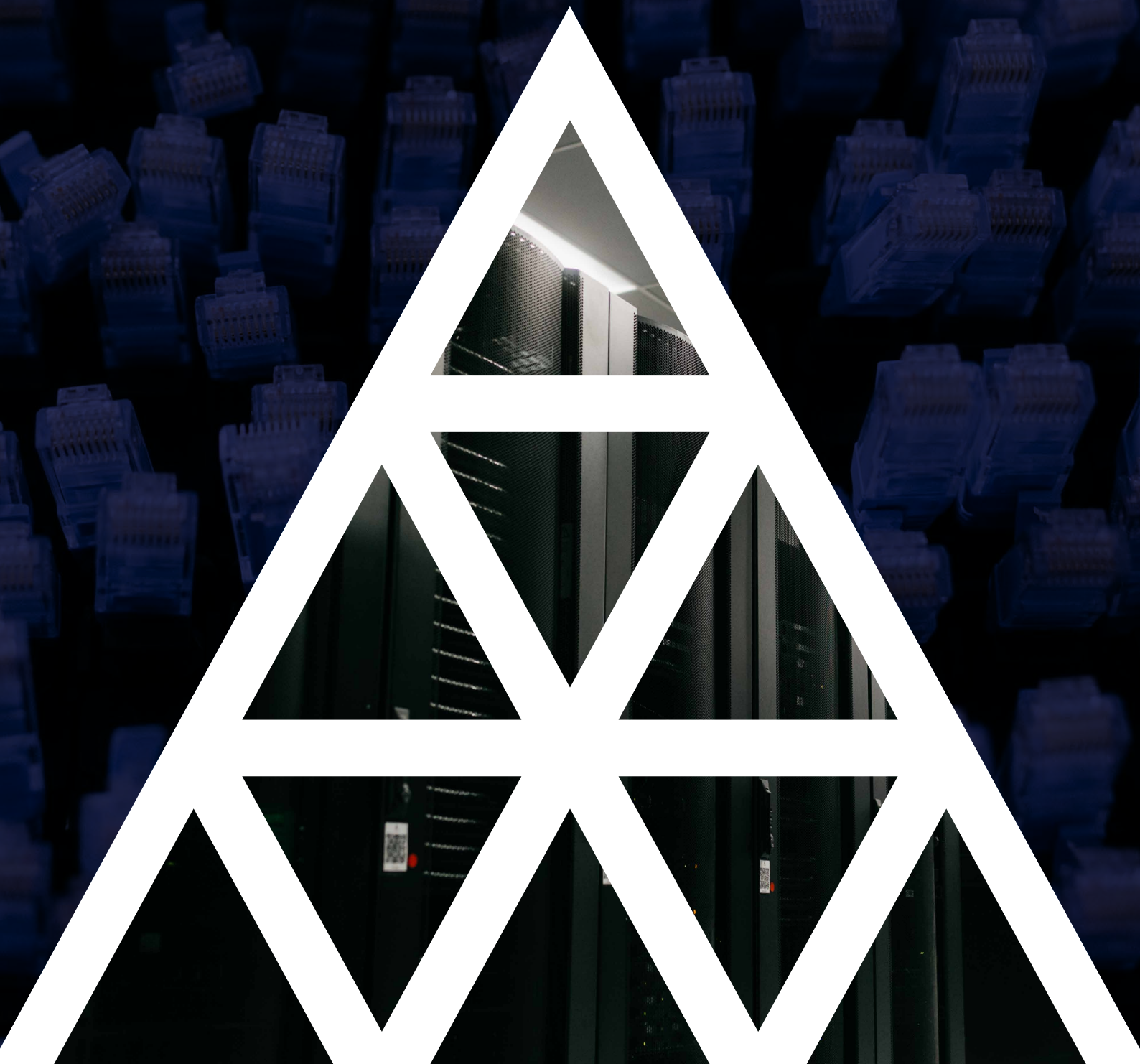
TRG Datacenters

The Ultimate Guide to Data Center Compliance Standards



The Ultimate Guide to Data Center Compliance Standards

Data center certification and compliance standards are defined to reduce client risk and set a baseline for data center and cloud operations. Standards help ensure that data, intellectual property, and people are protected from varying types of harm and that providers and their clients can be held accountable for non-compliance.

While sometimes perceived as a burden, standards help advance operational excellence by requiring data center providers to enhance their capabilities to meet their clients' needs as relevant industry technologies evolve.

We have developed this guide to quickly reference the compliance and certification standards that apply to your industry. We provide links to the source for each compliance summary so you can easily find more information on each standard, better understand how it applies to your enterprise, and determine if your data center provider also needs to be capable of addressing it.

TRG Datacenters

Two Guidelines from Three Ministries

2G3M

Medical institutions in Japan that place medical information in a 3rd party service (eg cloud) must review their risk management measures against the requirements of two guidelines set by three different government ministries. The guidelines are collectively referred to as the "Two Guidelines from Three Ministries" (2G3M).

https://www.mhlw.go.jp/stf/shingi2/0000166275.html

Association of Banks in Singapore

ABS

"The Association of Banks in Singapore is an industry association that represents the interests of the commercial and investment banking community in Singapore and provides practical steps for financial institutions (FIs) wanting to leverage cloud computing technology.

The ABS Cloud Computing Implementation Guide 2.0 (ABS Guide) is closely aligned to the MAS's Guidelines on Outsourcing and contains best–practice recommendations and considerations to support FIs' safe adoption of cloud, including guidelines on due diligence reviews, vendor management, and key controls to implement when using cloud service providers (CSPs)."

https://www.abs.org.sg/

Prudential Control and Resolution Authority

ACPR

"The Autorité de contrôle prudentiel et de résolution ("ACPR") is an independent administrative authority that monitors the activities of banks and insurance companies in France. ACPR is responsible for preserving the stability of the financial system and protecting customers, insurance policyholders, members, and beneficiaries of the persons that it supervises.

The ACPR Order of 3 November 2014 addresses requirements that a regulated entity is required to implement to ensure that outsourced services are adequately monitored and controlled. It provides specific guidance for regulated entities, including guidelines on qualifications and authorization, monitoring the service, controls to manage risk, service levels, termination, continuity of services, confidentiality, audit rights, notification, and reporting."

https://acpr.banque-france.fr/

American Institute of Certified Public Accountants — AICPA

Founded in 1887, the AICPA represents the CPA profession nationally regarding rule-making and standard-setting, and serves as an advocate before legislative bodies, public interest groups and other professional organizations. The AICPA develops standards for audits of private companies and other services by CPAs; provides educational guidance materials to its members; develops and grades the Uniform CPA Examination; and monitors and enforces compliance with the profession's technical and ethical standards.

The AICPA's founding established accountancy as a profession distinguished by rigorous educational requirements, high professional standards, a strict code of professional ethics, a licensing status and a commitment to serving the public interest.

https://www.aicpa.org/

Building Industry Consulting Service International 002-2019, Data Center Design — ANSI/BICSI 002

ANSI/BICSI 002-2019, BICSI's international best-seller, covers all major systems found within a data center. Written by industry professionals from all major disciplines, this standard not only lists what a data center requires, but also provides ample recommendations on the best methods of implementing a design to fulfill your specific needs.

While the traditional data center continues to be the focus, the breadth of content can also be applied to modular, containerized, edge and hyperscale data centers.

https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-2019-data-center-design

Australian Privacy Principles (APPs) — APPs

The Privacy Act 1988 (Cth) (Privacy Act), which includes the Australian Privacy Principles (APPs), regulates the way individuals' personal information is collected, used, and managed. The Act gives people the right to know why their personal information is being collected, how it will be used, and to whom it will be disclosed, and to ask for access to, or correction of, this information. While Google Cloud customers are responsible for ensuring that they comply with their obligations under the Privacy Act (including the APPs), we have provided an Australian Privacy Principles whitepaper that helps you meet your compliance requirements by detailing how information is stored, processed, maintained, accessed, and secured in Google Cloud Platform and Google Workspace.

https://www.oaic.gov.au/privacy/australian-privacy-principles/

Australian Prudential Regulation Authority Prudential Standard - CPS 231 Outsourcing

APRA Prudential Standard CPS 231

The Australian Prudential Regulation Authority (APRA) is an independent statutory authority that supervises institutions across banking, insurance and superannuation. The APRA Prudential Standard CPS 231 Outsourcing (Prudential Standard) specifies the key requirements that APRA regulated institutions must implement and maintain when they outsource business activities to service providers.

In particular, the Prudential Standard specifies the matters that should be included in the agreement between the regulated institution and their service provider, including requirements on audit and monitoring procedures, termination provisions, sub-contracting, security of information and termination rights.

https://www.apra.gov.au/

Australian Prudential Regulation Authority Prudential Standard - CPS 234 Information Security

APRA Prudential Standard CPS 234

The Australian Prudential Regulation Authority ("APRA") is an independent statutory authority that supervises institutions across banking, insurance and superannuation. The APRA Prudential Standard CPS 234 Information Security ("Prudential Standard CPS 234") aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. In particular, the Prudential Standard lays out information security requirements for several domain areas including: Information Security Capability, Policy Framework, Information asset identification and classification, Implementation of Controls, Incident Management, Testing Control Effectiveness, Internal Audit and APRA Notification.

https://www.apra.gov.au/

Bundesanstalt für Finanzdienstleistungsaufsicht Cloud Outsourcing Guidance

BaFin Cloud Outsourcing Guidance

The Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) is responsible for the supervision of all banks, credit institutions, insurers, funds and financial institutions in Germany. Its objective is to ensure the functioning, stability and integrity of the German financial market. BaFin issued guidance on outsourcing to cloud service providers (BaFin Cloud Outsourcing Guidance) to create greater transparency into the supervisory assessment of cloud outsourcing. The BaFin Cloud Outsourcing Guidance provides specific outsourcing guidance for financial institutions on contractual terms, including information and audit rights, the right to issue instructions, data security / protection, termination and chain outsourcing.

https://www.apra.gov.au/

Banco de España - Circular 2/2016

Banco de España - Circular 2/2016

The Banco de España supervises credit institutions and financial entities in Spain. The Banco de España is responsible for safeguarding the stability of the financial system, preventing significant disturbances in the banking sector and verifying regulated entities compliance with banking regulations. The Banco de España issued Circular 2/2016, which sets out the minimum requirements that Banco de España expects regulated entities to meet when outsourcing. Circular 2/2016 provides specific guidance on risk management, concentration risk, data locations, due diligence, monitoring the service, audit, termination, transition, sub-contracting, business continuity and security.

https://www.boe.es/

Banco de Portugal - Circular Letter

Banco de Portugal - Circular Letter

The Banco de Portugal regulates and supervises credit institutions, financial companies, and payment institutions in Portugal to ensure that the funds they were entrusted to hold are secure. Banco de Portugal issued Circular n.º CC/2019/00000065 ("Circular Letter") underlining the importance for institutions to adopt strong outsourcing practices, including the need to ensure contractual rights of access, information, and auditing that allow for both adequate control by institutions and, if necessary, the provision of information to Banco de Portugal. In this context, Circular n.º CC/2019/00000065 requires institutions subject to the supervision of Banco de Portugal to comply with the EBA Outsourcing Guidelines.

https://www.bportugal.pt/

Bank of Italy

Bank of Italy

The Bank of Italy is responsible for ensuring the sound and prudent management of intermediaries, the overall stability and efficiency of the financial system, and compliance with the rules and regulations of those subject to supervision. Circular 285 addresses the approach that the Bank of Italy expects regulated entities, such as banks and other financial institutions, to undertake in relation to outsourcing. Circular 285 provides specific guidance on data system security requirements, monitoring, accountability, traceability, and termination.

https://www.bancaditalia.it/

The Central Bank of Argentina

BCRA

The Central Bank of Argentina (the "BCRA") is responsible for monitoring the appropriate operation of the financial market and implementing the Law on Financial Institutions and other regulations. BCRA Comunicacion A 6375 addresses the minimum requirements for the management, implementation and control of risks related to information technology, information systems and related resources for financial entities. BCRA Comunicacion A 6375 provides specific guidance on: information security governance, access control, monitoring, incident management and continuity.

http://www.bcra.gov.ar/

Building Industry Consulting Service International - 002 2010

BICSI 002 2010

BICSI's international best-seller, covers all major systems found within a data center. Written by industry professionals from all major disciplines, this standard not only lists what a data center requires, but also provides ample recommendations on the best methods of implementing a design to fulfill your specific needs.

While the traditional data center continues to be the focus, the breadth of content can also be applied to modular, containerized, edge and hyperscale data centers.

https://www.bicsi.org/

Building Industry Consulting Service International - Accredited Personnel

BICSI Accredited Personnel

BICSI's international best-seller, covers all major systems found within a data center. Written by industry professionals from all major disciplines, this standard not only lists what a data center requires, but also provides ample recommendations on the best methods of implementing a design to fulfill your specific needs.

