CYBER GRC & SECURITY COMPLIANCE

DEFINITIONS (TO FAMILIARIZE YOURSELF WITH DEFINITIONS)

SECURITY COMPLIANCE

Given the importance tied to ensuring security and privacy of information assets, a lot of information & cybersecurity frameworks and standards have been established by reputable bodies and institutes to provide best practices and guidance on safeguards for information assets, and ensure compliance to these standards where necessary. Such standards includes ISO 27001, PCI DSS, SOC 1, 2, 3, SOX, NIST, CIS CSC, CCM, HIPAA, HITRUST, EU GDPR, and lots more.

Information security ensures the implementation of effective physical, technical, and administrative controls to protect the **CIA** of digital assets, **Compliance** is the application of information security practices to ensure adherence to regulatory requirements and to build trust with other security-minded businesses.

Security compliance can be external (i.e. regulatory) and internal (i.e. management). Even though the best part about technology is seeing what the world does with it, the better part about technology is seeing that the world complies with acceptable usage standards as defined by the regulators or product owners.

Ensuring compliance at both external and internal levels can be driven through automated (i.e. system enforced) and manual processes (e.g. periodic assessments and audits).

Just as information security establishes a comprehensive baseline for digital asset protection, compliance ensures adherence to the control baselines.

ISO 27001 & ISO 27002 - Building Information Security Management System (ISMS) (LINK HERE)

ISO 27001 is a management standard for building and maintaining Information Security Management Systems (ISMS). ISO 27001 helps with the design and implementation of an organization's information security management system to ensure protection of information assets through implementation of the **Clauses 4 to 10,** and also the Controls in the **Annex A** section of the standard.

ISO 27002 is a GUIDANCE document that is used to supplement **ISO 27001**. The ISO 27002 is used as implementation guidance as it contains guidance for implementing the controls listed in the **Annex A of the ISO 27001.**

ISO 27001 standards uses a risk-based approach to initiating, implementing, maintaining, developing and improving effective security management practices to help secure digital assets.

To implement the ISO 27001, the requirements in Clauses 4 to 10 are mandatory and must be satisfied by the entity to ascertain compliance with ISO standards. Entities are allowed to select only the controls that are applicable to their business from the **ANNEX A** controls during ISO 27001 audit and assessment. The applicable controls will be documented in a document called **STATEMENT OF APPLICABILITY (SOA)**. However, for all the controls that are deemed to be **NOT_APPLICABLE**, the entity must document the **RATIONALE FOR EXCLUSION**

The ISO 27001:2013 version has a total of **14 DOMAINS** and **114 CONTROLS** as part of the ANNEX A.

A.5: Information security policies (2 controls)

A.6: Organization of information security (7 controls)

A.7: Human resource security - 6 controls that are applied before, during, or after employment

A.8: Asset management (10 controls)

A.9: Access control (14 controls)

A.10: Cryptography (2 controls)

A.11: Physical and environmental security (15 controls)

A.12: Operations security (14 controls)

A.13: Communications security (7 controls)

A.14: System acquisition, development and maintenance (13 controls)

A.15: Supplier relationships (5 controls)

A.16: Information security incident management (7 controls)

A.17: Information security aspects of business continuity management (4 controls)

A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

A new version of ISO 27001: 2022 just got approved in October 2022 and a new version of ISO 27002:2022 got approved in February 2022. The new version has about 98 controls for Annex A which is a reduction from the 114 controls in the previous version, with other changes as such. Privacy of information asset is also included in the standard which already contains details on security of information

PDCA CYCLE

PDCA CYCLE

This is an approach/ process used for implementing the Information Security Management Systems in line with ISO standard:

- **Plan (establishing the ISMS)**

  Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.
- **Do (implementing and workings of the ISMS)**

  Implement and exploit the ISMS policy, controls, processes and procedures.
- **Check (monitoring and review of the ISMS)**

  Assess and, if applicable, measure the performances of the processes against the policy, objectives and practical experience and report results to management for review.
- **Act (update and improvement of the ISMS)**

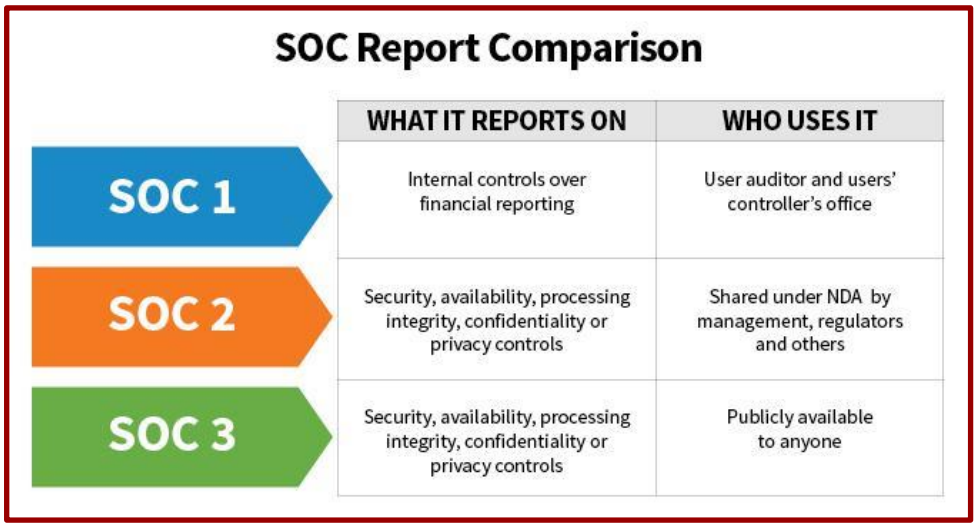
  Undertake corrective and preventive actions, on the basis of the results of the ISMS internal audit and management review, or other relevant information to continually improve the said system.

SOC 2 & 3 (LINK HERE)

NT: SOC Reports are usually obtained by 3rd-party companies or Service Organisations

