there is a generally agreed set of industry-accepted controls to manage the security or technology; or compensating controls in place within the regulated entity are sufficient to reduce residual risk within the regulated entity's risk appetite".

As a cloud-based organization operating in Australia, the onus of demonstrating that your compliance posture is in line with industry best practices falls on you.

6. EU: GDPR

Known as one of the most stringent Data Privacy laws around the world, the main goal of the General Data Protection Regulation (GDPR) is to protect the personal data of all individuals and entities under the European Union (EU).

The GDPR governs all organizations that either operate in the EU, process data from EU citizens or residents, or offer goods and services to EU citizens or residents.

The GDPR stands on 8 fundamental rights that individuals possess over their personal data:

- The right of access: To know what information is gathered and how it is processed
- The right to be informed: To ask the organization to be completely transparent about data processing
- The right of rectification: To correcting any incomplete or incorrect personal data
- The right to restrict processing: To block the processing of personal data
- The right to be forgotten: To remove personal data at anytime for any reason
- The right to data portability: To transfer data from one service to another

- The right to object: To object data being used for certain purposes, including marketing research
- The right to be notified: To be notified within 72 hours of any personal data breach

Non-compliance to the GDPR can have very steep consequences — fines can reach up to €20 million, or 4% of the organization's worldwide annual revenue, whichever amount is higher.

Even with these fundamental rights in mind, your organization still needs to take concrete steps to have the right cloud processes and technology that honors the personal data entrusted to you by the customer. These concrete steps can come in the form of security-centric frameworks below.

Security-Centric Frameworks

Security-centric frameworks are independent of legal and financial regulations, but they are robust guidelines that your organization can use to meet regulatory requirements.

7. ISO 27001

The International Organization for Standardization (ISO) 27001 is the gold standard in information security and compliance. ISO developed the standard to help organizations protect their information according to best practices.

Being a CSP-neutral international standard, compliance to ISO27001 is internationally-recognized and can be a hard requirement for companies to become approved third party vendors. In the cloud, ISO 27001 contains end-to-end governance of items from asset management and access control to cryptography and operations security.

8. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) is a U.S. government agency responsible for developing standards and metrics that promote competition in the U.S. science and technology industries.

NIST developed their Cybersecurity Framework for compliance with U.S. standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA) in mind. They especially emphasize the classification of assets according to business value and securing them accordingly.

Relevant NIST standards for the cloud include NIST Special Publication 800-53 — Security and Privacy Controls for Federal Information Systems and Organizations and NIST 800-144 — Guidelines on Security and Privacy in Public Cloud Computing. These publications detail various security controls organizations can use to secure their systems.

9. CIS Controls

The Center of Internet Security (CIS) Controls are a set of open source, consensus-based guidelines that help organizations secure their systems. All controls go through a rigorous review process from various experts until they reach a consensus.

Each CIS control falls under one of two categories:

- Level 1: Controls that help narrow down an organization's attack surface without sacrificing functionality
- Level 2: In-depth controls aimed at organizations that require more stringent security measures

To quickly reference a set of controls for the cloud, your organization can refer to the relevant CIS Benchmarks, which have been adapted to specific CSPs, for instance, CIS-AWS, a set of controls tailored for workloads on Amazon Web Services (AWS).

10. CSA STAR

The Cloud Security Alliance (CSA) Security Trust And Risk Assurance (STAR) is a comprehensive program for cloud security assurance. Having controls mapped to PCI DSS, ISO 27001, NIST, and ISACA COBIT, CSA STAR stores documentation of the security and privacy controls from major CSPs.

By adhering to the STAR framework relevant to your CSP, your organization validates security posture and can demonstrate proof of secure cloud controls.

Cloud Well-Architected Frameworks

The major CSPs today have their own WAF (Well-Architected Frameworks) that are best practices covering not only security, but also efficiency and cost.

11. AWS Well-Architected Framework

The AWS Well-Architected Framework provides AWS users a guide to effectively architect solutions in the cloud. It provides a consistent benchmark for architects and evaluators that can aid in evaluating cloud systems in AWS.

- Operational Excellence: Bringing value to the business
- Security: Protecting assets, systems, and information in the cloud
- Reliability: Recovering from disruptions and meet its demand
- Performance Efficiency: Using resources efficiently as things evolve
- Cost Optimization: Minimizing or eliminating unnecessary costs

12. Google Cloud Architecture Framework

For organizations with workloads on the Google Cloud Platform (GCP), Google has provided its counterpart framework called the Google Cloud Architecture Framework. They have designed the framework in such a way that organizations can take note of the parts of the framework that most apply to their requirements.

This framework consists of four pillars.

- Operational excellence: Contains guidelines on how to increase efficiency, like monitoring, disaster recovery, and automation.
- Security, privacy, and compliance: A set of security controls and which ones are best suited to various use cases.
- Reliability: Suggestions on how to ensure high reliability and availability.
- Performance Cost Optimization: Recommendations on how to balance both performance and cost.

13. Azure Architecture Framework

If you're on the Microsoft Azure cloud, turn to the Azure Architecture Framework for guidance. Like other architecture frameworks, it's divided into several pillars:

- Cost: Bringing the most value for the least cost
- DevOps: Keeping systems running in production environments
- Resiliency: Recovering gracefully from failures.
- Scalability: Adapting to load changes, whether increasing or decreasing.
- Security: Protecting your data and applications from security threats.

No Compliance Without Security

Common to all the compliance frameworks for cloud-based organizations is that security plays a central role in building a trustworthy business. As your organization grows and expands across different regions, you may face various location-specific challenges.

It is Horangi's philosophy that compliance is a by-product of being secure. Your organization can pivot on a security-first mindset and be diligent about best practices to maintain a cost-effective compliance program, no matter the regulatory requirement.

If your organization is on AWS, you can now check if your AWS resources are properly configured with a free 14-day Horangi Warden trial. Warden helps you manage your compliance risks for MAS Cyber Hygiene, ISO 27001, PCI-DSS, and other compliance standards.