While the traditional data center continues to be the focus, the breadth of content can also be applied to modular, containerized, edge and hyperscale data centers.

https://www.bicsi.org/

Bank Negara Malaysia

BNM

Bank Negara Malaysia ("BNM") is responsible for developing, enhancing and implementing an effective supervision framework to ensure the safety and soundness of financial institutions and to enforce sound practices. The Risk Management in Technology guidelines ("RMIT guidelines") address BNM's expectations of how financial institutions manage their ongoing operational risks associated with the growing adoption of technology in the financial service industry. In particular, the RMIT guidelines lay out requirements for several domain areas including: cybersecurity, network resilience, risk management, data center security, implementation of internal controls, and internal audit functions.

https://www.bnm.gov.my/

Banking Regulation and Supervision Agency

BRSA

The Banking Regulation and Supervision Agency (the "BRSA") is responsible for oversight and regulation of the banking sector of the Turkish financial services industry. The Regulation on Banks' Information Systems and Electronic Banking Services ("IS Regulation") addresses outsourcing of information technology by Turkish banks. The IS Regulation provides specific guidance on: risk assessment, contractual standards, security and audit.

https://www.bddk.org.tr/

Bangko Sentral ng Pilipinas

BSP

The Bangko Sentral ng Pilipinas ("BSP") supervises the operations of banks in the Republic of the Philippines and is responsible for establishing monetary authority and oversight of the Philippine financial system. The Information Technology Risk Management guidelines ("ITRM guidelines") address the BSP's expectations of how financial institutions manage their ongoing operational risks associated with the growing adoption of technology in the financial service industry. In particular, the ITRM guidelines lay out requirements for several domain areas including: risk management, business continuity, asset classification, implementation of internal controls, compliance frameworks, internal audit, and reporting requirements.

https://www.bsp.gov.ph/

Bankwissenschaftliche Gesellschaft Austrian Financial Market Authority

BWG

The Austrian Financial Market Authority ("Austrian FMA") is responsible for the supervision of banks (in cooperation with the Austrian Central Bank), insurance companies, pension companies and the financial securities sector, including stock exchanges to promote cooperation on financial market issues and financial market stability. The Bankwesengesetz ("BWG") addresses the Austrian FMA's expectation of credit institutions when outsourcing functions. The BWG provides specific guidance on: audit rights, due diligence, monitoring, termination rights, security, business continuity and the location of data.

https://www.bwg.at/

California Consumer Privacy Act

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is a data privacy law that provides California consumers with a number of privacy protections, including right to access, delete, and opt-out of the "sale" of their personal information. Starting January 1, 2020, businesses that collect California residents' personal information and meet certain thresholds (e.g., revenue, volume of data processing) will need to comply with these obligations. The California Privacy Rights Act (CPRA) is a data privacy law that amends and expands upon the CCPA. The law takes effect on January 1, 2023.

https://oag.ca.gov/privacy/ccpa

Certified Fiber Optic Technician

CFOT Accredited Personnel

CFOT® - Certified Fiber Optic Technician - is the primary FOA certification for all fiber optic technicians. CFOTs have a broad knowledge, skills and abilities (KSAs) in fiber optics that can be applied to almost any job - design, installation, operation – and for almost any application using fiber optic communications. Prerequisites: None, online course Fiber U Basic Fiber Optics recommended for all students to prepare for the classroom courses or direct exam What To Expect In Training Programs For CFOT Certification To qualify for CFOT® Certified Fiber Optic Technician certification, a training program will cover at least the following topics: Overview of fiber optic applications and installations Communications systems utilizing fiber optics Fiber optic components appropriate for fiber optic networks Installation of premises and outside plant fiber optic cable Splicing and termination Testing fiber optic components and cable plants Hands-On Lab Exercises including hands-on splicing, termination and testing.

https://www.thefoa.org/cfot.htm

Criminal Justice Information Services

CJIS

The Criminal Justice Information Services Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI) sets standards for information security, guidelines, and agreements for protecting Criminal Justice Information (CJI). These standards are reflected in the CJIS Security Policy, which describes the appropriate controls to protect the sources, transmission, storage, and access to data. Google Cloud is able to support law enforcement agencies in states that have executed a CJIS Information Management Agreement with Google. For certain Google Cloud Platform products and services, Google Cloud offers security controls to protect and store Criminal Justice Information (CJI) data through Assured Workloads for Government.

https://www.fbi.gov/services/cjis

Cloud Computing Compliance Criteria Catalog (C5:2020)

Cloud Computing Compliance Criteria Catalog (C5:2020)

The Cloud Computing Compliance Criteria Catalogue, also referred to as C5:2020, was developed by the German Federal Office for Information Security (BSI) as a way to assess the information security of cloud services that leverage internationally recognized security standards like ISO/IEC 27001 to set a consistent audit baseline that helps establish a framework of trust between cloud providers and their customers.

https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html

Comisión Nacional Bancaria y de Valores

CNBV

The Comisión Nacional Bancaria y de Valores ("CNBV") is responsible for supervising and regulating financial institutions that make up the financial system in Mexico. The CNBV looks to ensure the stability and correct operation of the Mexican financial system as well as maintain and promote the healthy and balanced development of the system as a whole. The CNBV provides guidance for how financial institutions can effectively manage outsourcing risk in various frameworks. These frameworks provide specific guidance on: due diligence, monitoring the service, subcontracting, confidentiality and security of data, audit and access rights, business continuity and data portability.

https://www.gob.mx/cnbv

Cloud Security Alliance

CSA

The Cloud Security Alliance is a non-profit organization whose mission is to "promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing." The CSA's Security, Trust & Assurance Registry Program (CSA STAR) is designed to help customers assess and select a Cloud Service Provider through a three-step program of self-assessment, third-party audit, and continuous monitoring.

https://cloudsecurityalliance.org/

Cloud Security Alliance - Security Trust Assurance and Risk

CSA STAR

The Cloud Security Alliance (CSA) designed the Security, Trust, Assurance, and Risk (STAR) program as an assurance framework for cloud service providers (CSPs.) Combining the principles of transparency, rigorous auditing, and harmonization of standards, it provides organizations with cloud-specific structure and detail for their information security programs. The voluntary self-assessments, attestations, and certifications allow CSPs to validate their security posture and demonstrate their commitment to best practices.

https://cloudsecurityalliance.org/

Commission de Surveillance du Secteur Financier

CSSF

Commission de Surveillance du Secteur Financier ("CSSF") is responsible for supervision of the markets and ensuring the safety and soundness of the financial sector in Luxembourg. The CCSF published Circular 17/654 to provide a regulatory framework for financial institutions on IT outsourcing to public cloud service providers. Circular 17/654 provides specific guidance on: management of outsourcing risks, business continuity, systems security, monitoring of activities, contractual clauses and the right to audit.

https://www.cssf.lu/

Cyber Essentials

Cyber Essentials

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. Our advice is designed to prevent these attacks.

https://iasme.co.uk/cyber-essentials/

CyberGRX

CyberGRX

CyberGRX provides a third-party validated cyber risk assessment of Google Cloud's security posture. This assessment details our compliance with industry standards and the security protocols built into our infrastructure.

https://www.cybergrx.com/platform/cybergrx-exchange

DoD Information Assurance Certification and Accreditation Process

DIACAP

The DoD Information Assurance Certification and Accreditation Process (DIACAP) is a deprecated United States Department of Defense (DoD) process meant to ensure companies and organizations applied risk management to information systems (IS). DIACAP defined a DoD-wide formal and standard set of activities, general tasks and a management structure process for the certification and accreditation (C&A) of a DoD IS which maintained the information assurance (IA) posture throughout the system's life cycle. As of May 2015, the DIACAP was replaced by the "Risk Management Framework (RMF) for DoD Information Technology (IT)". Although re-accreditations via DIACAP continued through late 2016, systems that had not yet started accreditation by May 2015 were required to transition to the RMF processes.[1] The DoD RMF aligns with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

https://www.defense.gov/

U.S. Defense Information Systems Agency Provisional Authorization

DISA

The United States Defense Information Systems Agency (DISA) manages the evaluation and authorization of cloud services for the U.S. Department of Defense (DoD). Based on our FedRAMP Moderate authorization, DISA Cloud Service Support granted Google Cloud a DoD Impact Level 2 provisional authority to operate (P-ATO). An assessment at Impact Level 2 (IL2) allows storage or hosting of non-controlled, unclassified information as defined by the Cloud Computing Security Requirements Guide.

https://disa.mil/

Decree on Prudential Rule for Financial Undertakings

DNB Decree

The De Nederlandsche Bank ("DNB") is the central bank of the Netherlands. It supervises financial institutions in the Netherlands. The DNB Decree on Prudential Rule for Financial Undertakings ("DNB Decree") defines the supervisory conditions applicable to outsourcing by financial institutions. The purpose of these conditions is to control the relevant risks and ensure that outsourcing does not impede adequate supervision.

https://www.dnb.nl/

The Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide (CC SRG)

DoD DISA SRG

The Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide (CC SRG) outlines how the US Department of Defense (DoD) will assess the security posture of non-DoD cloud service providers (CSPs). Additionally, the CC SRG explains how non-DoD CSPs can show they meet the security controls and requirements before handling any DoD data. CC SRG provides for the following categorization: •Impact Level 2: Data cleared for public release (note: Level 1 was combined with Level 2) •Impact Level 4: Controlled unclassified information (CUI) over the Non-Secure Internet Protocol Router Network (NIPRNet). CUI includes protected health information (PHI), privacy information (PII) and export controlled data (note: Level 3 was combined with Level 4) •Impact Level 5: Higher sensitivity CUI, mission-critical information, or NSS over NIPRNet •Impact Level 6: Classified data over Secret Internet Protocol Router Network (SIPRNet).

https://public.cyber.mil/dccs/

European Banking Authority

EBA

The European Banking Authority (EBA) is an independent EU Authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector. The EBA Guidelines on Outsourcing Arrangements (EBA outsourcing guidelines) specify the internal governance arrangements that financial institutions within the EBA's mandate should implement when they outsource functions to service providers, including cloud service providers. These guidelines replace the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing that were issued in 2006. They also replace the EBA's recommendations on outsourcing to cloud service providers published in 2018.

https://www.eba.europa.eu/

European Insurance and Occupational Pensions Authority

EIOPA

The European Insurance and Occupational Pensions Authority ("EIOPA") is an independent EU Authority that works to foster financial stability and confidence in the insurance and pensions markets. The EIOPA Guidelines on Outsourcing to Cloud Service Providers ("EIOPA cloud outsourcing guidelines") specify the internal governance arrangements that insurance and re-insurance undertakings within EIOPA's mandate should implement when they outsource functions to cloud service providers. The guidelines clarify how the requirements in Directive 2009/138/EC (Solvency II Directive) and Commission Delegated Regulation (EU) No 2015/35 (Delegated Regulation) apply when outsourcing to a cloud service provider.

https://www.eiopa.europa.eu/

Energy Star Certified

Energy Star Certified

ENERGY STAR certified buildings save energy, save money, and help protect the environment by generating fewer greenhouse gas emissions than typical buildings. To be certified as ENERGY STAR, a building must meet strict energy performance standards set by EPA.

https://www.energystar.gov

Information technology - Data Centre Facilities and Infrastructures

EN 50600

EN 50600-3-1 Information technology - Data centre facilities and infrastructures - Part 3-1: Management and operational information - This European Standard specifies processes for the management and operation of data centres. The primary focus of this standard is the operational processes necessary to deliver the expected level of resilience, availability, risk management, risk mitigation, capacity planning, security and energy efficiency. The secondary focus is on management processes to align the actual and future demands of users. Figure 2 shows an overview of related processes. The transition from planning and building to operation of a data centre is considered as part of the acceptance test process in Clause 6. (...) NOTE 1 Only processes specific for data centres are in the scope of this document. Business processes like people management, financial management, etc. are out of scope. NOTE 2 Specific skill sets are required of those working in and operating a data centre.

https://www.en-standard.eu/csn-en-50600-3-1-information-technology-data-centre-facilities-and-infrastructures-part-3-1-management-and-operational-information/

Esquema Nacional de Seguridad

ENS

Law 11/2007 in Spain establishes a legal framework to give citizens electronic access to government and public services. Aligned with the ISO/IEC 27001 Standard, the framework defines a set of security controls for availability, authenticity, integrity, confidentiality, and traceability. The certification establishes security standards that apply to all government agencies and public organizations in Spain, as well as related service providers. For more information, see.

https://joinup.ec.europa.eu/collection/spain-center-technology-transfer/solution/national-security-scheme-ens

European Securities and Markets Authority

ESMA

The European Securities and Markets Authority ("ESMA") is an independent European Union authority that contributes to safeguarding the stability of the EU's financial system by enhancing the protection of investors and promoting stable and orderly financial markets. ESMA aims to promote supervisory convergence across the financial sector and works closely with the European Banking Authority and the European Insurance and Occupational Pensions Authority.

https://www.esma.europa.eu/

Electronic Transaction Development Agency

ETDA

The Information Security Standard for Meeting Control Systems, prescribed by the Thai Ministry of Digital Economy and Society (MDES), is a guideline for providers of meeting control systems (like Google Meet) to establish reliability of the meeting systems, in compliance with MDES' notification Re: Security Standards of Meetings via Electronic Means, B.E. 2563. Certification against B.E. 2563 is awarded by the Electronic Transaction Development Agency (ETDA).

https://www.mdes.go.th/

EU Cloud Code of Conduct

EU Cloud Code of Conduct

The EU Cloud Code of Conduct (CoC) was designed to contribute to an environment of trust and transparency in the European cloud computing market and to simplify the risk assessment process of Cloud Service Providers (CSPs) for cloud customers.