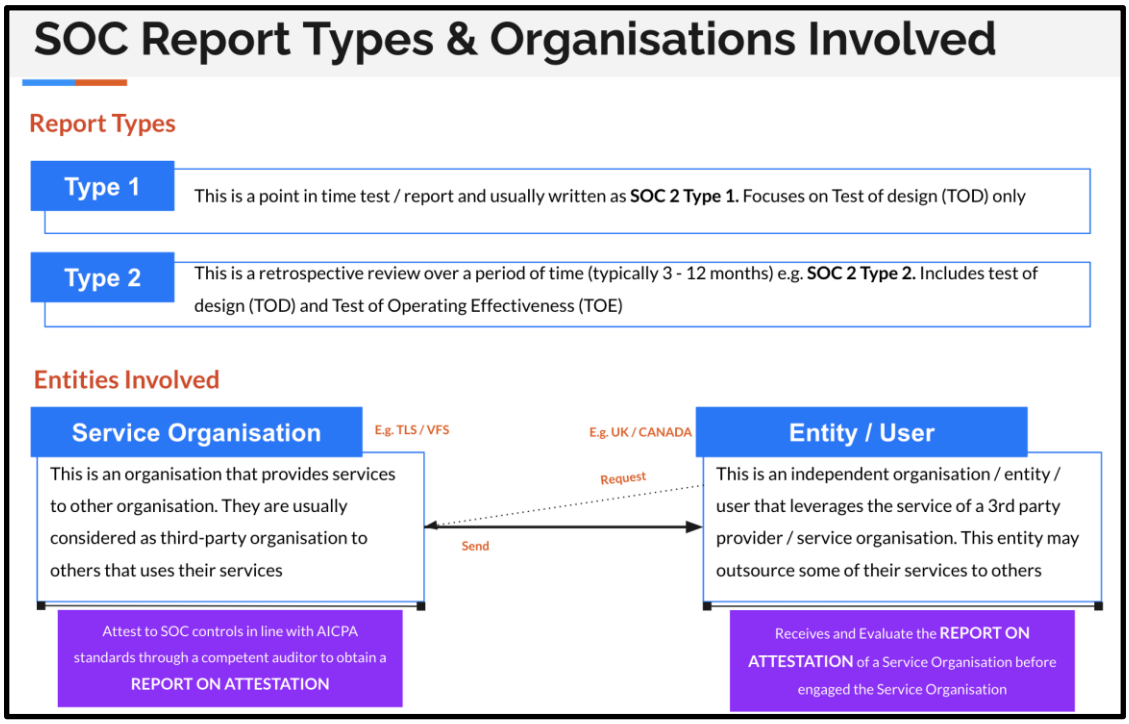
SOC report is an attestation report that shows a service organization's ability to protect information and digital assets. It was created by the American Institute of Certified Public Accountant (AICPA) in 2010.

There are three types of SOC reports namely SOC 1, SOC 2 and SOC 3.



SOC 1 and SOC 2 reports are intended to provide user entities with a description of the service organization's system as well as a detailed understanding of the design of controls at that service organization and the tests performed by the service auditor to support his/her conclusions on the operating effectiveness of those controls.

3rd party organizations obtain SOC reports to demonstrate compliance with standards, and also gain market edge.



SOC 2 report is an attestation report that shows a 3rd-party / service organization's ability to protect information and digital assets. SOC 3 report is a summarized and publicly accessible version of SOC 2 report. The main difference is that SOC 2 is a **restricted use report (i.e. only shared with the stakeholder on a need to know basis)** and a SOC 3 is a **general use report (i.e. available to the general public).**

CIS Critical Security Controls (CSC) (LINK HERE)

CSC Controls are guidelines from Center for Internet Security (CIS) that provide organizations with a list of effective, high-priority tasks for defending against the most common and devastating cybersecurity attacks. They provide a starting point for any organization to improve its cybersecurity. CIS Controls are a set of cybersecurity defensive actions and best practices developed by the Center for Internet Security (CIS).

The current version is version 8, which contains **18 controls** and **153 safeguards** (i.e. Sub controls) in total and they are aimed at preventing pervasive and harmful attacks, as well as offer support compliances in a multitude of frameworks.

- CIS Control 1: Inventory and Control of Enterprise Assets
- CIS Control 2: Inventory and Control of Software Assets
- CIS Control 3: Data Protection
- CIS Control 4: Secure Configuration of Enterprise Assets and Software
- CIS Control 5: Account Management
- CIS Control 6: Access Control Management
- CIS Control 7: Continuous Vulnerability Management
- CIS Control 8: Audit Log Management
- CIS Control 9: Email and Web Browser Protections
- CIS Control 10: Malware Defenses
- CIS Control 11: Data Recovery
- CIS Control 12: Network Infrastructure Management
- CIS Control 13: Network Monitoring and Defense
- CIS Control 14: Security Awareness and Skills Training
- CIS Control 15: Service Provider Management
- CIS Control 16: Application Software Security
- CIS Control 17: Incident Response Management
- CIS Control 18: Penetration Testing

It has 3 implementation groups (i.e IG 1, IG 2 and IG3) which guides organization of different scale and sizes on how to implement the CIS controls depending on their IGs

NT: The image above links to CIS website for more details on Implementation Groups (IGs)

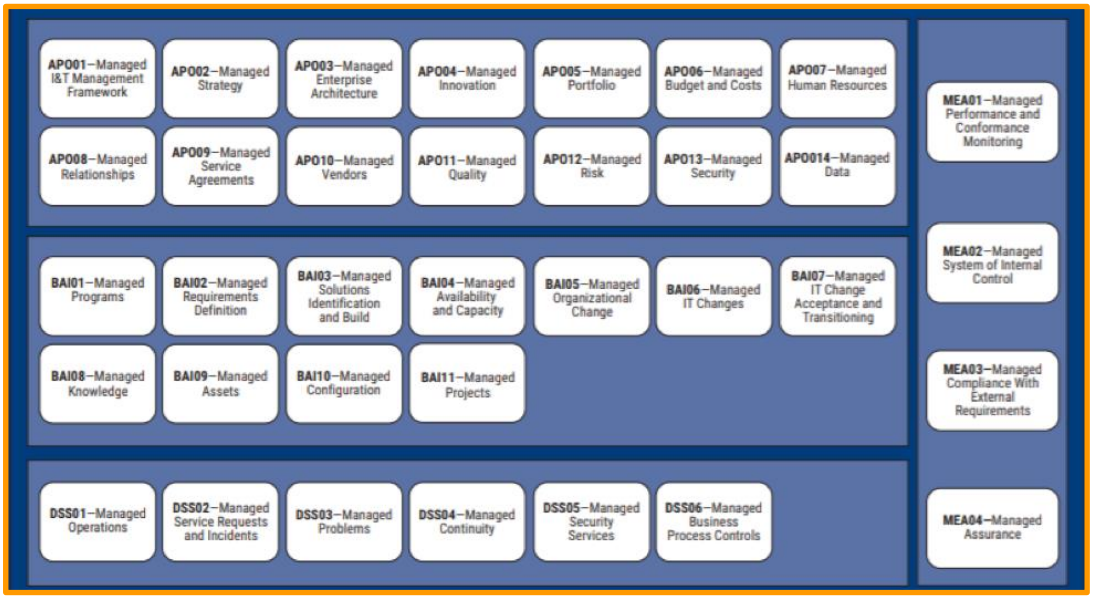
COBIT 2019 - FRAMEWORK FOR GOVERNANCE & MANAGEMENT OF IT (LINK HERE)

The COBIT framework is a good-practice framework for **governance** and **management** of enterprise IT. As part of its principles, the framework is set out to separate Governance of IT from the Management of IT, whilst enabling a holistic approach and applying a single integrated framework.

The framework consists of 5 domains and 40 processes:

- **Governance of Enterprise IT:** it ensures that enterprise objectives are achieved by evaluating stakeholder needs, setting direction; and monitoring compliance and progress against agreed-on objectives
  - Evaluate, Direct and Monitor (EDM) – 5 processes

- **Management of Enterprise IT** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives
  - Align, Plan and Organize (APO) – 14 processes
  - Build, Acquire and Implement (BAI) – 11 processes
  - Deliver, Service and Support (DSS) – 6 processes
  - Monitor, Evaluate and Assess (MEA) - 4 processes



Overall, COBIT ensures quality, control, and reliability of information systems in an organization, which is also the most important aspect of every modern business. One of the main principles of COBIT is to take a holistic approach to governance and work with IT, auditing, and management to create effective and enterprise-wide governance using certain ‘enablers’.

