GRC 100 Project - Phase 1

By

Damsith Marasinghe

Students Cohort 3/14/2022

Submitted to: Erick Keith

TABLE OF CONTENTS

Abstract

Governess is the process of everyday decisions making that an organization should make in managing its business, while dealing with external and internal influences. Corporate governance involves organizational alignment, compliance and information privacy. The form of a business affects the governance strategy because the direction depends on the ownership. There are some basic corporate governance documents that a business may develop related to information security. CMMI (Capability Maturity Model Integration) is a model where you measure the maturity of an organization in terms of risks it takes. There are 5 levels of CMMI. First level is the initial state which can be thought of as a company just starting up whose processes are not controlled well and inconsistent. Organizations want to consider adopting the CMMI when they come online and need to consider internet security. Some of the advantages of CCMI model are having in-depth analysis of the processes inside the business in order to make effective improvements of processes. Disadvantages of CMMI are unsuitable security standards, not applicable and not compatible with some businesses. Open Compliance and Ethics Group are a nonprofit organization. OCEG's objective is to help people and organizations to reach their goals by circumventing uncertainty and perform with integrity. The Standards are about governance rules and laws that business, shareholders and owners must follow in order to keep their companies in the alignment with the rest of world. OCEG Membership Account Activity covers a lot of free information regarding standards, resources, events, which explain how business connects to life with principled performance, certifications, education and blog articles. According to Lawfulness(six lawful foundations), fairness, and transparency principle GDPR Article 5(1), personal data has to be processed lawfully, fairly and in a transparent manner with respect to the subject in concern. As far as differences between EU and US legislations, GDPR is more general than US tool to address particular use cases. Company's data protection strategy and compliance with GDPR requirements requires four people in general; Data controller, data custodian, data subject and data protection officer.

M1-2 – Concepts of Governance

Governess is the process of everyday decisions that an organization should make in managing its business. In this decision making process, organizations would have to deal with external and internal influences that affect how they control their activities. Examples are laws, regulations, and policies which are referred to as compliance. Businesses are also affected by the risks that they have to undergo when they make decisions for their organizations. The standards that apply to organization's compliance program can be categorized as regulatory, contractual and organizational requirements.

Corporate governance consists of organizational alignment, compliance and information privacy. Organizational alignment is considering the following factors before securing an organization. They are goals, governance, leadership style, philosophy, standards, values and policies. Compliance is making sure we are compliant with regulatory, contractual and organizational requirements. Information privacy is referred to as agreements that we have to sign in order to protect information when securing organizations.

The **form of a business** affects the governance strategy. In a single owner business (Proprietorship), it focuses mainly on profit, thereby enforcing very little effort on governance. The owner's business management style affects the governance of the business as he stipulates direction, target and objective of the business. Partnership business is owned by multiple owners where governance depends on the expertise of the owners involved and therefore more complicated than single owner business. The third form of business is corporations. In a corporation, the legal body is separate from the individual owners. The governance of a corporation depends on the legal document written when the corporation is formed. The business driver could be shareholders investments which in turn affects the governance of the business.

Some basic **corporate governance documents** that a business may develop related to information security or data protection are GPDR (General Protection Data Regulation of the European Union), CCPA (California Privacy Act), HIPPA (Health Care Industry Privacy Act), and PII (Personally Identifiable Information)

M1-3 – Capability Maturity Model Integration (CMMI)

CMMI (Capability Maturity Model Integration) is a model where you measure the maturity of an organization in terms of risks it takes, being in the range from a highly reactive state to a proactive one. Maturity of an organization impacts corporate governance.

There are **5 levels of CMMI**. First level is the initial state which can be thought of as a company just starting up whose processes are not controlled well and inconsistent. Second level can be thought of as state where processes are being managed and defined for projects but not documented as these are reactive. At the third level, processes are defined for the whole project policies and procedures are documented proactive state. At the 4th Level, processes are being managed quantitatively with assistance from senior managements for better proactive performance. During the fifth, level processes are being optimized nonstop looking for better efficiency and effectiveness.

Organizations want to consider **adopting the CMMI** when they come online and need to consider internet security. They need to align their business internet security with CMMI model after evaluating with Cybersecurity professionals where they fit in to the model between most reactive to most proactive risk scale. Business unit manager align their business according to goals, governance, leadership style, philosophy, values, standards and policies to considering the stage where they in the business.