The CoC was developed by Scope Europe, an independent third party association, in collaboration with several industry players.

https://eucoc.cloud/

European Union Model Clauses

EU Model Contract Clauses

in 2010, the European Commission approved model contract clauses as a means of complying with the requirements of the EU Data Protection Directive, which in May 2018 was replaced by the General Data Protection Regulation (GDPR). Model contract clauses can be used between Google and its customers to ensure personal data leaving European Economic Area is transferred in accordance with the GDPR.

https://docs.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses#european-union-model-clauses-overview

Federal Deposit Insurance Corporation

FDIC

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the United States Congress to maintain stability and public confidence in the United State's financial system. The FDIC examines and supervises financial institutions for safety and soundness of their third-party engagements. The FDIC's Financial Institution Letter 44-2008 on Guidance for Managing Third-Party Risk (FDIC Guidance) provides financial institutions with information and guidance on identifying and managing risks associated with outsourced service providers.

https://www.fdic.gov/

Federal Reserve System

FED

The Federal Reserve System (Federal Reserve) is the central bank of the United States. It promotes the safety and soundness of individual financial institutions and monitors their impact on the financial system as a whole. The Board of Governors of the Federal Reserve System issued guidance on managing outsourcing risk ("Federal Reserve Guidance") to help financial institutions conduct a risk assessment of outsourced service providers.

https://www.federalreserve.gov/

Federal Risk and Authorization Management Program

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a US government program designed to provide a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. US federal agencies are directed by the Office of Management and Budget (OMB) to leverage FedRAMP to ensure security is in place when accessing cloud products and services.

FedRAMP uses the National Institute of Standards and Technology (NIST) Special Publication 800-53, which provides a catalog of security controls for all US federal information systems. FedRAMP requires cloud service providers (CSPs) to receive an independent security review performed by a third-party assessment organization (3PAO) to ensure authorizations are compliant with the Federal Information Security Management Act (FISMA).

https://www.fedramp.gov/

Federal Emergency Management Agency

FEMA

The mission of the Federal Emergency Management Agency (FEMA) is to support our citizens and first responders to ensure that, as a Nation, we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

https://www.fema.gov

Federal Emergency Management Agency - Flood Zones

FEMA - Flood Zones

Flood hazard areas identified on the Flood Insurance Rate Map are identified as a Special Flood Hazard Area (SFHA). SFHA are defined as the area that will be inundated by the flood event having a 1-percent chance of being equaled or exceeded in any given year. The 1-percent annual chance flood is also referred to as the base flood or 100-year flood. SFHAs are labeled as Zone A, Zone AO, Zone AH, Zones A1-A30, Zone AE, Zone A99, Zone AR, Zone AR/AE, Zone AR/AO, Zone AR/A1-A30, Zone AR/A, Zone V, Zone VE, and Zones V1-V30. Moderate flood hazard areas, labeled Zone B or Zone X (shaded) are also shown on the FIRM, and are the areas between the limits of the base flood and the 0.2-percent-annual-chance (or 500-year) flood. The areas of minimal flood hazard, which are the areas outside the SFHA and higher than the elevation of the 0.2-percent-annual-chance flood, are labeled Zone C or Zone X (unshaded).

https://www.fema.gov/glossary/flood-zones

The Family Educational Rights and Privacy Act

FERPA

Student educational records are protected under FERPA (The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99). This federal law applies to any school with certain programs funded by the U.S. Department of Education.

More than 140 million students and faculty rely on Google Workspace for Education. Google Workspace for Education can be used in compliance with FERPA, our commitment to which is included in our agreements.

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

The Family Educational Rights and Privacy Act

FERPA

Student educational records are protected under FERPA (The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99). This federal law applies to any school with certain programs funded by the U.S. Department of Education.

More than 140 million students and faculty rely on Google Workspace for Education. Google Workspace for Education can be used in compliance with FERPA, our commitment to which is included in our agreements.

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Federal Financial Institutions Examination Council

FFIEC

The Federal Financial Institutions Examination Council ("FFIEC") is a United States interagency body that prescribes principles and standards for oversight of financial institutions by United States regulators. The Outsourcing Technology Services Booklet ("FFIEC Booklet") provides guidance to assist examiners in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships. The FFIEC Booklet addresses financial institutions' responsibility to manage the risks associated with outsourced IT services, including due diligence, contract issues and ongoing monitoring.

https://www.ffiec.gov/

Financial Conduct Authority

FG16/5 – FCA

The Financial Conduct Authority ("FCA") is responsible for regulating the conduct of financial services firms and financial markets in the United Kingdom, in addition to being a prudential supervisor and setting standards for the firms it regulates. The FG16/5 Guidance for firms outsourcing to the cloud and other third-party IT services ("FG16/5") clarifies the requirements on regulated firms when outsourcing to the cloud and other third party IT services. FG 16/5 provides specific guidance on: risk management, due diligence, monitoring and oversight, data security, audit and effective access to data, continuity and business planning.

https://www.fca.org.uk/

Swiss Financial Market Supervisory Authority

FINMA

The Swiss Financial Market Supervisory Authority ("FINMA") is responsible for inspection and supervision of banks, insurance companies, financial institutions, collective investment schemes, fund managers and insurance intermediaries. FINMA is responsible for protecting creditors, investors and policyholders in addition to ensuring that Switzerland's financial markets function effectively.

https://www.finma.ch/en/

Federal Information Processing Standard Publication 140-2 (FIPS 140-2)

FIPS 140

The Federal Information Processing Standard Publication 140-2 (FIPS 140-2) is a US government security standard published by the National Institute of Standards and Technology (NIST) that specifies the security requirements related to the design and implementation of cryptographic modules protecting sensitive data.

nist.gov

Federal Information Processing - Standard Publication 140-2 (FIPS 140-2)

FIPS 140-2

The Federal Information Processing Standard Publication 140-2 (FIPS 140-2) is a US government security standard published by the National Institute of Standards and Technology (NIST) that specifies the security requirements related to the design and implementation of cryptographic modules protecting sensitive data.

nist.gov

Federal Information Processing Standard - Publication 140-2 Validated

FIPS 140-2 Validated

The National Institute of Standards and Technology (NIST) developed the Federal Information Processing Standard (FIPS) Publication 140-2 as a security standard that sets forth requirements for cryptographic modules, including hardware, software, and/or firmware, for U.S. federal agencies. FIPS 140-2 Validated certification was established to aid in the protection of digitally stored unclassified, yet sensitive, information. Google Cloud Platform uses a FIPS 140-2 validated encryption module called BoringCrypto (certificate 3318) in our production environment. This means that both data in transit to the customer and between data centers, and data at rest are encrypted using FIPS 140-2 validated encryption. The module that achieved FIPS 140-2 validation is part of our BoringSSL library.

nist.gov

Financial Industry Information Systems

FISC

The Center for Financial Industry Information Systems established the "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions" as security guidelines for financial institutions in Japan. It describes controls and security measures related to facilities, operations and technical infrastructure.

https://www.fisc.or.jp/english/

Financial Supervisory Commission - Insurance Outsourcing Directions

FSC Insurance Outsourcing Directions

The Financial Supervisory Commission ("FSC") is responsible for the inspection and supervision of banks, insurance enterprises and financial institutions in Taiwan with the objective of improving business operations, maintaining financial stability, and promoting the development of financial markets. The FSC Directions for Operation Outsourcing by Insurance Enterprises ("Insurance Outsourcing Directions") have been developed with the key objectives of safeguarding the interests of consumers and regulating the outsourcing operations of insurance enterprises. The Insurance Outsourcing Directions provide specific guidance on continuity, monitoring the outsourcing agreement, sub-outsourcing, audit, access and information rights.

https://www.fsc.gov.tw/en/

Federal Information Security Management Act

FISMA

The Federal Information Security Modernization Act of 2014 (FISMA 2014) updates the Federal Government's cybersecurity practices by: Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; Amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting.

https://www.cisa.gov/federal-information-security-modernization-act

Federal Information Security Management Act

FISMA NIST SP 800-53

Note that NIST Special Publications 800-53, 800-53A, and 800-53B contain additional background, scoping, and implementation guidance in addition to the controls, assessment procedures, and baselines. This NIST SP 800-53 database represents the controls defined in NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations. Derivative data formats of the forthcoming SP 800-53A, Revision 5 controls will be available when the publication is finalized (anticipated by early 2022). If there are any discrepancies noted in the content between this NIST SP 800-53 database and the latest published NIST SP 800-53 Revision 5 and NIST SP 800-53B, please contact sec-cert@nist.gov and refer to the official published documents as the normative source.

https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53

Danish Financial Supervisory Authority

FSA

The Danish Financial Supervisory Authority or Finanstilsynet, (“Danish FSA”) is the financial regulatory authority responsible for the supervision of financial undertakings (banks, mortgage-credit institutions, pension and insurance companies etc) in Denmark. The Danish FSA monitors the activities of financial undertakings to ensure they manage their risk.

https://www.dfsa.dk/

Korean Financial Services Commission

FSC

The Financial Services Commission (FSC), formerly Financial Supervisory Commission, is South Korean government's top financial regulator. It makes financial policies, and directs the Financial Supervisory Service. The Financial Supervisory Commission was established in 1998. With the start of Lee Myung-bak administration, the Commission was rearranged into the Financial Services Commission; the new one took over the policy-making authority from the Finance Ministry. As part of social responsibility, in 2014 the FSC Chairman Shin Je-yoo made plans to regulate the degree of innovativeness of banks requiring them to make the public the wages employees and executives in comparison to overall profit. This part of measured to encourage financial banks to create more value and jobs with an innovative management. It will see whether the banks are financing enough promising tech firms for going conservative practices and filling their social responsibility.

https://www.fsc.go.kr/

Financial Supervisory Commission - Banking Outsourcing Regulations

FSC Banking Outsourcing Regulations

The Financial Supervisory Commission ("FSC") is responsible for the inspection and supervision of banks, insurance enterprises and financial institutions in Taiwan with the objective of improving business operations, maintaining financial stability, and promoting the development of financial markets. The FSC Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation ("Banking Outsourcing Regulations") have been developed to assist banks in meeting their legal obligations under the Banking Act to protect customer rights and provide guidance on how to manage risk effectively when outsourcing to third parties. The Banking Outsourcing Regulations provide specific guidance on continuity, monitoring the outsourcing agreement, sub-outsourcing, audit, access and information rights.

https://www.fsc.gov.tw/en/

Financial Industry Information Systems

FISC

The Center for Financial Industry Information Systems established the "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions" as security guidelines for financial institutions in Japan. It describes controls and security measures related to facilities, operations and technical infrastructure.

https://www.fisc.or.jp/english/

General Data Protection Regulation

GDPR

The General Data Protection Regulation (GDPR) is a privacy legislation that replaced the 95/46/EC Directive on Data Protection of 24 October 1995 on May 25, 2018. GDPR lays out specific requirements for businesses and organizations who are established in Europe or who serve users in Europe. It: Regulates how businesses can collect, use, and store personal data Builds upon current documentation and reporting requirements to increase accountability Authorizes fines on businesses who fail to meet its requirements

https://eur-lex.europa.eu/eli/reg/2016/679/oj

Electronic Based Government System Presidential Regulation No. 95 of 2018 GR 95/2018 guidelines

GR 95/2018 Guidelines

The Electronic Based Government System ("SPBE") is a government administration in Indonesia that leverages information technology to provide public services to businesses and government agencies. SPBE's goal is to ensure governance around public services are in place to safeguard the public. The Presidential Regulation No. 95 of 2018 ("GR 95/2018 guidelines") is responsible for providing guidance to government agencies and businesses to implement online governance tools used for public services. The GR 95/2018 guidelines provide specific guidance on: risk management, information security, data management, technology asset management, audit rights and confidential information for regulated entities.

https://spbe.go.id/tentang

GxP

GxP

In the life sciences industry, GxP is an abbreviation referencing the various "good practice" regulations and guidelines that apply to organisations that manufacture products that are consumed or used by humans or animals. This includes medical, cosmetic, tobacco, products or devices and food products. The "x" variable in GxP covers a wide range of processes utilized in the development, manufacturing, and distribution of regulated products such as Good Manufacturing Practices (GMP), Good Clinical Practices (GCP), Good Laboratory Practices (GLP), Good Storage Practices (GSP), etc.

http://www.ispe.org/gamp-good-practice-guide/gxp-compliant-laboratory-computerized-systems

HDA Asset Management

HDA/HADS

As it owns attractive and specific perspectives, the hospitality industry requires specific expertise to succeed. Founded by hoteliers, HDA Asset Management is developing a full range of tailor-made services to support all phases of the investment strategy of its partners: hotels, institutional, fund manager and private wealth. From support to investment up to operational management, this offer benefits from the business expertise and international experience of HDA Asset Management executives. Our mission is to support our clients throughout their projects in order to comply with the objectives that we will have set together.

https://www.hda-am.com/

Hébergeur de Données de Santé

HDS

Hébergeur de Données de Santé (HDS) is a formal certification required by French laws. It is required for any commercial organizations who control, store, process, or transmit personally identifiable healthcare information in France. For more informatio

https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante

Higher Education Cloud Vendor Assessment Toolkit

Higher Education Cloud Vendor Assessment Tool (HECVAT)

The higher education information security community, EDUCAUSE, Internet2, and the Research & Education Networks Information Sharing & Analysis Center (REN-ISAC) created the Higher Education Cloud Vendor Assessment Toolkit (HECVAT), a self-assessment that attempts to standardize higher education information security and data protection requirements around cloud service providers. The assessment helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, and allows a consistent, easily-adopted methodology for those who want to use cloud services.

