**(ISC)2 - International Information System Security Certification Consortium**  A security certification granting organization that has a long history of certifications that were difficult to get. This difficulty has made their certificates seen as having higher value in the industry.

**(ISC)2 Cloud Secure Data Life Cycle** Based on CSA Guidance. 1. **Create**; 2. **Store**; 3. **Use**; 4. **Share**; 5. **Archive**; 6. **Destroy**.

**(SAS) 70** Statement on Auditing Standards (SAS) No. 70 was a recognized standard of the American Institute of Certified Public Accountants (AICPA) in response to the issues that also lead to Sarbanes-Oxley (SOX). Deprecated in 2011 by the Statement on Standards for Attestation Engagements (**SSAE) No. 16**.

**AICPA -- American Institute of Certified Public Accountants** which established SAS 70 and later SAAE 16.

**American Institute of Certified Public Accountants (AICPA)**

**Application Normative Framework** (ANF), **Organizational Normative Framework** (ONF) are concepts of ISO 27034. There is only one ONF for an organization but potentially as many ANF's as applications.

**ASHRAE** - American Society of Heating, Refrigerating and Air-Conditioning Engineers is an American professional association seeking to advance heating, ventilation, air conditioning and refrigeration systems design and construction.

**Biba** - an access control model designed to preserve data integrity. It has 3 goals. Maintain internal and external consistency; prevent unauthorized data modification even by authorized parties; prevent data modification by unauthorized individuals.

**Capability Maturity Model (CMM)** is a development model where the maturity relates to the formality and optimization of processes. When applied to cloud security it would focus on those aspects as they relate to cloud security.

**Child Online Protection Act (COPA)** - An attempt to restrict access by minors to material defined as harmful to minors. A permanent injunction against the law in 2009.

**Cloud Access Security Brokers (CASBs)** monitors network activity between users and cloud applications and enforces security policy and blocking malware.

**Cloud Security Alliance** (CSA) publishes the **Notorious Nine**: 1) Data breaches; 2) Data Loss; 3) Account service traffic hijacking; 4) Insecure Interfaces and APIs; 5) Denial of Service; 6) Malicious Insiders; 7) Abuse of Cloud Services; 8) Insufficient Due Diligence; 9) Shared technology Vulnerabilities. There are also implications and controls associated with each.

**Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR)** or **CSA STAR** -- uses the Consensus Assessments Initiative Questionnaire (CAIQ), Cloud Controls Matrix (CCM), and GDPR Self-Assessment as inputs to certify an organization to Level 1. Level 2 integrates the CSA Cloud Controls Matrix and the AICPA Trust Service Principles - AT 101 for STAR attestation. STAR Certification for level to uses the CSA Cloud Controls Matrix and the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix. Certification certificates follow normal ISO/IEC 27001 protocol for a 3rd party assessment

**Cloud Security Alliance Cloud Controls Matrix (CSA CCM)** Composed of 17 domains covering key elements of cloud. It contains 170 objectives within the domains. They integrate with the STAR program**.**

**COBIT** or Control Objectives for Information and Related Technologies is a framework for IT governance and management. Initially used to achieve compliance with Sarbanes-Oxley and focused on IT controls. Since 2019 the emphasis has shifted to information governance. It is focused on these 5 principles: 1: Meeting Stakeholder Needs; 2: Covering the Enterprise End-to-End; 3: Applying a Single Integrated Framework; 4: Enabling a Holistic Approach; and 5: Separating Governance from Management.

**Common Criteria and the EAL rating** An EAL rating is assigned to an IT product after it has been evaluated by an independent lab. The level indicates the degree and type of testing with 1 the least and 7 the most. Common criteria contain 60 functional requirements in 11 classes and is an accepted standard among the military organizations of the US and many allies.

**Consensus Assessments Initiative Questionnaire (CAIQ)** is an initiative of the Cloud Security Alliance to provide an industry-accepted documentation of security controls and as of 2020 is combined with the Cloud Controls Matrix. They can be used as evidence for entry to the CSA STAR registry.

