Governance, Risk Management and Compliance (GRC)

Taylor J. O’Leary

SecureSet Academy

**Table of Contents**

Class 1 - Concepts of Governance…….………………………………………………...4-6

Class 2 – Capability Maturity Model Integration (CMMI)……………………………...7-8

Class 3 – OCEG Membership Account Activity………………………………………..9-12

Class 4 – GDPR SIA Partners………………………………………………………......13-14

Class 5 – Enterprise Architecture……………………………………………………….15-16

Class 6 – Final Project…………………………………………………………………..

References………………………………………………………………………………

Abstract

Governance, Risk Management and Compliance is a framework to improve the culture as well as the function of a company. Governance can be defined as the company’s leadership effectively consolidating efforts, information and making decisions. Risk Management is a way to understand some of the possible risks, determine which risks to the company they are or are not willing to accept. The Compliance portion of Governance, Risk Management and Compliance (GRC) involves the entire company. The employees must work together with the leadership to ensure they are following the guidance set forth by the executives. GRC can only be effective if it is part of the company’s culture.

Class 1 – Concepts of Governance

Governance can be defined as the act or process of overseeing the control and direction of something”(such as a country or an organization) (Merriam-Webster). The Governance of a company is no different. Each company has a leader or multiple leaders that act as executives of the company. These executives are responsible for everything the company accomplishes or fails to accomplish. The leaders of the company make many decisions about the way the company operates: plans, policies, procedures, public relations, product development, product or service quality and pricing, employee development, benefits for employees, marketing and even what the colors the brand’s logo. All of the above is ultimately the responsibility of the company’s leadership.

For the executives to make these decisions they must have accurate, timely information. They must also follow applicable laws and industry standards. To accomplish these legal and industrial standards, there must be an internal compliance program to ensure the employees and the executives are functioning on a mutual understanding. It is far too easy for miscommunication or lack of communication to occur. Effective leaders must bridge the gaps of understanding between the executives and the employees to accomplish their goals for the company, stakeholders, and their employees.

There are multiple forms of businesses that operate in the United States. Typically, there are four main types of businesses: Sole Proprietorships, Partnerships, Limited Liability Companies (LLC), and Corporations (CorporateFinanceInstitute.com). Different businesses each can have their own cultures. A company cannot have effective governance without an understanding of the company’s culture.

Since different business types have different sizes, products, tasks, aspirations, and cultures they each need their own governance strategy. While a sole proprietorship can create and then enforce policies immediately, it may take considerably longer for a much larger corporation to do the same. Every business type needs a set of governing legal documents. For a corporation, these include a certificate of incorporation, bylaws and often a shareholders’ agreement (Capobiancolaw.com). These documents relay the company’s governance strategy by putting on paper the bylaws and shareholder’s agreement. In this way, each different business has its own formalized governance strategy.

Information security and data protection has become a large topic recently. Indeed, Forbes magazine says “Consumers are more aware than ever of the [impact of data privacy](https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#50b987d51bc1) on their personal lives.” And businesses that will not or cannot effectively protect their intellectual property and their customer’s data will face repercussions in the form of profit losses and lawsuits. An effective data protection policy (International Association of Privacy Professionals) will help govern the roles of employees and executives of a company. This will help ensure steps are taken to protect data. If the data protection plan is taken seriously by all of the company’s employees, and if more importantly it becomes a part of the company’s culture-then the data (or any policy) will be much more secure than if it was just written down for inspections by regulators.

In summary, governance is the way executives lead their organization. To effectively lead their company, they must follow the organizational founding papers, laws, industry standards and perhaps just as importantly, they must create a culture of doing the right thing for all members of the company and their consumers. The employees must faithfully follow the lawful governance to reduce gaps in understanding and policy enforcement. And in today’s day and age, that certainly includes the defense of the company’s intellectual property as well as the consumer’s data from any ill willed adversary.

Class 2 CMMI

Capability Maturity Model Integration (CMMI) is a five-step model of an organization’s ability to process. There are five levels to CMMI. The first level is known as “Initial” at this step processes are unpredictable, and the organization is reactive. Level two is known as “Managed” here there is some project management achieved. Level three is “Defined” organizations are more proactive than reactive. Level four is “Quantitatively Managed” processes are controlled using statistical data. Level five is “Optimizing” organizations are stable and flexible. (cio.com)

An organization may consider CMMI if the company is experiencing a lack of customer satisfaction or is too reactive. Some other reasons to consider the CMMI process is to become more efficient, to reduce risks and to increase company profits.