Google Cloud has completed a HECVAT self-assessment for GCP and for Google Workspace. These assessments detail our compliance with industry standards and the security protocols built into our infrastructure.

https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

Health Information Trust Alliance (HITRUST) - Common Security Framework (CSF)

HIGHTRUST CSF

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network and process security measures are in place and followed. This includes: covered entities (CE); all treatment providers; healthcare payment and operations; business associates; personnel with access to patient information to provide support in treatment, payment or operations. Subcontractors and business associates must also follow HIPAA compliance.

https://hitrustalliance.net/

Health Insurance Portability and Accountability Act

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network and process security measures are in place and followed. This includes: covered entities (CE); all treatment providers; healthcare payment and operations; business associates; personnel with access to patient information to provide support in treatment, payment or operations. Subcontractors and business associates must also follow HIPAA compliance.

https://www.hhs.gov/hipaa/for-professionals/index.html

Health Information Technology for Economic and Clinical Health

HITECH

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations issued under HIPAA are a set of U.S. healthcare laws that establish requirements for the use, disclosure, and safeguarding of individually identifiable health information. The scope of HIPAA was extended with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. HIPAA applies to covered entities (specifically, health care providers, health plans, and health care clearinghouses) that create, receive, maintain, transmit, or access patients' protected health information (PHI). HIPAA further applies to business associates of covered entities that perform certain functions or activities involving PHI as part of providing services to the covered entity or on behalf of the covered entity.

https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

HITRUST

HITRUST

Assembling and maintaining all of the components of risk management and compliance programs comes with unique challenges. HITRUST understands and has built an integrated approach to solving these problems with components that are aligned, maintained, and comprehensive to support your organization's goals.

https://hitrustalliance.net/

Health Information Trust Alliance (HITRUST) - Common Security Framework (CSF)

HITRUST CSF

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network and process security measures are in place and followed. This includes: covered entities (CE); all treatment providers; healthcare payment and operations; business associates; personnel with access to patient information to provide support in treatment, payment or operations. Subcontractors and business associates must also follow HIPAA compliance.

https://hitrustalliance.net/

Hong Kong Monetary Authority

HKMA

The Hong Kong Monetary Authority (HKMA) is the central banking institution in Hong Kong. It is responsible for supervising authorized institutions (AIs) with the aim of promoting stability and integrity of the financial system, including the banking system. HKMA Outsourcing SA-2 outlines the HKMA's supervisory approach to outsourcing and the recommendations for AIs to address when outsourcing to third parties.. HKMA Outsourcing SA-2 provides specific guidance on outsourcing agreements, customer data confidentiality, control over outsourced activities, contingency planning, access to outsourced data and overseas outsourcing.

https://www.hkma.gov.hk/

Hong Kong Insurance Authority

IA

The Hong Kong Insurance Authority (""HKIA"") regulates and supervises authorized insurers in Hong Kong and looks to promote the general stability of the insurance industry, while also protecting policyholders.

The GL14 Guideline on Outsourcing (""HKIA Outsourcing GL-14"") outlines the HKIA's expectations from authorized insurers when formulating and monitoring its outsourcing arrangements to account for the protection of its existing and potential policyholders. HKIA Outsourcing GL-14 provides specific guidance on the contents of the outsourcing agreement, due diligence, confidentiality, monitoring and controlling outsourced activities, contingency planning, overseas outsourcing and subcontracting.

https://www.ia.org.hk/

Department of Defense (DoD) Impact Level 4 (IL4)

Impact Level 4 (IL4) (Beta)

The United States Defense Information Systems Agency (DISA) manages the evaluation and authorization of cloud services for the U.S. Department of Defense (DoD). Provisional authorization at Impact Level 4 (IL4) allows storage or hosting of controlled, unclassified information as defined by the Cloud Computing Security Requirements Guide. Google's DISA IL4 authorization for Google Cloud Platform is currently in process. Google Cloud Platform is able to provide IL4 compatible personnel and U.S. data residency controls for certain Google Cloud Platform products and services through Assured Workloads for Government.

https://dl.dod.cyber.mil/wp-content/uploads/cloud/SRG/index.html

Independent Security Evaluators

Independent Security Evaluators (ISE) Audit

The Independent Security Evaluators (ISE) is an independent third party dedicated to ensuring the overall security posture and protection of digital assets for global enterprises. One of the audits conducted by ISE includes a security audit of cloud platforms specifically tailored for the media industry. The audit focuses on high value workloads and demonstrates to a media organization that a cloud provider provides effective security capabilities aligned to specific industry standards and requirements.

https://www.ise.io/

Indonesia Government Regulation

Indonesia Government Regulation No. 71 (GR 71)

Indonesia's Government Regulation No. 71 of 2019 regarding Operation of Electronic System and Transactions ("GR 71") regulates the activities of Electronic System Operators (ESOs), generally defined as any person, government administrator, business entity, or member of society that provides, administers, and/or operates an electronic system individually or collectively for users. As of October 10, 2019, GR 71 amends Indonesia's previous Government Regulation No. 82 of 2012 to provide more clarity around data localization requirements, including additional flexibility for private-sector ESOs to store systems and data outside Indonesia, subject to certain restrictions. GR 71 also includes registration requirements for ESOs, general data protection and security requirements, erasure and delisting rights for data owners, and content prohibitions, among other requirements

https://siplawfirm.id/key-points-of-government-regulation-no-71-of-2019-on-organization-of-electronic-systems-and-transactions/

Information System Security Management and Assessment Program

Information System Security Management and Assessment Program (ISMAP)

The Information System Security Management and Assessment Program (ISMAP) is a Japanese government system for assessing the security of cloud service providers to participate in public sector projects. It is operated jointly by The National Center of Incident Readiness and Strategy for Cybersecurity (NISC), The National Strategy office of Information and Communications Technology, The Ministry of Internal Affairs and Communications (MIC) as well as The Ministry of Economy, Trade and Industry (METI). The Information-technology Promotion Agency (IPA), an independent administrative agency, provides practical technical support for the system. Google Cloud was successfully assessed for ISMAP compliance and subsequently registered as an ISMAP compliant Cloud Service Provider. Our registration can be seen at the Information Technology Promotion Agency (IPA) website.

https://aws.amazon.com/compliance/ismap/

Internal Revenue Service - 1075

IRS 1075

The Internal Revenue Service (IRS), is a bureau of the U.S. Department of Treasury that is the U.S. tax collection agency and administers the Internal Revenue Code . To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure.

https://www.irs.gov/privacy-disclosure/safeguards-program

Information Security Registered Assessors Program

IRAP

The Information Security Registered Assessors Program (IRAP) is an Australian Signals Directorate (ASD) initiative. IRAP is the assessors' program developed by the Australian government Cyber Security Centre (ASD/ACSC) for assessing cloud services for government and non-government agency use. It is intended "to provide the framework to endorse individuals from the private and public sectors to provide cyber security assessment services to Australian governments.

https://www.cyber.gov.au/acsc/view-all-content/programs/irap

International Standard on Assurance Engagements - 3000 Type 2 Report (FINMA)

ISAE 3000 Type 2 Report (FINMA)

The International Standard on Assurance Engagements (ISAE) 3000 is a standard which is applied for audits of internal controls, sustainability and compliance with -laws and regulations. The ISAE 3000 Type 2 Report is a self-assessment which is then audited by an independent third party, and provides assurance on the suitability of the design and existence of controls over a period of time. This report verifies the effectiveness of Google's internal controls to support adherence to certain FINMA (the Swiss Financial Market Supervisory Authority) requirements applicable to regulated financial services customers. The report covers the requirements of the following FINMA Circulars.

https://aws.amazon.com/blogs/security/aws-publishes-finma-isae-3000-type-2-attestation-report-for-the-swiss-financial-industry/

International Standard on Assurance Engagements - 3402

ISAE 3402

International Standard on Assurance Engagements 3402 (ISAE 3402), titled Assurance Reports on Controls at a Service Organization, is an international assurance standard that describes Service Organization Control (SOC) engagements, which provides assurance to an organization's customer that the service organization has adequate internal controls.[1] ISAE 3402 was developed by the International Auditing and Assurance Standards Board (IAASB) and published by the International Federation of Accountants (IFAC) in 2009. It supersedes SAS 70. and puts more emphasis on procedures for the ongoing monitoring and evaluation of controls.

https://www.isae3402.com/

International Standards for Assurance Engagements -3402 Type II

ISAE 3402 Type II

One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2012). A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2012 to June 30, 2012). The contents of each type of report is described in the following table:

https://www.isae3402.com/ISAE3402_reports.html

Korea - Information Security Management System

ISMS (Formerly K-ISMS)

The Korea Information Security Management System ("K-ISMS") is an information security management standard operated by Korea Internet & Security Agency ("KISA"). K-ISMS was prepared to evaluate whether enterprises and organizations operate and manage their information security management system (ISMS) consistently and securely such that they protect key information assets from various threats. The legal background for K-ISMS is provided in Article 47 of the Act on Promotion of Information and Communication Network Utilization and Information Protection (Certification of ISMS).

https://isms.kisa.or.kr/

International Organization for Standardization

ISO

The International Organization for Standardization (ISO /aɪ ɛs oʊ/) is an international standard-setting body composed of representatives from various national standards organizations.

https://www.iso.org/

International Organization for Standardization - Environmental Management System

ISO 14001

ISO 14001 sets out the criteria for an environmental management system and can be certified to. It maps out a framework that a company or organization can follow to set up an effective environmental management system.

Designed for any type of organization, regardless of its activity or sector, it can provide assurance to company management and employees as well as external stakeholders that environmental impact is being measured and improved.

https://www.iso.org/iso-14001-environmental-management.html

ISO/IEC 20000-1: Service Management Systems

ISO 2000-1

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) drafted the internationally recognized ISO/IEC 20000-1 service management system (SMS) standard. It is intended to help design, transition, deliver and improve services to fulfil agreed service requirements. For more information.

https://www.iso.org/standard/51986.html

ISO/IEC 22301:2019 Security and resilience - Business Continuity Management Systems

ISO 22301

This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. This document is applicable to all types and sizes of organizations that: a) implement, maintain and improve a BCMS; b) seek to ensure conformity with stated business continuity policy; c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption; d) seek to enhance their resilience through the effective application of the BCMS. This document can be used to assess an organization's ability to meet its own business continuity needs and obligations.

https://www.iso.org/standard/75106.html

ISO/IEC 27001: Information Security Management Systems

ISO 27001

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) drafted the internationally recognized ISO/IEC 27001 Standard. It is intended to provide guidance for establishment and continuous improvement of an information security management system (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

https://www.iso.org/isoiec-27001-information-security.html

ISO 45000: Family - Occupational Health and Safety

ISO 45001

According to the International Labour Organization, more than 7 600 people die from work-related accidents or diseases every single day. That's why an ISO committee of occupational health & safety experts set to work to develop an International Standard with the potential to save almost three million lives each year. Structured in a similar way to other ISO management systems, the approach will be familiar to users of standards such as ISO 14001 or ISO 9001. ISO 45001 builds on the success of earlier international standards in this area such as OHSAS 18001, the International Labour Organization's ILO-OSH Guidelines, various national standards and the ILO's international labour standards and conventions.

https://www.iso.org/iso-45001-occupational-health-and-safety.html

ISO 50001: Energy Management

ISO 50001

ISO 50001 is based on the management system model of continual improvement also used for other well-known standards such as ISO 9001 or ISO 14001. This makes it easier for organizations to integrate energy management into their overall efforts to improve quality and environmental management. For organizations committed to addressing their impact, conserving resources and improving the bottom line through efficient energy management, we developed ISO 50001.