**Digital Millennium Copyright Act (DMCA)** -- and occasionally controversial act intended to align the US copyright act with the requirements of treaties and the World Intellectual Property Organization.

**DLP -- Data Los Prevention** is ensured by a set of tools, procedures, and policy to ensure sensitive, proprietary, and PII is not lost or misused. It helps to provide compliance with numerous laws and compliance requirements by enforcing preventative and detective measures in the organization.

**ENISA - European Union Agency for Cybersecurity** is a Cyber Security awareness association that provides support, information, and collaboration on security issues. They also publish a top x threats each year. The last few years they have included 15 threats each year.

**EU Data Directive** regulates the processing of PII in the EU. Since it is a directive, each country must pass the laws that establish how each country will enforce the directive. It includes the 7 principles governing the OECD’s recommendations for protection of personal data.

**Eurocloud Star Audit Certification (ESAC)** is nonprofit organization that maintains information security standards or best practices and provides assessments and certification of compliance.

**European Union Agency for Network and Information Security (ENISA)** see ENISA above.

**Family Education Rights and Privacy Act (FERPA)** is a Federal law that protects the privacy of student education records. It applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

**Federal Information Processing Standard (FIPS) 140-2** is mandatory for all US government, military, contractors doing business with the government and regulated industries such as financial and health-care institutions. IT is being succeeded by FIPS 140-3. FIPS 140-2 has four levels with 1 being the lowest level of security through 4 as the highest. Testing under FIPS 140-2 is done by 23 accredited Cryptographic Module Testing laboratories.

**Federal Information Systems Management Act (FISMA)** is a US law that makes mandatory requirements for federal agencies to develop, document, and implement management cyber security. NIST plays a major role in implementing FISMA and has promulgated numerous security standards and guidelines.One key guideline is the Risk Management Framework (RMF). Office of Management and Budget (OMB) monitors compliance with NIST programs.

**Fiber Channel** is a data transfer protocol used to connect servers to Storage Area Networks (SAN) in data centers. It typically runs on fiber optic cables but can also run on copper. Data rates range from 1 to 128 gigabit/sec.

**Fiber Channel over Ethernet (FCoE)** encapsulates Fiber Channel frames over Ethernet networks. This technology can support speeds of up to 10Gigabit/sec. Using FCoE can allow network and storage traffic to connect using a wider range of networks and storage devices.

**FIPS 140-2** Used for protecting sensitive but unclassified information by the federal government. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards such as CMVP. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries.

**GDPR – General Data Protection Regulation** gives individuals control over their personal data. It also simplified regulation by forcing all member states to comply with a single regulation. GDPR specifies rights of the data subject, including access rectification, erasure, object to use of PII. It poses requirements on data controllers and data processors.

**Generally Accepted Privacy Principles described by the AICPA (GAPP)**  The generally accepted principles and practices (GAPP), were agreed upon by 23 countries in response to investors and regulators concerned about transparency, independence, and governance of the accounting industry. It was based on 24 principles in the areas of legal, institutional, and investment and risk.

**Gramm-Leach-Bliley Act (GLBA)** requires companies that offer financial products or services to safeguard sensitive data about customers and inform the customers of those requirements.

**Health Insurance Portability and Accountability Act (HIPAA)** modernized healthcare information and stipulated how PII kept by healthcare and healthcare insurance industries should be protected. The act was vague

**HIPAA** see above (**Health Insurance Portability and Accountability Act)**

**HITECH** act motivated the implementation of electronic health records (HER) and the supporting technology. Some penalties for non-compliance of HIPAA were increased under HITEC, as well as establishing breach notification to impacted patients.

**IDCA** or **International Data Center Authority** is attempting to be “the ultimate standardization, education, and certification body for the Application Ecosystem and its supporting digital infrastructure, helps deliver comprehensive, effective, up-to-date and uniquely innovative data compliance audits. The Application Ecosystem and digital infrastructure audits.” Auditors certified by IDCA will engage with cloud providers to assess their compliance to IDCA Grade Levels.

**International Standards Organization (ISO)** is an international standards body composed of representatives from various standards organizations.