NIST 800-53 (LINK HERE)

The NIST 800-53 is a cybersecurity standard and compliance framework developed by the National Institute of Standards in Technology. It's a continuously updated framework that tries to flexibly define standards, controls, and assessments based on risk, cost-effectiveness, and capabilities.

NIST SP 800-53 was created to provide guidelines that improve the security posture of information systems. It does this by providing a catalog of controls that support the development of secure and resilient information systems. These controls are operational, technical and management safeguards that when used maintain the confidentiality, integrity and availability (CIA triad) of information systems. The latest iteration of this publication is Revision 5.

NIST CSF - (Cyber Security Framework) - LINK HERE

NIST CSF provides a flexible framework that any organization can use for creating and maintaining an information security program. NIST 800-53 and NIST 800-171 provide security controls for implementing NIST CSF.

This framework addresses the lack of standards when it comes to cybersecurity and provides a uniform set of rules, guidelines, and standards for organizations to use across industries.

The NIST Cybersecurity Framework (NIST CSF) is widely considered to be the gold-standard for building a cybersecurity program. Whether you're just getting started in establishing a cybersecurity program or you're already running a fairly mature program, the framework can provide value — by acting as a top-level security management tool that helps assess cybersecurity risk across the organization.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities.

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References

PCI DSS (LINK HERE)

PCI DSS (Payment Card Industry Data Security Standard) is a set of requirements that was established by the PCI SSC (i.e. Security Standards Council) to protect card holders data. The PCI DSS contains a set of **12 requirements** across **6 Goals,** and it is applicable to every entity that **PROCESSES, STORES or TRANSMIT** cardholders data.

The PCI DSS contains **12 requirements** (i.e. controls) which are the minimum security standard to protect and secure payment card data during processing, handling, storage, and transmission. All businesses that handle payment card data, no matter their size or processing methods, must follow these requirements and be PCI compliant.

PCI DSS SCOPE

PCI deIncludes all systems, networks, and applications that process, store, or transmit cardholder data, and also systems that are used to secure and log access to the systems in scope

The whole purpose of the PCI DSS is to protect card data from hackers and thieves. By following this standard, you can keep your data secure, avoiding costly data breaches and protecting your employees and your customers.

PCI DSS Stakeholders

- **Card Holder:** The individual that owns the credit card (i.e. YOU)
- **Issuer:** The bank/ entity that issues the card to the cardholder (i.e. Barclays Bank, Revolut etc)
- **Merchant:** A vendor that sells goods or provides services to people in exchange for money through different means including electronic means and collections (e.g. Zara Store, Easy Jet, KFC, JD SPorts etc.). They often have POS or website where cardholder inputs their card details to shop for goods/ services
- **Acquirer:** The bank or entity that the merchant uses for collections. E.g the bank that gave the POS to the Merchant
- **Service Provider:** A third party organization that provides services to merchants or entities whereby it involves them having access to credit card details, or enables them to store, process or transmit credit card details e.g. AWS, Microsoft Azure
- **Payment Brands:** The payment brands are also known as the PCI Security Standards Council. This is the coalition of Credit Card Providers that formulated PCI DSS. They include VISA, MASTERCARD, AMEX, JCB & DISCOVER

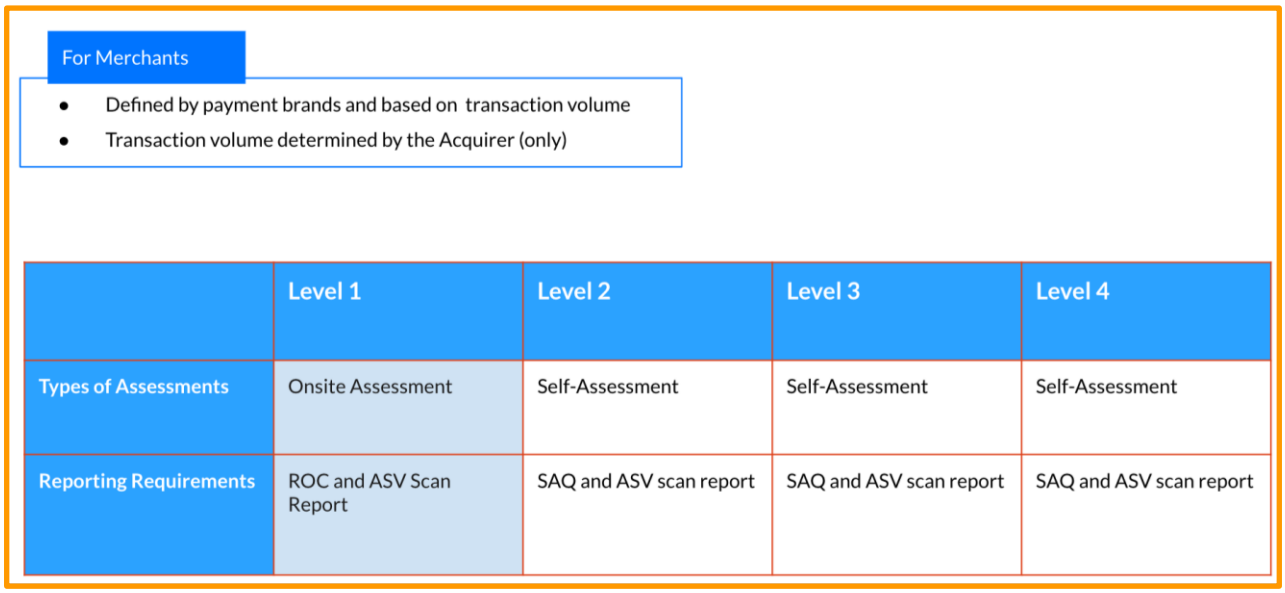
PCI DSS LEVELS & REPORTING REQUIREMENTS

PCI DSS uses levels to determine the reporting requirements of **merchants** and **service providers.** These levels are based on the total number of transactions that are processed by the entity (i.e., merchant or service provider) in a calendar year.

The levels also vary across different **payment brands.** For instance, as a merchant to VISA, if an entity processes between 2.5 million to 6 million and above transaction, the merchant will be classified as LEVEL 1 and as such will be required to perform an **Online Assessment** instead of **Self Assessment** to demonstrate compliance with PCI DSS requirements.