Some of the **advantages of CCMI model** are having in-depth analysis of the processes inside the business in order to make effective improvements of processes, clearly defined objectives of the business processes are recognized, and better assessment of goals for future appraisals. Other advantages of CMMI are having deeper and clear understanding of the business process, can provide suggestions that work for the business, and progress and future planning can be assessed. **Disadvantages of CMMI** are security standards not being suitable for some businesses, not globally applicable to all priorities that some businesses may have, and some business processes and frameworks will not be compatible to be used together with CMMI model.

In a single owner business (**Proprietorship**), it focuses mainly on profit, thereby enforcing very little effort on governance. **Partnership** business is owned by multiple owners where governance depends on the expertise of the owners involved and therefore more complicated than single owner business. The governance of a **corporation** depends on the legal document written when the corporation is formed

M2-2 – OCEG Membership Account Activity

OCEG or Open Compliance and Ethics Group are a nonprofit organization. OCEG's objective is to help people and organizations to reach their goals by circumventing uncertainty and perform with integrity. The name GRC was created by OCEG which refers to the combination of potentials that integrate the governance, management and assurance of performance, risk and compliance activities. OCEG members include professionals from small and midsize businesses, large corporations and government agencies.

The **Standards** are about governance rules and laws that business, shareholders and owners must follow in order to keep their companies in the alignment with the rest of world. Policies develop the code of conduct that the organization's employees, management, shareholders must follow. Establishing a policy structure is the way to improvise policies that are passed. Organization must abide by them. Under GRC standards tab we can see GRC Assessment Tools Burgundy Book Sample Pages standard, GRC Capability Model - Arabic version standard, Policy Management Capability model standard, GRC Capability model (Red Book) Full Version standard, GRC Assessment Tools (Burgundy Book) 3.0 standard, OCEG GRC Capability Model (Red Book) Version 3 Practices standard, GRC-XML Spec and Schema standard, GRC solutions guide and other Spanish versions standard.

Free **resources** available under resource tab are OCEG Impact of Digitization Survey 2022, Webinar recording of "How to make GRC real (and Important) for our executive team, GRC Capability Model Arabic Version, Policy Management Capability Model, e-book on "Strong We-rounded Team", e-book on "Make a Winning Business Case Toolkit", Webinar recording on "Open Source Standards for Governance, Risk Compliance", and building blocks of GRC". Under this resource tab we can also see a lot useful illustrations such as "The New Imperative for Energy and Utilities", "Prevent Fraud by Segregating Roles", "Conducting Defensible Supply Chain Due Diligence", "Policy Management Step-by-Step", "Illustration – Audit Ready Access and Control"

Under **events** tab upcoming events such "Preparing for the Unexpected"- Integrated Policy Management is Key (June 2 and "The Impact of Digitalization on Your Enterprise Risk Profile" which is based on findings from OCEG Research (June 16). The strategy of business of connecting business to life is called **Principled Performance**. They use GRC and GRC Capability Model to apply the "Principled Performance". To achieve Principled Performance one must combine the roles; Governance and Strategy, Risk Management, Internal audit, Compliance management, Ethics and culture and IT and Security. The pillars of Principled Performance are Principled Purpose, Principled People, and Principled Pathway. **Ten universal outcomes of Principled Performance** are Achieve Business Goals, Emphasize Risk Aware Setting of Objectives and Strategic Planning, Improve Organizational Culture, Improve Stakeholder Confidence, Prepare and Protect the Organization, Prevent, Detect, and Reduce Adversity and Weaknesses, Motivate and Inspire Desired Conduct, Stay Ahead of the Game, Improve Reactive Efficiency, and Enhance Return and Values.

GRC **Certification** enhance your skill by either renewing your current certifications or just replace them altogether. These certifications are globally certified. Two types of certifications are available. They are GRC Professional and GRC Audit. The GRC Professional (GRCP) certification gives you the knowledge and skill to make you company GRC compliant. GRC Professional certification is the foundation for all other certification that a GRC professional must attain during their career. GRC Professional certification covers basic knowledge in the management of risk, internal controls, key functions of compliance, and how these must be combined for effective and proper governance.