Designed to support organizations in all sectors, this ISO standard provides a practical way to improve energy use, through the development of an energy management system (EnMS).

https://www.iso.org/iso-50001-energy-management.html

ISO 9000: Family - Quality Management

ISO 9000

For organizations asking how to improve the quality of their products and services and consistently meet their customers' expectations, ISO has an answer. Addressing various aspects of quality management and containing some of ISO's best-known standards, there's the ISO 9000 family.

https://www.iso.org/iso-9001-quality-management.html

ISO 9001: Quality Management Systems

ISO 9001

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) form the specialized system for worldwide standardization. The ISO 9001 standard family is based on a number of quality management principles including a strong customer focus. It is intended "to help organizations demonstrate its ability to consistently provide customers good quality products and services.

https://www.iso.org/iso-9001-quality-management.html

ISO 9001: Quality Management Systems - Requirements

ISO 9001: 2015

ISO 9001:2015 specifies requirements for a quality management system when an organization: a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements. All the requirements of ISO 9001:2015 are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.

https://www.iso.org/standard/62085.html

ISO/IEC 20000-1: Service Management Systems

ISO/IEC 20000-1

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) drafted the internationally recognized ISO/IEC 20000-1 service management system (SMS) standard. It is intended to help design, transition, deliver and improve services to fulfil agreed service requirements. For more information.

https://www.iso.org/standard/51986.html

ISO/IEC 27000:2018 Information Technology - Security Techniques - Information Security Management Systems

ISO/IEC 27000

ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations). The terms and definitions provided in this document - cover commonly used terms and definitions in the ISMS family of standards; - do not cover all terms and definitions applied within the ISMS family of standards; and - do not limit the ISMS family of standards in defining new terms for use.

https://www.iso.org/ru/standard/73906.html

ISO/IEC 27018: Personal Information Protection Controls

ISO/IEC 27018

ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

https://www.iso.org/standard/76559.html

ISO/IEC 27002: 2013 Information Technology - Security Techniques

ISO/IEC 270717

The International Organization for Standardization (ISO) is an independent, non-governmental organization with an international membership of 163 national standards bodies. The ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: Additional implementation guidance for relevant controls specified in ISO/IEC 27002 Additional controls with implementation guidance that specifically relate to cloud services This standard provides controls and implementation guidance for both cloud service providers like Google and our cloud service customers. ISO/IEC 27017 provides cloud-based guidance on 37 ISO/IEC 27002 controls, along with seven new cloud controls that address.

https://www.iso.org/standard/54533.html

ISO/IEC 27701: Privacy Information Management

ISO/IEC 27701

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing. This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

https://www.iso.org/standard/71670.html

IT Infrastructure Library - Compliant Reporting

ITIL Compliant Reporting

ITIL stands for Information Technology Infrastructure Library. The acronym was first used in the 1980s by the British government's Central Computer and Telecommunications Agency (CCTA) when it documented dozens of best practices in IT service management and printed them for distribution. Today, ITIL no longer refers to "Information Technology Infrastructure Library"—instead, it is a standalone term.

https://www.ibm.com/cloud/learn/it-infrastructure-library

Korea - Information Security Management System

K-ISMS

The Korea Information Security Management System ("K-ISMS") is an information security management standard operated by Korea Internet & Security Agency ("KISA"). K-ISMS was prepared to evaluate whether enterprises and organizations operate and manage their information security management system (ISMS) consistently and securely such that they protect key information assets from various threats. The legal background for K-ISMS is provided in Article 47 of the Act on Promotion of Information and Communication Network Utilization and Information Protection (Certification of ISMS).

https://isms.kisa.or.kr/

Polish Financial Supervision Authority

KNF

The Polish Financial Supervision Authority (the "KNF") is responsible for the supervision of the financial markets to ensure its proper functioning, security, and transparency in addition to protecting the interests of market participants. The Communication of 23 January 2020 from the KNF on information processing by supervised entities using public or hybrid cloud computing services (the "framework") addresses how supervised entities subject to financial market supervision by the KNF should assess cloud services to minimize operational risk. The framework provides specific guidance on the minimum requirements for cloud-based information processing, including the agreement with the cloud service provider, requirements for cloud service providers, cryptography, and monitoring information processing in the cloud computing environment.

https://www.knf.gov.pl/

Know Your Third Party (KY3P) Report

KY3P

KY3P (Know Your Third Party) by IHS Markit produces a report that serves as an assessment of Google Cloud's activities across numerous risk domains such as information security, compliance, privacy, physical security, technology management, financial health, and people security. It aligns with NIST, ISO, CSA, and many other cross-industry standards and regulations.

https://ihsmarkit.com/products/ky3p.html

Leadership in Energy and Environmental Design

LEED

Leadership in Energy and Environmental Design (LEED) is a green building certification program used worldwide.[9] Developed by the non-profit U.S. Green Building Council (USGBC), it includes a set of rating systems for the design, construction, operation, and maintenance of green buildings, homes, and neighborhoods, which aims to help building owners and operators be environmentally responsible and use resources efficiently. By 2015, there were over 80,000 LEED-certified buildings and over 100,000 LEED-accredited professionals. Most LEED-certified buildings are located in major U.S. metropolises. LEED Canada has developed a separate rating system for the regulations and climate of that country.

https://www.usgbc.org/leed

Leadership in Energy and Environmental Design - Certified

LEED Certified

LEED is a certification system that deals with the environmental performance of buildings based on overall characteristics of the project. We do not award credits based on the use of particular products but rather upon meeting the performance standards set forth in our rating systems. It is up to project teams to determine which products are most appropriate for credit achievement and program requirements.

https://www.usgbc.org/leed

Leadership in Energy and Environmental Design - Gold

LEED Gold

Leadership in Energy and Environmental Design (LEED) is a green building certification program used worldwide.[9] Developed by the non-profit U.S. Green Building Council (USGBC), it includes a set of rating systems for the design, construction, operation, and maintenance of green buildings, homes, and neighborhoods, which aims to help building owners and operators be environmentally responsible and use resources efficiently. By 2015, there were over 80,000 LEED-certified buildings and over 100,000 LEED-accredited professionals. Most LEED-certified buildings are located in major U.S. metropolises. LEED Canada has developed a separate rating system for the regulations and climate of that country.

https://www.usgbc.org/leed

Leadership in Energy and Environmental Design - Platinum

LEED Platinum

Leadership in Energy and Environmental Design (LEED) is a green building certification program used worldwide.[9] Developed by the non-profit U.S. Green Building Council (USGBC), it includes a set of rating systems for the design, construction, operation, and maintenance of green buildings, homes, and neighborhoods, which aims to help building owners and operators be environmentally responsible and use resources efficiently. By 2015, there were over 80,000 LEED-certified buildings and over 100,000 LEED-accredited professionals. Most LEED-certified buildings are located in major U.S. metropolises. LEED Canada has developed a separate rating system for the regulations and climate of that country.

https://www.usgbc.org/leed

Leadership in Energy and Environmental Design - Silver

LEED Silver

Leadership in Energy and Environmental Design (LEED) is a green building certification program used worldwide.[9] Developed by the non-profit U.S. Green Building Council (USGBC), it includes a set of rating systems for the design, construction, operation, and maintenance of green buildings, homes, and neighborhoods, which aims to help building owners and operators be environmentally responsible and use resources efficiently. By 2015, there were over 80,000 LEED-certified buildings and over 100,000 LEED-accredited professionals. Most LEED-certified buildings are located in major U.S. metropolises. LEED Canada has developed a separate rating system for the regulations and climate of that country.

https://www.usgbc.org/leed

Lei Geral de Proteção de Dados Pessoais

LGPD

The General Personal Data Protection Law (Brazil) 13709/2018 (Portuguese: Lei Geral de Proteção de Dados Pessoais, or LGPD), is a statutory law on data protection and privacy in the Federative Republic of Brazil. The law's primary aim is to unify 40 different Brazilian laws that regulate the processing of personal data.[1] The LGPD contains provisions and requirements related to the processing of personal data of individuals, where the data is of individuals located in Brazil, where the data is collected or processed in Brazil, or where the data is used to offer goods or services to individuals in Brazil.[2] The LGPD became law on September 18, 2020 but its enforceability was backdated August 16, 2020. Sanctions under the regulation will only be applied from August 1, 2021.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Malaysian Administrative Modernisation and Management Planning Unit

MAMPU

The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU; Malay: Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia) is one of the prominent (MAMPU Portal, Malaysia) government agencies in Malaysia, that is responsible for 'modernising and reforming' the public sector.

https://www.mampu.gov.my/en/

MaRisk AT 9 Outsourcing

MaRisk AT 9 Outsourcing

The Bundesanstalt für Finanzdienstleistungsaufsicht ("BaFin") is responsible for the supervision of all banks, credit institutions, insurers, funds and financial institutions in Germany. Its objective is to ensure the functioning, stability and integrity of the German financial market. Article 9 of the Minimum Requirements for Risk Management (MaRisk AT 9 Outsourcing) provides guidance on how financial institutions can meet the outsourcing requirements in section 25b of the German Banking Act (Kreditwesengesetz). According to this section of the German Banking Act, financial institutions should take reasonable precautionary measures to avoid risk when outsourcing activities.

https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2018/meldung_181015_veroeffentlichung_marisk_englisch_en.html

The Monetary Authority of Singapore Act

MAS

An Act to establish a corporation to be known as the Monetary Authority of Singapore, to provide for the exercise of control over and the resolution of financial institutions and their related entities by the Monetary Authority of Singapore and other authorities, and to establish a framework for the issue of securities by the Monetary Authority of Singapore and the regulation of primary dealers of such securities, and for matters incidental thereto and connected therewith.

https://sso.agc.gov.sg/Act/MASA1970

MAS Technology Risk Management Guidelines

MAS TRM

With the rising numbers and scale of cyberattacks, the Monetary Authority of Singapore (MAS) revised its technology risk management (TRM) guidelines on January 18, 2021. The TRM guidelines apply to all FIs that MAS regulates, ranging from large ones like banks, insurers and exchanges to small ones like venture capital managers and payments services firms. The TRM guidelines address increased reliance on emerging technologies like cloud computing, application programming interfaces (APIs) and rapid software development and the fast-changing cyber threat landscape. We view the 2021 version as a "best practice framework" for FIs outlining governance practices and internal controls to pre-empt and address current risks that adopt most of the prior 2013 version as a base.

https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

Ministry of Electronics and Information Technology

MeitY

Mission of Ministry of Electronics and Information Technology : e-Development of India through multi pronged strategy of e-Infrastructure creation to facilitate and promote e-governance, promotion of Electronics & Information Technology- Information Technology Enabled Services (IT-ITeS) Industry, providing support for creation of Innovation / Research & Development (R&D), building Knowledge network and securing India's cyber space.

https://www.meity.gov.in/

Ministry of Electronics and Information Technology

MeitY

Mission of Ministry of Electronics and Information Technology : e-Development of India through multi pronged strategy of e-Infrastructure creation to facilitate and promote e-governance, promotion of Electronics & Information Technology- Information Technology Enabled Services (IT-ITeS) Industry, providing support for creation of Innovation / Research & Development (R&D), building Knowledge network and securing India's cyber space.

https://www.meity.gov.in/

Motion Picture Association - Content Security Best Practice Guidelines

MPA - Content Security

The Motion Picture Association (MPA) Content Security Best Practice Guidelines help cloud service providers and entertainment industry assess the security of entertainment content. Under a shared security model, customers who use Google Cloud can configure their cloud services to support MPA best practices. While not a formal certification, the controls map closely to Google's existing third-party audited core compliance programs, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 as well as our CSA STAR self-certification.

https://www.motionpictures.org/

Monetary Authority of Singapore

MSA

MAS is at the forefront of Singapore's rapidly growing financial industry, creating new policies and initiatives that address the ever-changing landscape. Work at MAS promises not only challenges worthy of your intellectual abilities, but also the personal satisfaction that comes from building one of Asia's premier financial hubs. We invite you to take up the challenge and make a difference to Singapore's economic and financial development! At MAS, we place a great emphasis on developing a vibrant and conducive work environment that motivates each and every employee to make a meaningful contribution to the organisation. Our people recognize the importance of upholding our values to achieve more together. We believe that it is essential that our people enjoy working here with one another. MAS' Functions - To act as the central bank of Singapore, including the conduct of monetary policy, the issuance of currency, the oversight of payment systems and serving as banker to and financial agent of the Government - To conduct integrated supervision of financial services and financial stability surveillance - To manage the official foreign reserves of Singapore - To develop Singapore as an international financial centresee less.

https://www.mas.gov.sg/

National Cyber Security Centre - Cyber Essentials

NCSC – Cyber Essentials

The Cyber Essentials certification was established by the National Cyber Security Centre (NCSC) in the UK to demonstrate that an organization has established safeguards to protect against the most common cyber threats. This certification is required in order to work for UK government agencies and the enterprises that serve them who handle sensitive and personal information or the provision of certain technical products and services.

https://www.ncsc.gov.uk/

Multi-Tier Cloud Security - Tier 3

MTCS Tier 3

The Multi-Tier Cloud Security (MTCS) Singapore Standard (SS)584 is a cloud security certification managed by the Singapore Info-comm Media Development Authority (IMDA). This standard's three tiers are designed to certify cloud service providers at different levels of operational security, with Tier 3 having the most stringent requirements.