For Merchant, there are 4 Levels, (i.e. Level 1 - Level 4), only the LEVEL 1 merchants are required to perform **Onsite Assessment** through a 3rd Party Auditor/ PCI Qualified Security Assessor (PCI QSA) to demonstrate compliance with PCI DSS. Merchants that are categorized at other levels asides Level 1 are only required to demonstrate compliance with PCI DSS through a Self Assessment Questionnaire. Also all levels must provide ASV Scan Report in addition to their SAQs (for self assessment) or ROC (for onsite assessment)

The common Self Assessment Questionnaire that I have assessed is the SAQ Type D. The are other types of SAQs (such as SAQ A, SAQ A-EP, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT, and SAQ P2PE)



	Level 1	Level 2	Level 3	Level 4
Types of Assessments	Onsite Assessment	Self-Assessment	Self-Assessment	Self-Assessment
Reporting Requirements	ROC and ASV Scan Report	SAQ and ASV scan report	SAQ and ASV scan report	SAQ and ASV scan report

For Service Provider, there are 2 Levels (i.e. Level 1 and Level 2). Similarly, only the LEVEL 1 service providers are required to perform **Onsite Assessment** through a 3rd Party Auditor/ PCI Qualified Security Assessor (PCI QSA) to demonstrate compliance with PCI DSS. LEVEL 2 Service Providers users relevant SAQ depending on the applicable SAQ types to demonstrate compliance with PCI DSS. In addition to these, they must also provide ASV Scan Reports

For Service Providers

- Defined by the payment type according to transaction volume and/or type of service provider
- Determined by the Payment Brand or Acquirer (or by service provider).

	Level 1	Level 2
Types of Assessments	Onsite Assessment	Self-Assessment
Reporting Requirements	ROC and ASV	SAQ D and ASV scan report

Approved Scanning Vendor Scan (ASV SCAN)

An Approved Scanning Vendor (ASV) is an entity that can perform ASV scans that will validate adherence to the external scanning requirement as per PCI DSS Requirement. The ASV must be approved by the PCI SSC and will then be added to the list of Approved Scanning Vendors. Quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV).

PCI Internal Security Assessors (ISA)

Internal Security Assessor (ISA) is a designation given by the PCI Security Standards Council to eligible internal security audit professionals working for a qualifying organization. The ISA Program provides an opportunity for eligible internal security audit professionals of qualifying organizations to receive PCI DSS training and certification that will improve the organization's understanding of the PCI DSS, facilitate the organization's interactions with QSAs, enhance the quality, reliability, and consistency of the organization's internal PCI DSS self-assessments, and support the consistent and proper application of PCI DSS measures and controls.

PCI Qualified Security Assessors (QSA)

A Qualified Security Assessor (QSA) is an independent security organization that has been qualified and approved by the Payment Card Industry Security Standards Council (PCI SSC) to confirm and validate an entity's compliance with the PCI Data Security Standard (DSS). Examples of such companies include KPMG, EY, PWC, Deloitte, Accenture etc.

A QSA is responsible for the assessment of security controls within an organization. Their goal, in part, is to understand and document the extent to which the controls are configured correctly, operating as expected, and producing the desired outcome associated with that security control and the controls to which it interconnects.

PCI DSS Report On Compliance (ROC)

A Report on Compliance (ROC) is a form that must be completed by all Level 1 Visa merchants undergoing a PCI DSS (Payment Card Industry Data Security Standard) audit. A Level 1 merchant is one who processes over 6 million Visa transactions in a year. The RoC is developed through a thorough assessment completed by a QSA that includes an onsite audit and review of controls. After an auditor tests your controls and obtains documentation of your processes, a summary of findings is developed which culminates in a final RoC.

Every RoC is organized according to the PCI Security Standards Council's specifications for a qualified RoC which is derived from the RoC Reporting Template provided to all QSAs. The standardization of reporting allows your organization to provide every stakeholder, client, or interested party with a clear representation of your status on PCI compliance.

PCI DSS Self Assessment Questionnaire (SAQ)

An SAQ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with PCI DSS. The SAQ will require you to attest how your organization meets PCI DSS standards. With a series of yes or no questions, the SAQ will state each PCI requirement and the expected testing, then ask whether the **CONTROL** is:

- In place
- In place with a Compensating Control Worksheet or CCW*
- Not in place
- N/A
- Not tested

Compensating controls are considered when an organization cannot meet a requirement exactly as stated (due to technical or business constraints) but has sufficiently mitigated the risk.

If you answer "no" to any of the questions, you'll be required to explain what your plans are for remediating the gap and the expected timeline. You must meet each control to be compliant with PCI DSS. There are 8 types of self-assessment questionnaires for merchants and service providers to prove their PCI DSS compliance:

- SAQ A,
- SAQ A-EP,
- SAQ B,
- SAQ B-IP,
- SAQ C,
- SAQ C-VT,
- SAQ D

Compensating Control Worksheet (CCW)

Compensating controls are an alternate solution or measure to a security or compliance requirement that is not feasible for the organization to implement in its original form. PCI Council defines compensating controls as "Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical

or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls". Therefore, Compensating controls must:

- Meet the intent and rigor of the originally stated PCI DSS requirement
- Provide a similar level of defense as the original PCI DSS requirement
- Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
- Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement."

So, this means that any organization which cannot meet the requirements of PCI DSS must investigate and deploy similar levels of security measures that meet the specific standard requirements.

Attestation on Compliance (AOC)

An Attestation of Compliance (AoC) is a declaration of an organisation's compliance with Payment Card Industry Data Security Standard (PCI DSS). It is testimony that an organisation can successfully demonstrate exceptional security best practices to secure cardholder data. An AoC must be completed by a Qualified Security Assessor (QSA) or the merchant if the merchant's internal audit performs validation.

Assessments result in either a Report on Compliance (RoC), AoC or both. The documents are provided to the merchant's credit card acquirer each year to prove compliance with the PCI DSS.

SOX - 404 (LINK HERE)

The Sarbanes–Oxley Act of 2002 commonly called SOX, is a United States federal law enacted on July 30, 2002. It is named after sponsors U.S. Senator Paul Sarbanes and U.S. Representative Michael G. The bill was enacted as a reaction to a number of major corporate and accounting scandals including those affecting Enron and other organizations.

SOX is an act that mandates that all publicly listed entities must establish an appropriate internal control environment to mitigate risks related to financial processing and reporting, and that publicly listed entities must be audited by an independent 3rd party organization.

Many organizations (including some that are not subject to SOX) use SOX reviews to enhance internal controls, implement best practices, and improve business efficiency. Section 302 and 404 guarantees that the security of data cannot be hidden from auditors, and security breaches must be reported. (ELC & ITGC).

SOX focuses on the evaluation of the internal control vis-à-vis management's responsibility for adequate internal control structure and management's assessment of the effectiveness of the control structure.

Through application of SOX principles, Auditors review the design and implementation of management controls over financial processing and reporting within an organization. The control include:

- Entity level controls (ELC)
- IT General Controls (ITGC)
- IT Application Controls (ITAC)

I have experience in leading teams on SOC ITGC controls testing and I have managed several engagements where I am responsible for planning, execution and reprinting on such engagements.

Disaster Recovery and Business Continuity (DR/ BCP)

Disasters are inevitable but mostly unpredictable and they vary in type and magnitude.

In preparation for disasters, organizations need to have an effective Disaster Recovery Plan & Business Continuity Plan (DRP/BCP) to minimize disaster losses and ensure continuity within the organization's acceptable Recovery Time Objective (**RTOs**) and Recovery Point Objective (**RPO**).