A business unit manager may align their business processes to CMMI by requesting an appraisal by a CMMI partner that will evaluate three separate areas: process and service department, service establishment and management, and product and service acquisitions. (cio.com)

Advantages for the Sole Proprietor would be to start a streamlined business to scale quicker, disadvantages for the Sole Proprietor can include the time and resources incurred with the appraisal and subsequent interactions with CMMI. CMMI also may not be suitable for this level of an organization. (cmmiconsultantblog.com)

Some advantages for the Partnership type of business would include improving the current day to day activities. It would also enforce having formal, written down processes and help to improve the business. Disadvantages for the Partnership may include appraisal costs and timeline. There would also be a need to use other manpower resources for interactions with CMMI Institute or their partners.

A corporation may be large enough to take serious advantage of the CMMI process. The advantages for the Corporation type of business would be remarkably similar to the other classes of business. The disadvantages for the Corporation, however, would be absorbed easier perhaps due to the higher level of available resources a large corporation my have available. One of the toughest setbacks for a larger company may be the changing of behavior, the culture of a larger company may be more established and less likely to change their daily operations.

In summary, CMMI may be useful to help companies realize where they are currently at process wise and where they need to go to improve their profitability. The five steps in CMMI are logical and can bring value to any business, even without spending the money to buy an appraisal one can learn from the five-step model.

Class 3 OCEG

The Open Compliance & Ethics Group (OCEG) is a nonprofit think tank aimed at increasing awareness of “Principled Performance” and GRC. The OCEG website has many resources including publications standards. Some of the resources available include: OCEG’s “GRC Capability Model”, an illustrated “Pathway to Principled Performance”, a research paper covering OCEG’s 2019 Technology Strategy Survey”, another illustration about OCEG, and many other resources located at the website’s “resources” page.

OCEG’s website also has a “Standards” button at the top of the page. Some of the standards available are: GRC Capability Model (Red Book), GRC Assessment Tools, GRC Capability Model, OCEG GRC Capability Model Practices, GRC-XML Spec and Schema, and GRC Technology Solutions Guide.

One of the available publications in the standards section is the GRC Capability Model version 3.0 also known as the “Red Book” covers a vast amount of information. Some of the information covered in “Red Book” includes: Introduction to Principled Performance and GRC, Anatomy of the GRC Capability Model, and GRC Capability Model Version 3.0.

GRC Capability Model Version 3.0 has four components, they are: Learn, Align, Perform, and Review. The learn portion of the model covers context, culture, and stakeholders. The Align portion of the model covers: direction, objectives, identification, assessment, and design. The third portion of the model is called “perform” there are eight pieces to perform. They are controls, policies, communication, education, incentives, notification, inquiry, and response. The last of the four parts of the model is “Review”, three portions of review are monitoring assurance and improvement.

Back to the website’s menu you will find the “Events” page. The self-descriptive “Events” page shows future virtual, in person, and hybrid events. The next event as of this writing is titled “Achieving LeanGRC” on September 17th, 2020. The event will provide value to individuals interested in applying “Lean principles to GRC capabilities for greater growth and profitability.”

There is also an “Education” page available. The Education page has multiple resources including GRC Fundamentals, GRC Audit, GRC Tech Talks, and information about OCEG certifications. Under GRC Fundamentals, there is a “Principled Performance” page. The Pillars of Principled Performance are Principled Performance, Principled People, and Principled Pathway. According to the Pillars of Principled Performance Page, “A principled purpose is perhaps the most basic starting point for principled performance.”, “Leadership, the workforce and extended enterprise must comprise principled people who have strong character”, and “Break down silos and leverage common capabilities in every key system that keeps an organization on track including governance”.(OCEG)

According to OCEG, there 10 Universal Outcomes of Principled Performance, they are listed as “Achieve Business Objectives - Ensure that all parts of the organization work together toward the achievement of enterprise objectives. Ensure Risk Aware Setting of Objectives and Strategic Planning - Provide timely, reliable, and useful information about risks, rewards, and responsibilities to the governing authorities, strategic planners, and business managers responsible for execution at all levels. Enhance Organizational Culture - Inspire and promote a culture of performance, accountability, integrity, trust, and communication. Increase Stakeholder Confidence - Grow stakeholder trust in the organization. Prepare and Protect the Organization - Prepare the organization to address risks and requirements while protecting the organization from adversity and surprise and enabling it to grasp opportunities. Prevent, Detect, and Reduce Adversity and Weaknesses - Establish actions and controls to prevent negative outcomes, reduce impact, detect potential problems, and address issues as they arise. Motivate and Inspire Desired Conduct - Provide incentives and rewards for desirable conduct, especially in the face of challenging circumstances. Stay Ahead of the Game - Learn information necessary to support quick changes in strategic and tactical direction while avoiding obstacles and pitfalls. Improve Responsiveness and Efficiency - Establish capabilities that make the organization more responsive and efficient so that it has a competitive advantage. Optimize Economic Return and Values - Allocate human and financial resources in a way that maximizes the economic return generated for the organization while maximizing its values.” (OCEG)