Blog Article: The Critical Six Disciplines to Integrate GRC

As defined GRC is an integration of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity. As defined by an acronym GRACE-IT, these specific capabilities or skills are named as “Critical Six”, at least cover one aspect of GRC. The six skills defined by the acronym are Governance & Strategy, Risk & Performance, Audit & Assurance, Compliance & Quality, Ethics & Culture, and Information Technology

M2-3 – GDPR SIA Partners

According to Lawfulness, fairness, and transparency principle **GDPR** Article 5(1), personal data has to be processed lawfully, fairly and in a transparent manner with respect to the subject in concern. **Lawfulness** contains six lawful foundations for processing. They are consent, contract, and legal obligation, protection of vital interests, public task, and legitimate interest. **Fairness** is how reasonably you process personal data when expected from you. You should process your data in responsibly, so that you do not store, collect data in a deceiving manner. **Transparency** is the principle of clear, open and reliable communication of personal data. Being transparent will allow the individual to us the law of GDPR if he or she intends to do so. **Purpose limitation** is being clear about your reason to collect and process your data from the beginning. **Data minimization** provides limitation to collect, store and process personal data that is enough to fulfill the needed service. The **accuracy** indicates that you responsibly account for the personal data correctly and accurately. **Storage limitation** limits keeping personal data only for a specific period.

As far differences between **EU and US** legislations, GDPR is more general than US tool to address particular use cases but EU's intention was to enforce universal data privacy laws that would supersede all the prior ones. Another big difference is US is more worried about the data integrity as a commercial asset whereas EU strictly enforces individual right before business rights.

Data controller determines the purposes for which personal data is processed. **Data custodian** maintains access to others, produces reports for others, produces, interprets, and distributes information on datasets, logs all information access grants, and safeguards to protect the confidentiality, integrity, and availability of the information asset dataset. **Data subject** defines a living individual whose personal data is collected, held or processed by a company. A **data protection officer** is an organization security leader needed by GDPR. He is responsible for company's data protection strategy and compliance with GDPR requirements.

M3-1 – Enterprise Architecture

Enterprise Architecture actually defines the process that companies use to standardize and streamline IT infrastructure to align with business objectives. For every business, it is imperative that it should have a blue print that we can grow into some kind of architecture of a business. Enterprise Architecture is closely linked with Enterprise Architecture Frameworks, as these will help and guidance needed to maintain the businesses and IT alignments in companies. The Open Group Architecture Framework (**TOGAF**) provides universal guidance to ADM with a complete collection of artifacts and is the most popular. The NATO Architecture Framework, **NAF** is a defense industry framework, which provides rules and guidance for designing common architecture platform for amalgamating architectures in NATO. **UML** is an EA framework using Unified Modeling Language which is a descriptive visual language with scalable diagraming capabilities. UML Profile extension capability to customize and expand different business domains is very useful. The use stereotypes, tagged values and constraints by enterprise architects, make UML language fit into different environments. **SABSA** is an EA framework providing technical know-how and solutions for business objective in a risk free and opportunity focused manner. It is heavily used in Information Assurance Architectures, Risk Management Frameworks as it provided security architecture foundation for IT architecture methods. As per the Federal Enterprise Architecture Framework (**FEAF**), any architecture can be separated into 4 layers like business, data, applications, and technology architectures.

Business architecture is actually defined by terms “what, by whom, how, when and why”. Data Architecture is defined as information used by the agent to conduct its business. Application architecture is considered as computer applications and software process the data as per business rules. Technology Architecture is defined as computer, communications technology and hardware that supports the above mentioned 3 layers “business, data, applications” This is mainly used in Federal Government work.

The **advantages of applying EA** framework are planning transition effectively during the lifecycle, having the ability to build multi-national supporting systems with high flexibility, adaptability and productivity, adjusting to business changes, trends in industry and regulatory compliance, having the ability to set the priority to business and technology at the level, having the Capacity to plan, manage and invest with controlled expenses but improved communication with technical domains.

References

Concept of governess videos

GRC100-M1-1-Slides-Governance.pdf

GRC100-M1-2-Slides-Standards and Best Practices.pdf

GRC100-M1-1-Videos 3-Information Security Drivers (5 videos, Total time; 13:1)

Websites

https://www.digital-adoption.com/cmmi/

https://www.oceg.org/

https://dataprivacymanager.net/what-are-the-7-gdpr-principles/

https://gdpr-info.eu/art-37-gdpr/

https://www.itgovernance.co.uk/blog/what-are-the-data-subject-rights-under-the-gdpr

https://security.tcnj.edu/program/security-responsibilities/third-party-system-administrator-guidelines/

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/

https://www.cio.com/article/222421/what-is-enterprise-architecture-a-framework-for-transformation.html

https://sabsa.org/sabsa-executive-summary/https://www.academia.edu/50285397/A_Comparison_of_the_Top_Four_Enterprise_Architecture_Frameworks

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/EnterpriseArchitecture/FEAF

https://www.academia.edu/50285397/A_Comparison_of_the_Top_Four_Enterprise_Architecture_Frameworks

https://www.visual-paradigm.com/guide/enterprise-architecture/what-is-nato-architecture-framework/