In every disaster planning process, a risk assessment must be carried out, Business impact analysis, and a mitigation strategy before developing the actual Business Continuity Plan.

The backup policy must be in synchronization with the DRP/BCP to ensure RPO and RTO objectives are met.

It is also imperative that Disaster Recovery tests are performed periodically to ensure that in the event of any disaster, the organization can successfully fail-over to the DR site and continue business as usual in line with the specified RTO and RPO.

Key Details to Know with Respect to Disaster Recovery Planning

Disaster Recovery / Response Plan: A disaster recovery plan (DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events. The plan contains strategies on minimizing the effects of a disaster, helping an organization to quickly resume key operations or continue to operate as if there was no disruption.

Disaster Recovery Testing Methods: There are different methods for testing a Disaster Recovery plan to evaluate its effectiveness in the event of a disaster and to also check the organization's readiness to respond and recover from the event:

- Walkthrough Testing:
- Simulation Testing:
- Checklist Testing:
- Full Interruption Testing:
- Parallel Testing:

Business Continuity Plan: A Business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the

event of a disaster. Business continuity plans (BCPs) are prevention and recovery systems for potential threats, such as natural disasters or cyber-attacks.

Business Impact Analysis (BIA): A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries.

Recovery Time Objective: The recovery time objective (RTO) is the amount of time or real time during or after a disaster that can elapse without a business restoring its services and processes to acceptable levels before it will experience intolerable consequences associated with the disruption.

Recovery Point Objective: Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization.

Secure by Design (Secure SDLC)

Applying a security mindset in the development and deployment of IT systems. From scoping, planning, blueprinting, design, testing, deployment, continuous support. This is a concept that helps us to build and implement secure systems to enable protection of data and ensure system availability

Data Privacy

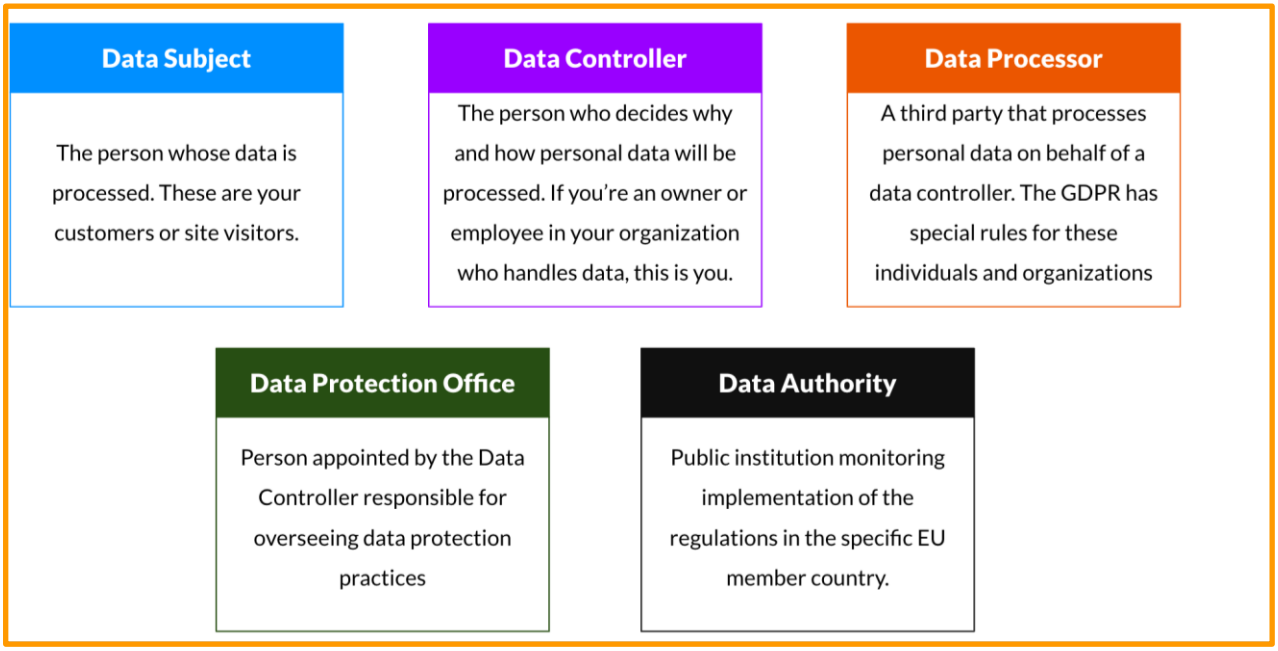
Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. Data privacy ensures that rights to determine how a data will be processed, stored, used and retained lies with the Data subject (i.e. the individual that the data applies to).

For entities, ensuring data privacy is critical as they owe the responsibility to data subjects in terms of collecting data lawfully based on consent, using the data for the intended purpose, retaining the data within the legal requirement, evaluating use of processors / subprocessors, and employing controls to secure the data from unauthorized access or disclosure, and ensuring that laws relating to data privacy are respected when dealing with PERSONAL INFORMATION.

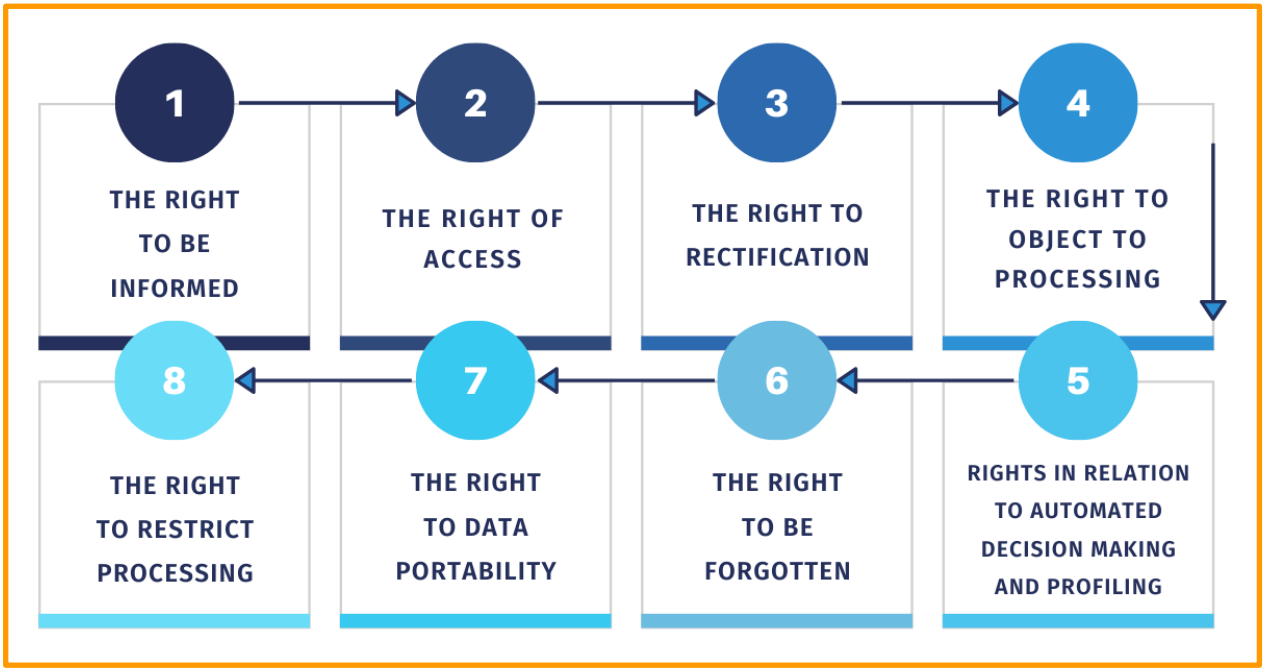
There are a lot of Privacy rules, but one stringent rule is the EU GDPR which focuses on protecting EU residents data and applies to entities that process or target EU residents and citizens.