**Internet Small Computer System Interface (iSCSI)** is a storage networking standard used to link data storage to systems using the Internet Protocol (IP).

**ISACA’s COBIT** see COBIT

**ISO/IEC 27001** Standard on managing Information Security. It includes requirements for establishing , implementing, maintaining, and continually improving information management.

**ISO/IEC 27002** provides best practices on information security controls for those attempting to be ISO/IEC 27001.

**ISO/IEC 27017** created to supplement ISO/IEC 27002 to provide additional security controls for the cloud.

**ISO/IEC 27018:2014 ISO/IEC 27018:2019** IT Security techniques. Cod of practice for protection of PII in public clouds.

**ISO/IEC 27034-1** mandates a framework for application security within an organization. According to the standard, each organization should have a(n) \_\_\_\_\_\_\_\_\_\_\_, and each application within the organization should have its own \_\_\_\_\_\_\_\_\_\_\_\_.

**ISO/IEC 28000:2007** is a standard for ensuring security assurance in the supply chain.

**ISO/IEC 31000:2009** is a standard providing industry independent principles and guidelines on risk management. It does not intend or attempt to achieve uniformity but rather the most appropriate risk management for each organization for its objectives, context, structure, operations, processes, functions, services, or assets employed.

**(ISC)2 - International Information System Security Certification Consortium**  A security certification granting organization that has a long history of certifications that were difficult to get. This difficulty has made their certificates seen as having higher value in the industry.

**(ISC)2 Cloud Secure Data Life Cycle** Based on CSA Guidance. 1. **Create**; 2. **Store**; 3. **Use**; 4. **Share**; 5. **Archive**; 6. **Destroy**.

**Key risk indicators (KRI)** critical predictors of risks or adverse events that can impact and organization.

**Lightweight Directory Access Protocol (LDAP)** environment, each entry in a directory server is identified by a Distinguished name (DN)

**Mean time between failure (MTBF)**  is the predicted time between failures of a system during normal system operation. It applies only to unplanned maintenance and excludes scheduled maintenance, inspection, recalibration, or prevent parts replacement.

**Mean time to repair (MTTR)** is the mean time it takes to repair a system. It includes both the repair time and testing time.

**NFPA** National Fire Protection Association. This is a nonprofit organization attempting to eliminate death, injury, property, and economic loss due to fire, electrical and related hazards.

**NIST** National Institute of Standards and Technology is an agency of the Department of Commerce whose mission is to promote innovation and industrial competitiveness. It also creates numerous standard and requirements for the DoD, Federal Government, and government contractors relating to Cyber security.

**NIST SP 800-37** establishes the Risk Management Framework using a life cycle approach for security and privacy. “The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels. The RMF also promotes near real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle.”

**NIST SP 800-53** provides security and privacy controls for information systems and organizations.

**NIST SP 800-92**  Guide to Computer Security Log Management “seeks to assist organizations in understanding the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization. The publication presents logging technologies from a high-level viewpoint.”

**Open Web Application Security Project (OWASP)** is a nonprofit organization working to improve the security of software. They are known for their top 10 most critical security concerns for web application security. See <https://owasp.org/www-project-top-ten/>

**Organization for Economic Cooperation and Development (OECD)** produced 7 principals to govern the protection of data. They are:

1. **Notice**—data subjects should be given notice when their data is being collected;
2. **Purpose**—data should only be used for the purpose stated and not for any other purposes;
3. **Consent**—data should not be disclosed without the data subject’s consent;
4. **Security**—collected data should be kept secure from any potential abuses;
5. **Disclosure**—data subjects should be informed as to who is collecting their data;
6. **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data
7. **Accountability**—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

**Organizational Normative Framework (ONF), Application Normative Framework (ANF)** The Organizational Normative Framework (ONF) is a framework which contains multiple application security best practices know as Application Normative Frameworks (ANFs). One ONF per organization with as many ANFs as needed.

**OSHA** is a large regulatory agency of the United States Department of Labor that originally had federal visitorial powers to inspect and examine workplaces.