After undergoing an audit conducted by an independent MTCS Certifying Body, Google Cloud received Tier 3 MTCS certification for a subset of GCP and Google Workspace services and data center sites.

https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Cloud-Computing-and-Services

National Cyber Security Centre

NCSC

The UK's National Cyber Security Centre (NCSC) offers a framework built around 14 Cloud Security Principles. These expansive principles apply to organizations in the UK's public sector and include important considerations such as protection of data in transit, supply chain security, identity and authentication, and secure use of cloud services. Google Cloud provides information (in the form of mappings for Google Cloud Platform and Google Workspace) on how our products and services align with these Cloud Security Principles.

https://www.ncsc.gov.uk/

Royal Netherlands Standardization Institute

NEN

The Royal Netherlands Standardization Institute (Nederlands Normalisatie Instituut or NEN) is a non-profit organization focused on developing standardization processes in the Netherlands. One of those standards is NEN 7510, an information security standard that provides guidelines for determining, establishing, and maintaining measures for health care organizations to protect and secure healthcare data.

https://www.nen.nl/en/

National Hurricane Center - National Oceanic and Atmospheric Administration - Category 2

NHC/NOAA (US) - Category 2

Extremely dangerous winds will cause extensive damage: Well-constructed frame homes could sustain major roof and siding damage. Many shallowly rooted trees will be snapped or uprooted and block numerous roads. Near-total power loss is expected with outages that could last from several days to weeks.

https://www.nhc.noaa.gov/aboutsshws.php

National Hurricane Center - National Oceanic and Atmospheric Administration - Category 1

NHC/NOAA (US) - Category 1

Very dangerous winds will produce some damage: Well-constructed frame homes could have damage to roof, shingles, vinyl siding and gutters. Large branches of trees will snap and shallowly rooted trees may be toppled. Extensive damage to power lines and poles likely will result in power outages that could last a few to several days.

https://www.nhc.noaa.gov/aboutsshws.php

National Hurricane Center - National Oceanic and Atmospheric Administration - Category 3

NHC/NOAA (US) - Category 3 (Major)

Devastating damage will occur: Well-built framed homes may incur major damage or removal of roof decking and gable ends. Many trees will be snapped or uprooted, blocking numerous roads. Electricity and water will be unavailable for several days to weeks after the storm passes.

https://www.nhc.noaa.gov/aboutsshws.php

National Hurricane Center - National Oceanic and Atmospheric Administration - Category 4

NHC/NOAA (US) - Category 4 (Major)

Catastrophic damage will occur: Well-built framed homes can sustain severe damage with loss of most of the roof structure and/or some exterior walls. Most trees will be snapped or uprooted and power poles downed. Fallen trees and power poles will isolate residential areas. Power outages will last weeks to possibly months. Most of the area will be uninhabitable for weeks or months.

https://www.nhc.noaa.gov/aboutsshws.php

National Hurricane Center - National Oceanic and Atmospheric Administration - Category 5

NHC/NOAA (US) - Category 5 (Major)

Catastrophic damage will occur: A high percentage of framed homes will be destroyed, with total roof failure and wall collapse. Fallen trees and power poles will isolate residential areas. Power outages will last for weeks to possibly months. Most of the area will be uninhabitable for weeks or months.

https://www.nhc.noaa.gov/aboutsshws.php

United Kingdom's National Health Service

NHS

The United Kingdom's National Health Service (NHS) Department of Health and Social Care Information Center policy mandates that all organizations that process NHS patient data and systems must provide assurances that they are practising good data security and that personal information is handled correctly. NHS Digital, a national public body in England, has developed the Data Security and Protection Toolkit (DSP Toolkit), an online self-assessment tool that allows organizations to assess themselves or be assessed against information governance policies and standards.

https://www.nhs.uk/

National Center of Incident Readiness and Strategy for Cybersecurity

NISC

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) is a Japanese government body that establishes standards for cybersecurity for government agencies. One of the documents NISC created for Japanese government and related agencies to outline steps that should be taken for the enhancement of information security is the "Common Standards for Information Security Measures for Government Agencies." In order to help customers understand how we support compliance with the NISC's common standards (2018 edition), we've created a NISC whitepaper. Third-party compliance programs such as ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 certifications map to many of the regulations described in the whitepaper.

https://www.nisc.go.jp/

National Institute of Standards and Technology

NIST

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

https://www.nist.gov/

National Institute of Standards and Technology - 800-171

NIST 800-171

The National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, creates standards and guidelines pertaining to information security. NIST's Special Publication 800-171 focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in non-federal information systems and organizations, and defines security requirements to achieve that objective. The security controls of NIST 800-171 can be mapped directly to NIST 800-53. This mapping is available on page D-2 of the publication NIST.SP.800-171.

https://www.nist.gov/

National Institute of Standards and Technology - 800-34

NIST 800-34 – Contingency Planning

The National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, creates standards and guidelines pertaining to information security. NIST developed Special Publication 800-34 (SP 800-34), Contingency Planning Guide for Federal Information Systems, to provide instructions and recommendations for information technology systems contingency planning.

https://www.nist.gov/

National Institute of Standards and Technology - 800-53

NIST 800-53

The National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, creates standards and guidelines pertaining to information security. NIST developed Special Publication 800-53 (NIST SP 800-53) to build on statutory responsibilities laid out in the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, which is a federal law that requires U.S. government agencies to create, review, and report on agency-wide practices that prioritize information security. NIST 800-53 mandates specific security and privacy controls required for federal government and critical infrastructure.

https://www.nist.gov/

National Institute of Standards and Technology - 800-53/FISMA

NIST-800-53/FISMA

The National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, creates standards and guidelines pertaining to information security. NIST developed Special Publication 800-53 (NIST SP 800-53) to build on statutory responsibilities laid out in the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, which is a federal law that requires U.S. government agencies to create, review, and report on agency-wide practices that prioritize information security. NIST 800-53 mandates specific security and privacy controls required for federal government and critical infrastructure.

https://www.nist.gov/

Office of the Comptroller of the Currency

OCC

The Office of the Comptroller of the Currency ("OCC") is an independent bureau of the United State Department of the Treasury that ensures that national banks and federal savings associations operate in a safe and sound manner. The OCC Bulletin 2013-29 Third-Party Relationship: Risk Management Guidance ("OCC Bulletin") provides guidance to banks for assessing and managing risks associated with outsourced service providers. The OCC Bulletin recommends risk management strategies for when banks outsource their banking functions, including in relation to due diligence, contract negotiation, ongoing monitoring and termination.

https://www.occ.gov/

Open Compute Project

OCP

The Open Compute Project Foundation (OCP) was initiated in 2011 with a mission to apply the benefits of open source and open collaboration to hardware and rapidly increase the pace of innovation in, near and around the data center. Now celebrating our 10th anniversary, just wait till you see what we have planned for the next ten years!

https://www.opencompute.org/

Otoritas Jasa Keuangan - Circular 21 of 2017

OJK Circular 21 of 2017 (SEOJK 21)

The Otoritas Jasa Keuangan ("OJK") is responsible for the inspection and supervision of activities in the banking, capital markets and financial services sectors in Indonesia. The OJK seeks to protect the interests of consumers, and promote prosperity and competition in the financial services industry. OJK Circular No. 21 of 2017, The Application of Risk Management in the Use of Information Technology by Commercial Banks ("SEOJK 21"), supplements the requirements in POJK 38 and provides guidance on how commercial banks can implement risk management effectively when outsourcing their information technology activities. SEOJK 21 provides specific guidance on the contents of the outsourcing agreement, due diligence, risk mitigation and the use of services outside of Indonesia.

https://www.ojk.go.id/

Otoritas Jasa Keuangan - No. 38 of 2016

OJK Regulation No. 38 of 2016 (POJK 38)

The Otoritas Jasa Keuangan ("OJK") is responsible for the inspection and supervision of activities in the banking, capital markets and financial services sectors in Indonesia. The OJK seeks to protect the interests of consumers, and promote prosperity and competition in the financial services industry. OJK Regulation No. 38 of 2016 The Application of Risk Management in the Use of Information Technology by Commercial Banks ("POJK 38") addresses how commercial banks can apply risk management effectively when outsourcing their information technology activities. POJK 38 provides specific guidance on the contents of the outsourcing agreement, due diligence, monitoring performance, contingency planning, audit and information access rights.

https://www.ojk.go.id/

Open-IX 1 Certified

Open-IX 1 Certified

Open-IX OIX-1 Certification is a best-in-class and first ever global certification for Internet Exchange Points. OIX-1 Certification sets a minimum level of service and engineering and was developed by the broad consensus of world-class IXP managers, engineers and their customers. OIX-1 Certification sets the Data Center and Network Operator, Interconnection Strategists and Peering Coordinator-defined standard for massive-scale interconnection, performance, resiliency and reliability for all networks that need to be able to efficiently interconnect networks.

https://open-ix.org/en/certification/ixp-oix-1/

Open-IX 2 Certified

Open-IX 2 Certified

Open-IX OIX-2 Certification is a best-in-class and first ever global certification for data centers desiring to serve as points of network interconnection. OIX-2 Certification sets a minimum level of service, SLA and engineering for data centers. OIX-2 was developed by the broad consensus of world-class data center managers, engineers and their customers. It sets the standard for massive-scale interconnection supporting facility performance, resiliency and reliability for all that need to be able to reliably interconnect networks.

https://open-ix.org/en/certification/dc-oix-2/

Office of the Superintendent of Financial Institutions Canada

OSFI

The Office of the Superintendent of Financial Institutions Canada ("OSFI") is responsible for regulating federally registered banks and insurers, trust and loan companies, as well as private pension plans in Canada. OFSI contributes to the safety and soundness of the Canadian financial system. The B-10 Outsourcing of Business Activities, Functions and Processes ("B-10 Guideline") addresses OSFI's expectations on regulated entities that outsource business activities to service providers, in particular the practices, procedures and standards that should be applied to the outsourcing arrangement. The B-10 Guideline provides specific guidance for regulated entities on: due diligence, contractual terms, data location, business continuity, outsourcing in foreign jurisdictions, monitoring and oversight.

https://www.osfi-bsif.gc.ca/

OSPAR

OSPAR

Financial Institutions (FIs) rely on the outsourced service providers to perform certain business functions. Loss of customer information or confidential data, or disruptions to critical bank services may result in reputational risk impacts or regulatory breaches. Outsourcing risks must be managed to safeguard the FIs' operations and customers. The Association of Banks in Singapore (ABS) has established these Guidelines on Control Objectives and Procedures for the FIs' Outsourced Service Providers (OSPs) operating in Singapore.

https://www.ospar.org/

Payment Card Industry

PCI

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. It is intended to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security practices globally. The PCI DSS standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI SSC).

https://www.pcisecuritystandards.org/

Payment Card Industry Data Security Standard

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. It is intended to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security practices globally. The PCI DSS standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI SSC).

https://www.pcisecuritystandards.org/

Payment Card Industry Data Security Standard

PCI DSS 3.2 Validation

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. It is intended to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security practices globally. The PCI DSS standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI SSC).

https://www.pcisecuritystandards.org/

Personal Data Protection Act 2012

PDPA

The Personal Data Protection Act 2012 (PDPA) is a data protection law administered and enforced by the Personal Data Protection Commission (PDPC). Singapore's PDPA governs the collection, use, disclosure, and care of personal data as described in the quick guide to the PDPA. At the center of the PDPA are the 9 main data protection obligations including consent, purpose limitation, notification, access and correction, accuracy, protection, retention, transfer, and openness.

https://www.pdpc.gov.sg/

Personal Data Protection Law

PDPL

The Personal Data Protection Law 25,326 (PDPL), Regulatory Decree 1558/2001, and other provisions issued by the National Directorate for Personal Data Protection comprise the current main legal framework of Argentine Data Protection Regulations. The PDPL outlines obligations and principles related to data processing, including on security and the transfer of data internationally between data controllers or data processors. As the PDPL only applies to reporting databases (PDPL, Section 1), we believe that the PDPL is not applicable to Google in connection with the provision of Google Cloud services.

https://www.ebv.com.ar/

PCI 3DS Core Security Standard

PIC 3DS Core Security Standard

The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. The Standards Council was established by the major credit card associations (Visa, MasterCard, American Express, Discover, JCB) as a separate organization to define appropriate practices that merchants and service providers should follow to protect cardholder data.

https://www.pcisecuritystandards.org/about_us/

Pharmaceuticals and Medical Devices Agency

PMDA

The Japanese Ministry of Health, Labour and Welfare formulated the "Guideline on Management of Computerized Systems for Validation for Marketing Authorization Holders and Manufacturers of Drugs and Quasi-drugs" standard to provide guidance for marketing authorization holders and manufacturers of drugs and quasi-drugs. In order to help customers understand how we support compliance with these guidelines, we've created a CSV Guidelines whitepaper as well as a CSV Guidelines Control mapping. Many of the regulations described in the whitepaper have been certified by third-party compliance programs, such as ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018.

https://www.pmda.go.jp/

Personal Information Protection Commission

PPC

The Personal Information Protection Commission (PPC) is a Japanese government commission primarily responsible for protecting the rights and interests of individuals, including considerations of the proper use of personal information.

https://www.ppc.go.jp/en/

Prudential Regulation Authority

PRA

The Prudential Regulation Authority ("PRA") is a part of the Bank of England and is responsible for prudential regulation in the UK. The PRA supervises banks, building societies, credit unions, insurers and major investment firms and looks to determine whether they are being run in a safe and sound manner.

https://www.bankofengland.co.uk/

Reserve Bank of India

RBI

The Reserve Bank of India ("RBI") is India's central bank and is responsible for the supervision of the Indian financial sector.