Key Details to Know with Respect to Data Privacy

Stakeholders



Data Subject Rights

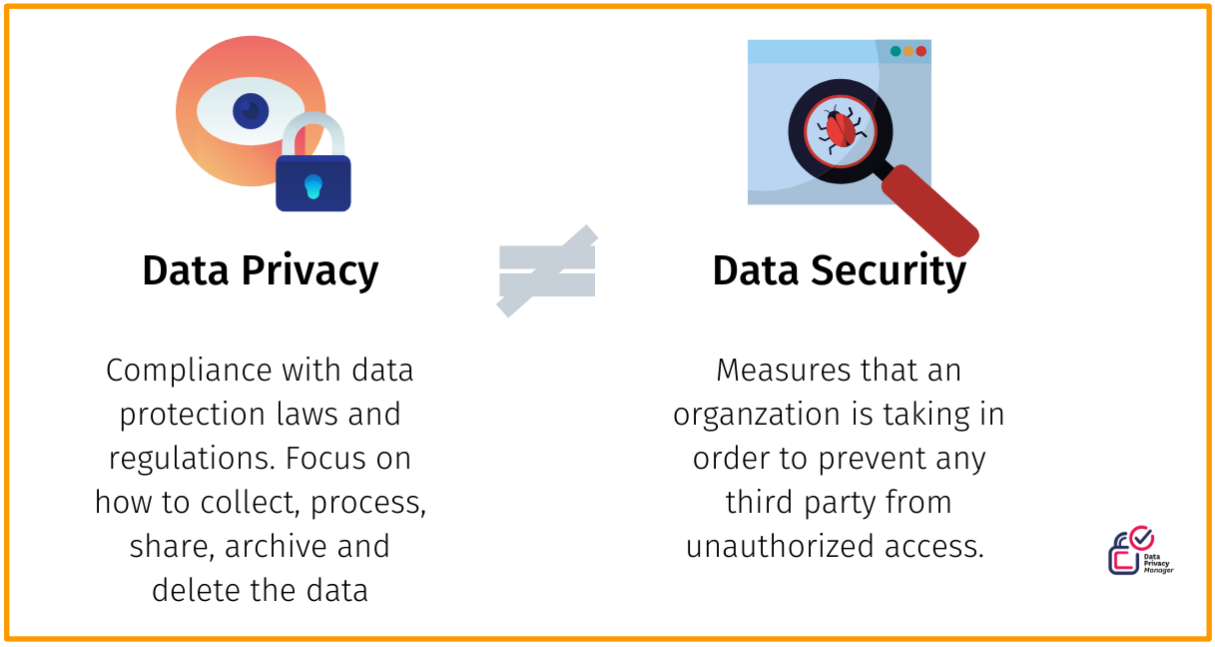


Data Security vs Data Privacy

Data security is different from Data privacy in terms of scope and focus. **Data security** focuses on implementing controls such as Access control, encryption, data loss prevention etc. to prevent unauthorized access to data, while **Data Privacy** focuses on lawful collection, processing, transferring, storing and retention of data in line with applicable laws and data subject's interest.

A combination of Data Security and Data Privacy gives an organization appropriate level of Data Protection

(i.e., **Data Protection = Data Security + Data Privacy)**



ITIL Framework

IT Infrastructure Library (ITIL) provides the guidance and approach of how IT service organizations can improve on service delivery. More importantly it provides the knowledge that will enable IT professionals to support their organization on their journey to digital transformation. With 5 guiding principles, ITIL provides the framework that enables ITSM services to be strategized, designed appropriately, transitioned effectively, operated optimally and continuously improved.

What this means is that we must first ensure that our process for ITSM services like ServiceDesk, Change and Configuration Management, Incident Management, and IT Asset Management must be strategically designed to align with, and support the Business Strategy.

The ITIL framework is a set of IT Service Management best practices and processes that helps organizations to align their IT service delivery with business goals. **ITIL Lifecycle includes:**

Service strategy

Facilitates organizations to set business goals and develop a strategy to meet customer requirements and priorities.

Service design

Includes designing of processes and functions. This covers designing of service management processes, technology, infrastructure and products.

Service Transition

Focuses on maintaining the current state of service while deploying new organizational change. It ensures that risk and impact are in control so that there are no interruptions to any ongoing services.

Service Operation

Service operation ensures day to day operational tasks are seamless and is responsible for monitoring infrastructure and application related services. This enables businesses to meet customer's requirements and priorities.

Continual Service Improvement

This is a part of quality check that aims towards continuous improvement of processes in an incremental manner. This happens throughout the service lifecycle.

COMPETENCY BASED (INTERVIEW QUESTIONS)

Do you have experience of working in an IT Assurance / Advisory Role?

Yes I have experience working on Cyber GRC, Information Assurance, IT Risk and Advisory related projects. I have been part of the GRC implementation project and also supported ISO 27001 implementation for an entity during the implementation of their ISMS.

In addition, I have experience with data assurance stemming from a migrations project where I was responsible for reviewing the migration process and providing assurance on the completeness and accuracy of the data that was migrated and the approach that was followed.

I have expertise in implementing controls in line with security frameworks such as ISO 27001, CIS CSC, NIST, and CSA CCM.

Do you have experience of managing aspects of an organization's external audit relationship?

In my previous role, as a team lead on different engagements, I was responsible for managing relationships with clients, senior management, and control operators. Specifically, I led conversations on scope discussions, agreed on work approaches, coordinated client care/ check-ins, ensured to create a collaborative environment with the client contact, and provided expert opinion and recommendations on how to improve their internal audit programs.

As an individual, I understand the importance of team collaboration and I ensure to build good relationships with my clients and colleagues.

Walk me through experience auditing or evaluating ISO 27001? OR Tell me about your experience with ISO 27001?

I have experience assessing and implementing ISO 27001 in my previous role. I have also performed Gap assessment, current state assessment and readiness assessment for ISO 27001 audit reviews in the past.

I supported the team on the ISO 27001 audit and readiness assessments in the past. In this role, I focused on evaluating Clauses 4 to 10 by requesting for evidence from the entity to provide reasonable assurance that the entity could meet the requirements.

I started by evaluating the Scope of the ISMS which should capture the entities and its context, the interest of the stakeholders, the scope of the ISMS including people, processes and technologies, the roles and responsibilities of senior leadership.