**Payment Card Industry Data Security Standard (PCI DSS)** is an industry requirement that imposes on anyone who processes or accepts credit cards. The PCI can impose fines on violators if they fail to meet PCI DSS requirements. Depending on the size of the vendor, external, independent audits can be required in addition to higher requirements.

**Personal Information Protection and Electronic Documents Act (PIPEDA)** is a Canadian data privacy law that protects the PII of individuals. It provides for individuals to inspect the data held by and organization and challenge its accuracy. It also requires an organization to obtain the consent of an individual when collecting, using, and disclosing that PII.

**Privacy Level Agreement (PLA)** is and agreement set to contract how a third-party provider will ensure the confidentiality of information an organization might permit them to access.

**Recovery time objective (RTO)** is the duration of time and specified service level to which a business process must be restored to.

**Risk Management Framework (RMF)** is a set of standards and guidelines to develop a risk-based approach to Information Security. It helps and organization **prepare** for risk management, **categorize** systems and information based on impact studies, **select** appropriate controls based on risk assessments, **implement** and document the controls, **assess** how well the controls work, authorize the system to operate, and **monitor** controls and changes to the risks to the system.

**RPO** Recovery Point Objective refers to how much data can be lost before that loss causes significant harm to the business. This often drives backup and real-time duplication requirements.

**RTO** is the maximum time after an outage of a computer or other resource to resume normal business operations.

**SABSA** stands for Sherwood Applied Business Security Architecture, which is a framework for enterprise security architecture and service management.

**Sarbanes-Oxley Act (SOX)** A law passed to increase independence in audit practices and require the retention and accuracy of financial records as a result of financial and stock scandals associated with Enron.

**SAS 70** Statement on Auditing Standards (SAS) No. 70 was a recognized standard of the American Institute of Certified Public Accountants (AICPA) in response to the issues that also lead to Sarbanes-Oxley (SOX). Deprecated in 2011 by the Statement on Standards for Attestation Engagements (**SSAE) No. 16**.

**SEC** is the US Securities and Exchange Commission whose primary purpose is to combat market manipulation. It also enforces the Sarbanes-Oxley Act.

**Secure Sockets Layer (SSL)**

**Sherwood Applied Business Structure Architecture (SABSA)** see SABSA

**SIEMs** are Security Event and Incident Managers. They collect, clean, and correlate

**SOC 1 Report** This report focuses on controls associated with financial services.

**SOC 2 Type 1 Report**

**SOC 2 Type 2 Report** the SOC 2 reports are composed of five principles: confidentiality, processing integrity, availability, privacy, and security.

**SOC 3 Report** is an attestation report or can be called a seal of approval. It lacks financial or security data but only attests that an audit was performed.

**SRE** stands for Site Reliability Engineering which is a set of practices and principles whose goal is to produce scalable and highly reliable software systems. Closely related to DevOPS, which are practices that combine software develop SRE and IT operations.

**SSAE 16** and subsequent SOC reports are the successors of the SAS 70.

**Standard Application Security (SAS), Application Normative Framework (ANF)**

Statement on Standards for Attestation Engagements (SSAE) auditing standard and certifies auditors for that standard?

Statement on Standards for Attestation Engagements 16 (SSAE 16) Service Organization Control (SOC) reports are audit tools promulgated by the American Institute of Certified Public Accountants (AICPA).

**Storage area networks (SAN)** is a dedicated, high-speed network that connects shared pools of storage to multiple servers.

**STRIDE Model** STRIDE is a threat model while DREAD is a risk assessment model. STRIDE stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of service, **E**levation of privilege.

**System and Organization Controls (SOC) reports** help companies establish trust and confidence in service delivery and controls. The reports are produced by third party certified public accountants.

**US Office of Management and Budget (OMB)** is a component of the Executive branch. Of import to us, they manage FedRAMP and direct it’s used for the Federal Governments use of the Cloud.

**Uptime Institute** has created and promoted the Tier Standard which guides the design, construction, and operation of sites world-wide. A data center can be rated from Tier 1, the lowest to Tier 4 based on built-in redundancy, distribution paths, concurrent maintenance, fault tolerance, compartmentalization, and cooling.

**USPTO** is the US Patent and Trademark Office which registers both.