The Guidelines on Managing Risk and Code of Conduct in Outsourcing of Financial Services by banks ("RBI Guidelines on Outsourcing") address RBI's expectations for managing the risks in outsourcing. The RBI Guidelines on Outsourcing provide specific guidance on risk management practices for outsourced financial services and off-shore outsourcing of financial services.

https://www.rbi.org.in/

Revised Federal Data Protection Act

revFADP

The Swiss Parliament passed the final version of the revised Federal Data Protection Act (revFADP) in 2020. The revFDPA aims to protect the personality rights and the fundamental rights of natural persons whose personal data is processed and seeks to align the current Swiss Data Protection Law with the Council of Europe's Convention 108 and with the General Data Protection Regulation (GDPR). The revFDPA sets out a new set of data protection principles for the processing of personal data laid out in Art. 6. These include principles of lawfulness, good faith, transparency and correctness, as well as the processing in a proportional manner for a defined purpose and the storage limitation.

https://www.edoeb.admin.ch/edoeb/en/home/data-protection/dokumentation/revision-of-the-federal-data-protection-act.html

Statement on Standards for Attestation Engagements

SAS 70 Type II – Now SSAE 16

Statement on Standards for Attestation Engagement (SSAE) 18 is an American auditing standard issued by the American Institute of Certified Public Accountants (AIPCA). ... The SSAE 18 standard is used to produce System and Organization Controls (SOC) reports.

https://www.ssae-16.com/

Securities and Exchange Commission - 17a-4(f)

SEC 17a-4(f)

U.S.-based financial service institutions such as banks, broker-dealers and record keepers are required to comply with a number of regulations specifying requirements for electronic records retention, including the Securities and Exchange (SEC) Rule 17a-4(f), Commodity Futures Trading Commission (CFTC) Rule 1.31(c)-(d), and Financial Industry Regulatory Authority (FINRA) Rule 4511(c). Requirement categories include retention length, record format, record quality, and record availability, among others.

https://www.sec.gov/

Swedish Financial Supervisory Authority

SFSA

The Swedish Financial Supervisory Authority ("SFSA") (Sw. Finansinspektionen) is responsible for promoting stability and efficiency in the Swedish financial system. The SFSA authorises and supervises all companies operating in the Swedish financial markets.

The Regulations and General Guidelines regarding governance, on risk management and control at credit institutions ("SFSA Guidelines") addresses the SFSA's expectations of how credit institutions manage their outsourcing arrangements. The SFSA Guidelines provide specific guidance on: due diligence, monitoring, control and supervision, termination, reporting, business continuity, audit rights and confidential information.

System and Organization Controls

SOC

SOC for Service Organizations reports are designed to help service organizations that provide services to other entities, build trust and confidence in the service performed and controls related to the services through a report by an independent CPA. Each type of SOC for Service Organizations report is designed to help service organizations meet specific user needs.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html

System and Organization Controls 1

SOC 1

The System and Organization Controls (SOC) is a program from the American Institute of Certified Public Accountants (AICPA). It is intended to provide internal control reports on the services provided by a service organization. A SOC 1 report helps companies to establish trust and confidence in their service delivery processes and controls. The intent of these reports focuses on Internal Controls over Financial Reporting (ICFR).

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html

System and Organization Controls 1 Type 2

SOC 1 Type 2

SOC1 is an American Institute of Certified Public Accountants (AICPA) report used to document controls relevant to an organization's Internal Controls over Financial Reporting (ICFR). The report focuses on an organization's services provided, along with supporting processes, policies, procedures, personnel and operational activities that constitute the core activities relevant to users. The auditing standards for an SOC1 report include SSAE 18 and ISAE 3402.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html

System and Organization Controls 2

SOC 2

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in: Oversight of the organization Vendor management programs Internal corporate governance and risk management processes Regulatory oversight Similar to a SOC 1 report, there are two types of reports: A type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1 report on management's description of a service organization's system and the suitability of the design of controls. Use of these reports are restricted.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

System and Organization Controls 2 Type 1

SOC 2 Type 1

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in: Oversight of the organization Vendor management programs Internal corporate governance and risk management processes Regulatory oversight Similar to a SOC 1 report, there are two types of reports: A type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1 report on management's description of a service organization's system and the suitability of the design of controls. Use of these reports are restricted.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

System and Organization Controls 2 Type 2

SOC 2 Type 2

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in: Oversight of the organization Vendor management programs Internal corporate governance and risk management processes Regulatory oversight Similar to a SOC 1 report, there are two types of reports: A type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1 report on management's description of a service organization's system and the suitability of the design of controls. Use of these reports are restricted.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

System and Organization Controls 3 - Trust Services Criteria for General Use Report

SOC 3

The System and Organization Controls (SOC) is a program from the American Institute of Certified Public Accountants (AICPA). It is intended to provide internal control reports on the services provided by a service organization. A SOC 3 report outlines information related to a service organization's internal controls for security, availability, processing integrity, confidentiality or privacy. These reports are shorter than SOC 2 reports and have less details.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc3report.html

South Africa's Protection of Personal Information Act

South Africa POPI

South Africa's Protection of Personal Information Act (POPI), signed into law by the president, establishes requirements for how both public and private organizations process personal information. Organizations who are subject to POPI and who engage in the collection, storage, or processing of personal information, must comply with this law.

https://www.gov.za/documents/protection-personal-information-act

Sarbanes–Oxley Act of 2002

SOX

The Sarbanes-Oxley Act of 2002 is a law the U.S. Congress passed on July 30 of that year to help protect investors from fraudulent financial reporting by corporations.1 Also known as the SOX Act of 2002 and the Corporate Responsibility Act of 2002, it mandated strict reforms to existing securities regulations and imposed tough new penalties on lawbreakers. The Sarbanes-Oxley Act of 2002 came in response to financial scandals in the early 2000s involving publicly traded companies such as Enron Corporation, Tyco International plc, and WorldCom.2 The high-profile frauds shook investor confidence in the trustworthiness of corporate financial statements and led many to demand an overhaul of decades-old regulatory standards.

https://www.soxlaw.com/

Spain Esquema Nacional de Seguridad

Spain Esquema Nacional de Seguridad (ENS)

The Spain Esquema Nacional de Seguridad (ENS) accreditation scheme has been developed by La Entidad Nacional de Acreditación (ENAC) in close collaboration with the Ministry of Finance and Public Administration and the National Cryptologic Centre (CCN). The ENS was established as part of Royal Decree 3/2010 (amended by Decree 951/2015) and serves to establish principles and requirements for the adequate protection of information for Spanish public sector entities. Google Cloud (GCP and Google Workspace) has met the requirements to comply with ENS at the "High" level.

https://ens.ccn.cni.es/es/

Singapore Standard for Information and Communications Technology Disaster Recovery Services

SS 507

Singapore Standard for Information and Communications Technology Disaster Recovery Services (SS 507) specifies requirements for the ICT DR services. These include both those provided in-house and outsourced and covers facilities and services capability and provides fallback and recovery support to an organization's ICT systems. It includes the implementation, testing and execution aspects of disaster recovery but does not include other aspects of business continuity management.

https://www.singaporestandardseshop.sg/Product/SSPdtDetail/12691c57-e1a4-4387-87b1-fe62d31f2731

Singapore Standard Sustainable Data Centres - Part 1: Energy and Environmental Management Systems

SS 564

Specifies the requirements for the management of a sustainable data centre. Specifies requirements for an organisation to establish and maintain an energy and environmental management system, which enables the organisation to take a systematic approach, in order to achieve continual improvement of energy and water performance of its data centre.

Focuses on sustainability applicable to the sustainability aspects of data centre, including energy and water usage, as well as their consumption and efficiency. Contains best practices in the design of a sustainable data centre, as well as those in managing its electrical systems, mechanical systems and ICT equipment. Also specifies relevant indicators necessary for measuring the achievement of a sustainable data centre.

https://www.singaporestandardseshop.sg/Product/SSPdtDetail/ac609aae-e97c-456f-a7a1-5258a2816b45

Singapore Standard Sustainable Data Centres - Part 1: Energy and Environmental Management Systems

SS 564

Specifies the requirements for the management of a sustainable data centre. Specifies requirements for an organisation to establish and maintain an energy and environmental management system, which enables the organisation to take a systematic approach, in order to achieve continual improvement of energy and water performance of its data centre.

Focuses on sustainability applicable to the sustainability aspects of data centre, including energy and water usage, as well as their consumption and efficiency. Contains best practices in the design of a sustainable data centre, as well as those in managing its electrical systems, mechanical systems and ICT equipment. Also specifies relevant indicators necessary for measuring the achievement of a sustainable data centre.

https://www.singaporestandardseshop.sg/Product/SSPdtDetail/ac609aae-e97c-456f-a7a1-5258a2816b45

Switching Cloud Providers and Porting Data Data Portability Code of Conduct

SWIPO Data Portability Code of Conduct

SWIPO (Switching Cloud Providers and Porting Data), a multi-stakeholder group facilitated by the European Commission, developed a set of Data Portability Codes of Conduct. These Data Portability Codes of Conduct, which are voluntary, were written to provide guidance on the proper application of Article 6 of the Free Flow of Non-Personal Data Regulation. Google Cloud is a member of SWIPO and supports this initiative.

https://swipo.eu/

SSAE 16 SOC 1 Type 1

SSAE 16 SOC 1 Type 1

There are significant differences between a Type I and Type II report, however, we aren't going to discuss that here, thats for another day. We will discuss the basics of a SSAE 16 Type I Report and some areas that should be focused on if this is the direction your company wants to take. While the Type I Report doesn't carry much weight, there are benefits, and that's why it exists as an option. A Type I Report is specifically defined by the SSAE 16 guidance as a "report on a description of a service organization's system and the suitability of the design of controls", essentially, a determination of if your company's controls designed appropriately. When performing a Type I report, the auditors will test the design effectiveness of your company's defined controls by examining a sample of 1 item per control. This provides a user organization with some comfort that your company (the service organization) has at least some controls in place. This can be useful when trying to obtain a contract and to show good faith to the potential user organization that your company is moving in the right direction. Most user organizations will require a Type II Report before contracting your company as a service organization of theirs.

https://www.ssae-16.com/type-i/

SSAE 16 System and Organization Controls 1 Type 2

SSAE 16 SOC 1 Type 2

There are significant differences between a Type I and Type II report, however, we aren't going to discuss that here, thats for another day. We will discuss the basics of a SSAE 16 Type I Report and some areas that should be focused on if this is the direction your company wants to take. While the Type I Report doesn't carry much weight, there are benefits, and that's why it exists as an option. A Type I Report is specifically defined by the SSAE 16 guidance as a "report on a description of a service organization's system and the suitability of the design of controls", essentially, a determination of if your company's controls designed appropriately. When performing a Type I report, the auditors will test the design effectiveness of your company's defined controls by examining a sample of 1 item per control. This provides a user organization with some comfort that your company (the service organization) has at least some controls in place. This can be useful when trying to obtain a contract and to show good faith to the potential user organization that your company is moving in the right direction. Most user organizations will require a Type II Report before contracting your company as a service organization of theirs.

https://www.ssae-16.com/type-i/

SSAE 18 SOC 1 Type 1

SSAE 18 SOC 1 Type 1

There are significant differences between a Type I and Type II report, however, we aren't going to discuss that here, thats for another day. We will discuss the basics of a SSAE 16 Type I Report and some areas that should be focused on if this is the direction your company wants to take. While the Type I Report doesn't carry much weight, there are benefits, and that's why it exists as an option. A Type I Report is specifically defined by the SSAE 16 guidance as a "report on a description of a service organization's system and the suitability of the design of controls", essentially, a determination of if your company's controls designed appropriately. When performing a Type I report, the auditors will test the design effectiveness of your company's defined controls by examining a sample of 1 item per control. This provides a user organization with some comfort that your company (the service organization) has at least some controls in place. This can be useful when trying to obtain a contract and to show good faith to the potential user organization that your company is moving in the right direction. Most user organizations will require a Type II Report before contracting your company as a service organization of theirs.

https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/

SSAE 18 SOC 1 Type 2

SSAE 18 SOC 1 Type 2

There are significant differences between a Type I and Type II report, however, we aren't going to discuss that here, thats for another day. We will discuss the basics of a SSAE 16 Type I Report and some areas that should be focused on if this is the direction your company wants to take. While the Type I Report doesn't carry much weight, there are benefits, and that's why it exists as an option. A Type I Report is specifically defined by the SSAE 16 guidance as a "report on a description of a service organization's system and the suitability of the design of controls", essentially, a determination of if your company's controls designed appropriately. When performing a Type I report, the auditors will test the design effectiveness of your company's defined controls by examining a sample of 1 item per control. This provides a user organization with some comfort that your company (the service organization) has at least some controls in place. This can be useful when trying to obtain a contract and to show good faith to the potential user organization that your company is moving in the right direction. Most user organizations will require a Type II Report before contracting your company as a service organization of theirs.

https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/

Standardized Information Gathering (SIG) Questionnaire

Standardized Information Gathering (SIG) Questionnaire

Shared Assessments (""SIG questionnaire"") allows organizations to build, customize, analyze and store vendor assessments for managing third party risk.