I also assessed the process in place for performing risk assessment by reviewing the enterprise risk management policy, and evaluating a sample of risk assessment that was performed within the period under review.

I obtained and evaluated the Statement of Applicability to the Annex A controls to determine the Annex A controls that were scoped in as part of the audit review, and what has been scoped out. My focus here is to determine what the rationales were for scoping out any of the Annex A controls.

I then reviewed evidence provided for each of the applicable control requirements across the 14 domains of ISO 27001. When testing my controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to document and conclude on the findings. There was no major finding but there were minor findings and OFIs (i.e. Opportunity For Improvements). I made recommendations on the findings and I followed up on the remediation of these findings?

FOLLOW-UP: What were the findings you noted?

Firstly, there were no procedures for certain controls such as user access reviews, and the use of cryptographic / encryption within the control environment.

Secondly, there was no provision for periodic review of the information security policies and procedures. In addition, certain controls were not performed in line with the management-approved frequencies. For instance, there were certain instances where backup of critical devices were not performed.

We noted these issues and reported it in our final report to the client with appropriate recommendations.

What is the difference between ISO 27001 and ISO 27002

The difference between the 2013 version of ISO 27001 and ISO 27002 is that the ISO 27001 is a certification standard which contains the requirements for an entity to build their ISMS and also ensure compliance with ISO 27001 requirements. The ISO 27001 contains Clauses 4 to 10 which are mandatory requirements, and also contains the **Annex A controls which contains 14 Domains and 114 Controls.**

ISO 27002 is an implementation guidance and not a certification standard. It contains guidance on how to implement the controls that are contained in the **Annex A of ISO 27001**.

There is a new version for both ISO 27001 and ISO 27002 which came out in 2022. Although not much on it in terms of entities implementing against it, I learned that the Annex A controls have been reduced to 98 from the 114 controls in the 2013 version.

What are the key expectations that you focus on when assessing an entity's compliance with ISO 27001 Standard?

When auditing ISO, these are the key expectations or information that I ask for includes:

- The Scope document that contains Scope of the ISMS and Context of the organization
- The Role matrix that contains roles and responsibilities for the senior management
- The Risk Assessment document showing that information security risks were assessment and treated
- The information security policies and procedures
- The statement of applicability showing the list of applicable controls and also rationale for excluding non-applicable controls
- Sample Evidence to evaluate the Test of Design (TOD) and the Test of Operating Effectiveness (TOE)

These are some of the key documents I expect to be able to deliver on the audit reviews and report my findings.

Walk me through experience evaluating / assessing an entity for PCI DSS? OR Tell me about your experience with PCI DSS?

I have experience in assessing an entity's compliance with PCI DSS requirements in my previous role. I have also performed **readiness assessment** for PCI DSS audits with ISAs as well. In addition, I have performed a gap assessment / current statement assessment to evaluate if the entity has implemented necessary controls to adequately meet the PCI DSS requirements.

I supported the team on the PCI DSS readiness assessments in the past. In this role, I focused on evaluating controls implemented to meet the 12 requirements by requesting for evidence from the entity to provide reasonable assurance that the entity could meet the requirements.

I started by evaluating the Scope of Cardholder Data Environment, which should capture the people, processes and technologies that are involved in processing, storing or transferring cardholders data.

I also assessed the process in place for performing risk assessment by reviewing the enterprise risk management policy, and evaluating a sample of risk assessment that was performed within the period under review.

I reviewed the controls in-line with SAQ D form, and I obtained the document showing the applicable PCI DSS requirements to determine the control requirements that were scoped in as part of the audit review, and what has been scoped out. My focus here is to determine what the rationales were for scoping out any of the 12 requirements.

I then reviewed evidence provided for each of the applicable control requirements across the 12 requirements. When testing my controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to document and conclude on the findings. There were certain findings where we noted that certain controls were not in place, and no evidence of compensating controls were provided as well. I made recommendations on the findings and I followed up on the remediation of these findings?

Specifically, the quarterly network scans were not performed based on the appropriate frequency and we reported this to the senior management as part of the readiness report.

Walk me through experience evaluating an entity for a SOC 2 Attestation Report? OR Tell me about your experience with SOC 2 Attestation Report?

I have performed attestations and reviews in line with AICPA SOC2 controls for service organizations. My experience has largely been on SOC 2 Type 1 and Type 2 where I have assessed how the entities have implemented controls to demonstrate compliance with the 5 Trust Services Criterias (TSC) being Security, Availability, Processing Integrity, Confidentiality and Privacy.

I have led / supported teams and I've also worked on the SOC 2 reviews in the past, and in this capacity, I focused on testing and evaluating controls that have been implemented to meet the AICPA requirements for the selected TSC (i.e. Security, Processing Integrity, Availability and Confidentiality) by requesting for evidence from the entity to provide reasonable assurance that the entity could meet the requirements.

I assessed the processes in place for performing risk assessment by reviewing the enterprise risk management policy, and evaluating a sample of risk assessment that was performed within the period under review.

I reviewed the controls that have been implemented for logical and physical access security to critical infrastructure, change management controls, network security controls, and operations management controls.

I performed walkthroughs with relevant personnel to understand the processes within the entity, and obtained evidence to test the Design of the controls and also to test the operating effectiveness of these controls.

When testing controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to conclude on the control design and effectiveness, and also documented my findings. For areas where we noted deficiencies, I made recommendations on the findings and I followed up on the remediation of these findings.

Walk me through experience evaluating / assessing an entity for NIST Framework? OR Tell me about your experience with NIST Framework?

During a Cyber risk advisory project for an insurance entity, I was tasked with assessing the entity's compliance with the NIST Cybersecurity Framework to protect their information asset and mitigate risks. Specifically, I reviewed how the entity controls have be implemented in line with the core objectives of the NIST framework which includes:

- **Identify**ing assets, vulnerabilities and threat
- **Protect**ing assets from unauthorized access
- **Detect**ing threats efficiently
- **Respond**ing to threats and risks, and
- **Recover**ing efficiently from security incidents and related events.

When testing controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to conclude on the control design and effectiveness, and also documented my findings. For areas where we noted deficiencies, I made recommendations on the findings and I followed up on the remediation of these findings.

Walk me through experience evaluating / assessing an entity for CIS Critical Security Control (CSC) Framework? OR Tell me about your experience with CSC Framework?

I led the IT risk advisory team on a Cyber Risk advisory project for a client in the banking sector. On this project, I was task with assessing the technical controls that have been implemented using the CIS critical Cybersecurity Framework. Specifically, I reviewed how the entity controls have be implemented in line with the Implementation Group 1 (i.e. IG 1) of the CIS CSC controls.

I reviewed controls around Asset management, Access management, configuration management, change management, backup and disaster recovery, user identification and authentication, vulnerability management, and network security controls.

When testing the controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to conclude on the control design and effectiveness, and also documented my findings. For areas where we noted deficiencies, I made recommendations on the findings and I followed up on the remediation of these findings.

Walk me through experience evaluating / assessing an entity for CSA Cloud Control Matrix (CCM)? OR Tell me about your experience with CSA CCM?