Under the “Certifications” tab there are two GRC certifications available, “GRC Professional Certification” and “GRC Audit Certification”. The GRC Professional Certification is intended for the IT Professional. This certification covers “the core understanding of GRC processes and capabilities, and the skills to integrate governance, performance management, risk management, internal control, and compliance activities.” (OCEG)

The “Blog” page provides access to at least 69 free articles. I read the article titled “Well, I Should Hope So / Hope Not Test for Core Values” by OCEG blogs. The article briefly described a way to create a core value quickly and effectively for your organization. The author recommends ensuring the core value statements have distinct, value, and nuance. Also, the author explained a simple “’Well, I should hope so / hope not’ test”. After you read the core value out loud, you should be able to easily say “Well, I should hope so / hope not” while referencing the core value you just read. I believe this article and OCEG goth are a valuable resource because of the sheer amount of accurate, simplified information regarding GRC. This new resource can greatly improve your knowledge of GRC for free in many cases.

Class 4 GDPR SIA Partners

The General Data Protection Regulation (GDPR) is a European law that went into effect in 2018. (gdpr-info.eu) Sia Partners is a global consulting firm that focuses on strategy, business transformation, internet technology, digital strategy, and data science. (sia-partners.com)

GDPR built on existing data protection principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, and storage limitation integrity and confidentiality.

About the new GDRP, hgpresearch.com says “The rule requires an explicit "opt-in" from every website visitor and covers *all* EU residents and citizens.” Whereas in the United States our data protection is much more focused on Personally Identifiable Information (PII) as it relates to health care, finances, and marketing. “At its core, the GDPR rests on a relatively simple premise - that each person has the fundamental right to privacy and to control what happens to information about them” (hgpresearch.com)

Under GDPR there are 99 Articles. A few of those articles and a description of each are below. A Data Controller and Processor must be aware of the way the information is to be processed as well as the protection of the data using certain measures. SAP says, “Data Custodian can help customers square the GDPR, data localization, and public cloud circle, balancing the requirements of data protection legal compliance with effective use of the public cloud.” (SAP). There is also a “Data Subject” which is, according to EU GDPR Compliant, “A data subject is any person whose personal data is being collected, held or processed. As you will see a bit later, personal data can refer to anything from your name, home address or your posts on social media.” And finally, there is the Data Protection Officer. The Data Protection Officer according to Investopedia “is a position within a corporation that acts as an independent advocate for the proper care and use of customer’s information. The role of a data protection officer was formally laid out by the European Union as part of its General Data Protection Regulation (GDPR). Under the regulation, all businesses that market goods or services to customers within the European Union and collect data as a result must appoint a data protection officer.”

In summary, GDPR is a new and exceptionally large European regulation that effects all businesses on the continent and their collection of data of citizens of European nations. The GDPR only allows collection of data if the individual “opts-in” and there are quite hefty fines if the business does not follow the guidelines put forth in the GDPR.

Enterprise Architecture

Enterprise Architecture (EA) is defined by The Enterprise Architecture Center of Excellence (EACOE) as “explicitly describing an organization through a set of independent, non-redundant artifacts, defining how these artifacts interrelate with each other, and developing a set of prioritized, aligned initiatives and road maps to understand the organization, communicate this understanding to stakeholders, and move the organization forward to its desired state.” (EACOE)

A proper Enterprise Architecture can help an organization align its strategy to business processes by setting the businesses priority processes. This leads to more progress and accountability. As CIO.com reports “EA is especially useful for large businesses going through digital transformation, because it focuses on bringing legacy processes and applications together to form a more seamless environment” (CIO)

The Open Group Architecture Framework (TOGAF) is base on three pillars. The first pillar of TOGAF is Enterprise Architecture Domains. The second pillar is Architecture Development Model (ADM). The third pillar is Enterprise Continuum.

The NATO Architecture Framework (NAF) aims “to provide a standard for developing and describing architectures for both military and business use. It provides a standardized way to develop architecture artefacts, by defining Methodology (how to develop architectures and run an architecture project), Viewpoints (conventions for the construction, interpretation and use of architecture views for communicating the enterprise architecture to different stakeholders), Meta-Model (the application of commercial meta-models identified as compliant with NATO policy), and a Glossary, References and Bibliography.”(NATO)

The Unified Modeling Language (UML) is used in software engineering. SBSA stands for Sherwood Applied Business Security Architecture. FEAF stands for Federal Enterprise Architecture. DoDAF stands for Department of Defense Architecture Framework.