The SIG questionnaire framework helps assess Google Cloud against risk areas including cybersecurity, IT, privacy, data security, and business resiliency, and is aligned to many industry standards (i.e., ISO/IEC 27002:2013, PCI, NIST SP 800-53 Rev 4, HIPAA, and GDPR).

Google Cloud has filled out the SIG core questionnaire, answering 956 controls questions scoped to CSA CCM and ISO/IEC 27002 controls.

https://sharedassessments.org/sig/

Financial Conduct Authority

SYSC 8 Outsourcing FCA Handbook

The Financial Conduct Authority ("FCA") is responsible for regulating the conduct of financial services firms and financial markets in the United Kingdom, in addition to being a prudential supervisor and setting standards for the firms it regulates. The Financial Conduct Authority released the FCA Handbook, which outlines a set of rules required to be followed by banks, insurers, investment businesses and other financial services in the United Kingdom under the Financial Services and Markets Act 2000. SYSC 8 is part of the FCA Handbook which ets out the FCA's expectations of regulated firms when outsourcing to service providers. It provides specific guidance on: monitoring, due diligence, supervision by the service provider, transition, audit, security, and business continuity.

https://www.fca.org.uk/

TIA-942 Certification

TIA 942 Certified

The TIA-942 Certification Program enables data centers to be reviewed and certified for conformity to the requirements of the globally-recognized ANSI/TIA-942 standard, providing greater assurance to customers and stakeholders. The program includes a worldwide listing of TIA-942 certified data centers, TIA-942 certified auditors, consultants and companies providing consulting and auditing services, as well as information and training for companies and individuals interested in becoming a certified auditor or consultant.

https://tiaonline.org/products-and-services/tia942certification/

Trusted Information Security Assessment Exchange — TISAX

TISAX (Trusted Information Security Assessment Exchange), governed by the ENX Association on behalf of the German VDA (Verband der Automobilindustrie, the German Automobile Industry Association), provides a single industry-specific security framework for assessing information security for the wide landscape of suppliers, OEMs, and partners that contribute to the automobile supply chain.

https://enx.com/en-US/TISAX/

Trusted Site Infrastructure — TSI

Trusted Site Infrastructure (TSI) is an assessment and certification program to evaluate the physical security and availability of data centers. TÜV Informationstechnik GmbH (TÜViT|TÜV NORD GROUP) has established criteria catalogues such as the TSI.STANDARD or TSI.EN50600, which take into account international guidelines and standards and address the critical aspects of a data center like the environment, construction, fire detection and extinguishing systems, security, cabling, power supply, air conditioning systems, organization and the documentation. The criteria catalogues are being continuously developed in order to always represent the current state of the art.

https://www.tuvit.de/en/services/data-centers-colocation-cloud-infrastructures/trusted-site-infrastructure/

Threat, Vulnerability And Risk Assessment — TVRA

Threat Vulnerability & Risk Assessments (TVRA) is the 1st step in developing an effective facility security program. A properly conducted TVRA provides a solid defensible foundation from which to develop a physical security program at any site, facility, or location. The TVRA identifies the security risk an organization or school faces and ensures that the physical security program is designed to properly address those risks. The TVRA findings provide a road map that can be used to refine or develop a properly integrated physical security program.

https://tvraa.com/

Abu Dhabi International Sculpture Symposium

UAE ADISS

ADISS is held under the patronage of His Highness Sheikh Mohammed bin Zayed Al Nahyan, the Crown Prince of Abu Dhabi and Deputy Supreme Commander of the U.A.E. Armed Forces, who is dedicated to establishing Abu Dhabi as the cultural center of the Middle East, in line with his 2030 vision.

This unique event is brought to Abu Dhabi under the direction of His Excellency Sheikh Nahayan Mabarak Al Nahayan - the Minister of Higher Education and Scientific Research and President of Zayed University (ZU). Sheikh Nahayan is committed to bringing together culture and education through ADISS, under the theme of ""Bridging Societies Through the Language of Art"".

ADISS 2010 will be held and organized under the umbrella of Zayed University - an internationally accredited university with campuses in Abu Dhabi and Dubai - in collaboration with Salwa Zeidan Gallery, one of Abu Dhabi's eminent contemporary art spaces.

The six-week symposium will run from February 25th to April 7th 2010 and will reveal the works of some of the most talented international artists who were carefully selected to give the Symposium a multi-cultural context.

http://www.adiss-uae.com/

UAE IAR Information Security Requirements

UAE IAR Information Security Requirements

In light of the rapidly evolving cyber threats, including hacktivists and organised cybercrime groups that challenge national security and compromise critical information assets, Telecommunications and Digital Government Regulatory Authority developed the 'UAE Information Assurance Regulation' to provide requirements to raise the minimum level of protection of information assets and supporting systems across all entities in the UAE. The regulation seeks a trusted digital environment throughout the UAE.

The IA Regulation provides management and technical information security controls for entities to establish, implement, maintain, and continuously improve information assurance. TDRA will designate the critical entities as per the UAE CIIP Policy to implement the IA Regulation and apply its requirements to the use, processing, storage and transmission of information or data, and the systems and processes used for those purposes. This includes information in physical or electronic form that may be owned, leased, or otherwise in the possession, custody, or control of the entities.

https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation

Uptime Institute

Uptime Institute

As an independent advisory organization, Uptime Institute is focused on improving the performance, efficiency, and reliability of the business critical infrastructure that underlies today's global information economy. Uptime Institute is recognized worldwide for the creation and administration of the Tier Standards & Certifications for Data Center Design, Construction (Facility) and Operational Sustainability.

https://www.uptimeinstitute.com

Uptime Institute - Construction

Uptime Institute - Construction

Tier Certification of Constructed Facility ensures that your facility has been constructed as designed, and verifies that it is capable of meeting the defined availability requirements. Even the best laid plans can go awry, and common construction phase practices or value engineering proposals can compromise the design intent of a data center.

https://uptimeinstitute.com/tier-certification/construction

Uptime Institute - Design

Uptime Institute - Design

When you're putting millions of dollars into building a new data center, you want to ensure that the facility is going to provide the level of IT performance and reliability that satisfies your business objective for 24 x 7 availability. At the same time, the project has to balance risk management, energy efficiency, and cost considerations, and ultimately deliver ROI. Designing a data center requires significant planning. Businesses must establish the locations of servers, prime and contingency power sources, network routes, cooling equipment, cable management, and required safety measures. This process is an undertaking that a majority of businesses cannot reliably perform in-house, creating worrisome financial risks to investors should any design mistakes slip past.

https://uptimeinstitute.com/tier-certification/design

Uptime Institute - M&O

Uptime Institute - M&O

In today's digital world, your data center is more important than ever. A single mission critical data center can house information representing hundreds of thousands of dollars, and vast amounts of sensitive data integral to keeping businesses running smoothly and efficiently. Maintaining uptime is of utmost importance. Most downtime can be attributed to human error, which is often preventable with the use of correct methods and techniques.

https://uptimeinstitute.com/professional-services/management-operations

Uptime Tier I

Uptime Tier I

A Tier I data center is the basic capacity level with infrastructure to support information technology for an office setting and beyond. The requirements for a Tier I facility include: An uninterruptible power supply (UPS) for power sags, outages, and spikes. An area for IT systems. Dedicated cooling equipment that runs outside office hours. An engine generator for power outages. Tier I protects against disruptions from human error, but not unexpected failure or outage. Redundant equipment includes chillers, pumps, UPS modules, and engine generators. The facility will have to shut down completely for preventive maintenance and repairs, and failure to do so increases the risk of unplanned disruptions and severe consequences from system failure.

https://uptimeinstitute.com/tiers

Uptime Tier II

Uptime Tier II

Tier II facilities cover redundant capacity components for power and cooling that provide better maintenance opportunities and safety against disruptions. These components include: Engine generators. Energy storage. Chillers. Cooling units. UPS modules. Pumps. Heat rejection equipment. Fuel tanks. Fuel cells. The distribution path of Tier II serves a critical environment, and the components can be removed without shutting it down. Like a Tier I facility, unexpected shutdown of a Tier II data center will affect the system.

https://uptimeinstitute.com/tiers

Uptime Tier III

Uptime Tier III

A Tier III data center is concurrently maintainable with redundant components as a key differentiator, with redundant distribution paths to serve the critical environment. Unlike Tier I and Tier II, these facilities require no shutdowns when equipment needs maintenance or replacement. The components of Tier III are added to Tier II components so that any part can be shut down without impacting IT operation.

https://uptimeinstitute.com/tiers

Uptime Tier IV

Uptime Tier IV

A Tier IV data center has several independent and physically isolated systems that act as redundant capacity components and distribution paths. The separation is necessary to prevent an event from compromising both systems. The environment will not be affected by a disruption from planned and unplanned events. However, if the redundant components or distribution paths are shut down for maintenance, the environment may experience a higher risk of disruption if a failure occurs. Tier IV facilities add fault tolerance to the Tier III topology. When a piece of equipment fails, or there is an interruption in the distribution path, IT operations will not be affected. All of the IT equipment must have a fault-tolerant power design to be compatible. Tier IV data centers also require continuous cooling to make the environment stable.

https://uptimeinstitute.com/tiers

VAG (Austria)

VAG

The Austrian Financial Market Authority ("Austrian FMA") is responsible for the supervision of banks (in cooperation with the Austrian Central Bank), insurance companies, pension companies and the financial securities sector, including stock exchanges to promote cooperation on financial market issues and financial market stability.

The Versicherungsaufsichtsgesetz ("VAG") addresses the Austrian FMA's expectations when insurance or reinsurance undertakings outsource activities. The VAG provides specific guidance on audit rights, monitoring the service, reporting and information access.

https://www.vag-group.com/en/

EU-US Privacy Shield

EU-US Privacy Shield

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

https://www.privacyshield.gov/

DMTF

DMTF

DMTF supports the management of existing and new technologies, such as cloud, by developing appropriate standards. Its working groups, such as Open Cloud Standards Incubator, Cloud Management Working Group and Cloud Auditing Data Federation Working Group, address cloud issues in greater detail.

Open Grid Forum

OGF

OGF is an open global community committed to driving the rapid evolution and adoption of modern advanced applied distributed computing, including cloud, grid and associated storage, networking and workflow methods. OGF is focused on developing and promoting innovative scalable techniques, applications and infrastructures to improve productivity in the enterprise and within the international research, science and business communities.

OGF accomplishes its work through open forums, interactions and events that build the community, explore trends, share optimal approaches, document findings and consolidate these results where appropriate into standards. The output products that result from this process document and codify best practices and standards that provide the basis for some of the largest and most powerful operational computing infrastructure systems in the world.

https://www.ogf.org/ogf/doku.php

Open Commons Consortium

OCC

The Open Commons Consortium (OCC) manages and operates cloud computing, data commons, and data ecosystems to advance scientific, medical, health care and environmental research for human and societal impact.

https://www.occ-data.org/

Organization for the Advancement of Structured Information Standards

OASIS

This nonprofit organization develops open standards for security, cloud technology, IoT, content technologies and emergency management. OASIS Open is where individuals, organizations, and governments come together to solve some of the world's biggest technical challenges through the development of open code and open standards.

https://www.oasis-open.org/

The Open Group

The Open Group

The Open Group works with customers and suppliers of technology products and services, and with consortia and other standards organizations to capture, clarify, and integrate current and emerging requirements, establish standards and policies, and share best practices. Our standards ensure openness, interoperability, and consensus.

https://www.opengroup.org/

Storage Networking Industry Association - Cloud Data Management Interface

SNIA - CDMI

The Cloud Data Management Interface defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud. As part of this interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data that is placed in them. In addition, metadata can be set on containers and their contained data elements through this interface.

This interface is also used by administrative and management applications to manage containers, accounts, security access and monitoring/billing information, even for storage that is accessible by other protocols. The capabilities of the underlying storage and data services are exposed so that clients can understand the offering.

https://www.snia.org/cdmi