During an audit of an insurance entity, one of the critical systems in scope is a cloud-based solution and we needed to include this in our assurance testing. In addition, the entity has implemented a hybrid cloud model where certain infrastructure were in the cloud and others were on-premise within the organization. Our scope of testing covered the cloud environment and I leverage the Cloud Control Matrix (CCM) from the Cloud Security Alliance to come up with an approach for evaluating the cloud element for the entity as a Cloud service customer.

I focused on the controls relating to Cloud Service Customer, and also controls where there is a shared responsibility between the cloud service customer and the cloud service provider. Using the CCM as my guide, I was able to identify and test the controls that are relevant to the entity as a cloud service customer.

I reviewed controls around Audit & Assurance, Business Continuity Management, Cryptographic and use of Encryption, Identity and Access management, configuration & change management, Logging and Monitoring, Security incident management, data security and privacy lifecycle management and other GRC related controls.

When testing the controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to conclude on the control design and effectiveness, and also documented my findings. For areas where we noted deficiencies, I made recommendations on the findings and I followed up on the remediation of these findings.

Tell me about your understanding of Cloud computing? Tell me your experience with cloud computing?

For me, Cloud computing is the future for most organizations given its efficiency, cost saving ability and scalability. Cloud computing enables organizations to share computing resources (such as storage, networking, compute, and servers) from a shared pool.

The service-based architecture have 3 different service models such as

- Infrastructure as a Service
- Platform as a Service, and
- Software as a Service

Most organizations already use the software as a service which enables them to leverage applications that are managed by third-party organizations to support their business processes.

I have a bit of experience with AWS cloud service and I am currently studying for my AWS cloud practitioner to broaden my understanding of cloud services from a major cloud service provider.

During an audit of an insurance entity, one of the critical systems in scope is a cloud-based solution and we needed to include this in our assurance testing. In addition, the entity has implemented a hybrid cloud model where certain infrastructure were in the cloud and others were on-premise within the organization. Our scope of testing covered the cloud environment and I leverage the Cloud Control Matrix (CCM) from the Cloud Security Alliance to come up with an approach for evaluating the cloud element for the entity as a Cloud service customer.

I focused on the controls relating to Cloud Service Customer, and also controls where there is a shared responsibility between the cloud service customer and the cloud service provider.

When testing the controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to conclude on the control design and effectiveness, and also documented my findings. For areas where we noted deficiencies, I made recommendations on the findings and I followed up on the remediation of these findings.

Tell me about your experience with cloud security? Tell me about a cloud security advisory project you have been on? What controls would you focus on for security of cloud environment

During an audit of an insurance entity, one of the critical systems in scope is a cloud-based solution and we needed to include this in our assurance testing. In addition, the entity has implemented a hybrid cloud model where certain infrastructure were in the cloud and others were on-premise within the organization. Our scope of testing covered the cloud environment and I leverage the Cloud Control Matrix (CCM) from the Cloud Security Alliance to come up with an approach for evaluating the cloud element for the entity as a Cloud service customer.

I focused on the controls relating to Cloud Service Customer, and also controls where there is a shared responsibility between the cloud service customer and the cloud service provider. Using the CCM as my guide, I was able to identify and test the controls that are relevant to the entity as a cloud service customer.

I reviewed controls around Audit & Assurance, Business Continuity Management, Cryptographic and use of Encryption, Identity and Access management, configuration & change management, Logging and Monitoring, Security incident management, data security and privacy lifecycle management and other GRC related controls.

When testing the controls, I evaluated the existence of a management-policies and procedures in place that specifies the intention of the management. Subsequently, I obtained sample evidence to test the design of the control and also the operating effectiveness of the control during the period we are reviewing.

Effectively, after testing the controls I was able to conclude on the control design and effectiveness, and also documented my findings. For areas where we noted deficiencies, I made recommendations on the findings and I followed up on the remediation of these findings.

What is your understanding of the Shared Responsibility Model for Cloud security

As a Cloud Service Customer (CSC), having your infrastructure and services in the cloud does not completely eliminate IT and information security risks from the cloud service customer. A Cloud Service Provider (CSP) is usually responsible for SECURITY **OF** THE CLOUD while the Cloud Service Customer (CSC) will be responsible for SECURITY **IN** THE CLOUD.

For the Infrastructure as a Service (Iaas) model, the **Cloud Service Customer** (CSC) is responsible for security of their cloud workload, resources and data including managing access, patching the OS, web application firewall, data encryption and security incident management, While the **Cloud Service Provider (CSP)** will security the physical server and data center

Technically, the responsibility for securing the cloud is shared depending on the service model (i.e. whether IaaS, Paas, or SaaS)

This is largely my understanding on the subject Matter.

What is your understanding of Data Privacy? What controls would you consider implementing to ensure data privacy?

Data privacy is the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. Just as someone may wish to exclude people from a private conversation, many online users want to control or prevent certain types of personal data collection.

Access Control

Protecting user-level access to information systems is my first line of defense, and proper account management and enforcement are paramount. The control of accounts, enforcement, and features is accomplished using authentication management and directory systems like Active Directory and Lightweight Directory Access Protocol (LDAP). These controls extend beyond user directories, including system accounts, networking equipment, and databases.

Systems integrity

Are the systems free of exploits? Safeguarding the system's integrity with technical and operational controls should be a top priority. This starts with installing malicious code blocking and spam protection mechanisms; these controls block endpoint attacks, working best in unison with user awareness and training programs.

Configuration management

Are your configuration changes authorized? Configuration management controls cover the policies and procedures for the authorized changing of system configurations. They prevent administrators' unauthorized adjustments and require all changes to be documented. These controls ensure all configurations are designed and maintained with security in mind.

Security assessment and authorization

Vulnerabilities are weaknesses in an information system, security procedure, internal control, or implementation that can be exploited by a threat source. Here is where the fun starts for many—some call it "ethical hacking" with the end goal of identifying vulnerabilities and determining the overall security of your environment.

Security assessments provide point-in-time snapshots of your environment, starting with vulnerability and risk assessments all the way to complete penetration tests. Organizations should track all discovered risks with a Plan of Action and Milestones (POAM). These reports list all risks and their security impact, proposed dates to address, and suggested mitigation plans.

Incident response

The last critical data security control domain to put in place is a documented response plan detailing the handling of events based on data classification and incident criticality. Incident response plans typically fall under IT and security jurisdiction but should include contributions from other teams. hey help safeguard your business and assist in recovery

after a security incident. If you lack an incident response plan, you signal a weaker security commitment to auditors in addition to risking fines and legal action when inevitable incident management missteps occur.

Have you been on a Data privacy related project? What would you consider relevant to ensure appropriate data privacy

I will start by controlling network access with an authentication management system based on least privilege and separation of duties. Ensure system integrity with malicious code and spam protection, continuous system monitoring, and a BCDR plan. Manage configurations to ensure all changes are authorized and documented. Continually assess your security posture with vulnerability scans and risk tracking. Finally, create and maintain a tested incident response action plan in the event of an emergency.

Walk me through experience evaluating / assessing an entity for EU GDPR? OR Tell me about your experience with EU GDPR?