If I were to pick one of the previously listed Enterprise Architectures, I would pick the NATO Architecture Framework. The NAF provides many benefits, most notably to me is the Viewpoints feature. With this feature conventions for the construction, interpretation and use of architecture views for communicating the enterprise architecture to different stakeholders is made easy. (NATO)

References

Johnson, K. (2018, 14 September). *The Impact of Data Privacy On Your Business*. Retrieved from Forbes: <https://www.forbes.com/sites/forbestechcouncil/2018/09/14/the-impact-of-data-privacy-on-your-business/#35616f3a196c>

“Governance.” (Accessed 2020, 13 Augaust) *Merriam-Webster.com Dictionary*. Retrieved from: Merriam- Webster, <https://www.merriam-webster.com/dictionary/governance>**.**

International Assosciation of Privacy Professoinals (2020) *Data Protection Policy*. Retrieved from: International Association of Privacy Professionals <https://iapp.org/resources/article/sample-data-protection-policy-template-2/>

Capobianco Law (2020) *The Importance of Corporate Governance Documents.* Retreived from Capobianco Law: <https://capobiancolaw.com/corporate-documents/>

Corporate Finance Institute (2020) *What are the types of businesses?* Retrieved from Corporate Finance Institute:<https://corporatefinanceinstitute.com/resources/knowledge/strategy/types-of-businesses/>

*White, S. (2018, 16 March) What is CMMI? A model for optimizing development processes.* Retrieved from CIO.com:

<https://www.cio.com/article/2437864/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html>

Khare, D. (2013, June 5) ***Advantages and Disadvantages of CMMI-DEV for a Software Development IT Organization?*** Retrieved from:CMMI Consultant Blog <https://www.cmmiconsultantblog.com/cmmi-faqs/advantages-and-disadvantages-of-cmmi-dev-for-a-software-development-it-organization-and-how-to-overcome-these-disadvantages/>

OCEG

<https://www.oceg.org/>

OCEG (2020)***Well I Should Hope So/ Hope Not*** Retrieved from: OCEG Blogs

<https://go.oceg.org/well-i-should-hope-so-hope-not-test#action>

GDPR (2020***) General Data Protection Regulation (GDPR)*** Retrieved from: GDPR-info

<https://gdpr-info.eu/>

Sia Partners (2020) ***Who We Are*** Retrieved from: Sia Partners

<https://www.sia-partners.com/en>

Iffergan, E. (2018, February 12) ***WHO OWNS PERSONAL DATA? GDPR VS USA*** Retrieved from: Hyperion GP Research

<https://insights.hgpresearch.com/who-owns-personal-data-gdpr-vs-usa>

SAP Community (2020) ***GRC Tuesdays: GDPR vs. Data Localization vs. Public Cloud*** Retrieved from: SAP Community

<https://blogs.sap.com/2018/09/11/grc-tuesdays-gdpr-vs-data-localisation-vs-public-cloud/#:~:text=By%20delivering%20improved%20data%20transparency%20and%20control%20of,compliance%20with%20effective%20use%20of%20the%20public%20cloud.>

EU GDPR Compliant (2020) ***WHAT IS A DATA SUBJECT?*** Retrieved from: EU GDPR Compliant <https://eugdprcompliant.com/what-is-data-subject/>

Kagan, J. (2018, January 3) ***Data Protection Officer – DPO*** Retrieved from: Investopedia

<https://www.investopedia.com/terms/d/data-protection-officer-dpo.asp>

EACOE (2020) ***What Is Enterprise Architecture?*** Retrieved from: EACOE

<https://www.eacoe.org/ea-definition?msclkid=5b98d1a68c77181de20f8ee04c8d3460&utm_source=bing&utm_medium=cpc&utm_campaign=EACOE%20High%20Intent&utm_term=enterprise%20architecture%20definition&utm_content=Training%20and%20Certification>

White, S. (2018, October 16) ***What is enterprise architecture? A framework for transformation*** Retrieved from: CIO.com

<https://www.cio.com/article/3313657/what-is-enterprise-architecture-a-framework-for-transformation.html#:~:text=Enterprise%20architecture%20is%20the%20process%20by%20which%20organizations,These%20strategies%20support%20digital%20transformation%2C%20IT%20growth%20>

NATO (2019, December 3) ***NATO Architecture Framework, Version 4*** Retrieved from: NATO

<https://www.nato.int/cps/en/natohq/topics_157575.htm>

Footnotes

Figures