Governance, Risk Management and Compliance

H. Morgan Jordan

Flatiron School

GRC 100

November 15th, 2021

Table of Contents

[Abstract 3](#_Toc87966199)

[Concepts of Governance 4](#_Toc87966200)

[Capability Maturity Model Integration (CMMI) 5](#_Toc87966201)

[OCEG Membership Account Activity 6](#_Toc87966202)

[GDPR SIA Partners 7](#_Toc87966203)

[Enterprise Architecture 9](#_Toc87966204)

[References 12](#_Toc87966205)

# Abstract

Governance, risk and compliance is a key component of any successful enterprise. From management style to ownership type and the industry that your enterprise is in, there are many aspects to consider when developing a model for your organization. By evaluating your enterprise’s maturity level, you can determine how OCEG, GDPR and an enterprise architecture can further help your organization grow.

# Concepts of Governance

Corporate governance refers to the structure that the owner(s) or shareholders would like to determine the internal conduct and long-term vision of the company. The owner(s) or shareholders would then determine who can make decisions regarding compliance and who is held liable for those decisions at the end of the day. The implementation of policies and procedures ensures that the company is compliant with current regulatory requirements depending on their industry. For example, some forms that would be used to implement such requirements from the GDPR would be privacy notices, personal data protection policy, or a data retention policy.

Governance within a company refers to the overall management of the company’s day-to-day functions. These functions are largely determined by the industry that the company is in because that will delineate which specific laws and regulations the company needs to comply with. Compliance to these laws and regulations are typically managed by a non-executive or department that can place their main focus on those specialty items and maintain the company’s compliance programs.

The type of ownership will greatly determine how a governance strategy is created and managed. The most common types of company ownership are proprietorships, partnerships, and corporations. With proprietorships, governance is at its simplest form since there is only one person making the major decisions for the company. Partnerships take governance to another level seeing as you are having to accommodate two or more partners and their desires. Corporations will tie their governance into the articles of incorporation making the shareholders largely responsible for handling GRC.

# Capability Maturity Model Integration (CMMI)

The Capability Maturity Model Integration (CMMI) is a method that assists organizations with streamlining and improving productivity while also minimizing risk. CMMI is delineated into five different levels of maturity. The maturity of a company determines its functionality as a whole and whether it is more reactive or proactive.

The first level of maturity is referred to as ‘Initial’. In this stage the company is more in a reactive state and constantly fixing issues. Level two is ‘Managed’. This means that while there are still some problems to fix, it is a little more organized. Maturity at the third level is ‘Defined’, so this is when you would see a company start becoming more proactive. They would have standards in place and while there may still be concerns, they know how to handle them and move forward. Level four is when a company would start implementing quantitative data to improve their business processes. With this ‘Quantitatively Managed’ level of maturity a company is getting more proactive and ahead of risk. The final level five is ‘Optimizing’. This is when a company is consistently enhancing themselves and can be more inventive in a comfortable environment.

Organizations would want to use the CMMI if they are looking to further their company and reach certain business goals. The more organized and prepared that you are allows you to progress within your industry and create a business built on a solid foundation. In order to integrate CMMI within your organization you would need to implement company-wide policies to have the best practices secured and embraced, put the correct staff in their appropriate positions and ensure critical information isn’t shared. The benefits of adopting this model would improve a business’ consistency, performance, and self-improvement but there could also be some disadvantages. This model could present an unnecessary amount of overhead regarding time and paperwork if the company considering this model is too small.

# OCEG Membership Account Activity

Open Compliance and Ethics Group (OCEG) originally started up in 2002 with a goal of improving corporate compliance and ethics but eventually evolved to include management of risk and performance, governance and assurance. OCEG saw the issues with having a “siloed” approach to governance, risk and compliance (GRC), and created a more contemporary idea for Principled Performance and GRC.

Through their website you have access to multiple resources to assist you and your company with all your GRC needs. Not only do they have the GRC Capability Model (also known as the OCEG Red Book) in various languages, but they have GRC Assessment tools, a Policy Management Capability Model, GRC Spec and Schema, and GRC Technology Solutions. They have many other resources as well in the form of illustrations, eBooks, playbooks, blogs, research, and webinars. Webinar events occur on a regular basis regarding Policy Management and how to integrate it to prepare for unexpected occurrences which is useful no matter what field your organization is in. There are education resources available regarding GRC fundamentals, audits and tech talks. Certifications can also be attained through their website for an IT specialist to become a GRC Professional or be able to perform GRC Audits.

The Red Book assists GRC professionals in planning, evaluating, and enhancing their GRC capabilities so that they may attain Principled Performance. The four main elements of the GRC Capability Model are learn, align, perform and review. First you need to *learn* about the key components of an organization so that you may outline their objectives, strategies and actions. In order to *align* those objectives, strategies and actions you must make effective decisions to achieve those goals. You need to *perform* actions that benefit your organization while also detecting and preventing any unwelcome events. Finally, in order to improve your organization, you need to consistently *review* your model and effectiveness of your strategies and actions while also maintaining adequate objectives.

Principled Performance consists of three pillars. Pillar one is Principled Purpose which consists of your organizations overall mission and values. Next is Principled People, and that means you need to have the appropriate people in place to achieve that Principled Purpose. Lastly is Principled Pathway. With this pillar you need to break down the barriers preventing you from achieving your company mission and use common abilities from each management system to stay on track. Following these pillars will help your organization accomplish 10 universal outcomes. These outcomes consist of attaining business objectives, being aware of risks and how to strategically plan for their occurrence, boost your organization’s culture, gain more confidence from your stakeholders, ready and defend your organization from risk, prevent negative outcomes from risk, promote preferred behavior, evolve while maintaining a competitive advantage efficiently, and improve economic return.

# GDPR SIA Partners

The General Data Protection Regulation (GDPR) is the world’s most substantial set of data protection rules. After approximately 4 years of deliberations, GDPR took full effect in the European Union (EU) on May 28th, 2018. The GDPR protects any personal data that makes you identifiable by any means. This could be but is not limited to your name, username, religious views, political opinions or location information.

When speaking about GDPR there are a few terms that should be understood. A data subject is the person whose data is being processed. The data controller is someone that decides why and how such personal data will be processed. Data processors is a third party that processes data for a data controller. There are also data custodians who handle the transportation and storage of personal data. Lastly, Data Protection Officers (DPOs) are required by the GDPR for any organization that handles personal information from the EU. DPOs are responsible for staying up to date with GDPR and how it applies to your organization as well advising and training individuals within the company, auditing, acting as a liaison with regulators and monitoring the organization’s compliance.

There are seven data protection principles that the GDPR enforces. The first principle is that all processing of a data subject’s information must be lawful, fair and transparent. There are also purpose limitations, which means that the data must processed for legitimate purposes that have been specified to the data subject at the time of collection. You must gather and process only as much information as necessary for those purposes as well. It is imperative that all personal data be kept accurate and up to date. You may only store the personal data of the data subject for as long as necessary to perform the specific purpose for which it was collected. Security, integrity and confidentiality must be ensured during the processing of personal data. Lastly, the data controller is responsible for establishing, maintaining, and keeping record of GDPR compliance with all principles.

The approach to data protection differs greatly between the United States (US) and the EU. While the EU came up with the GDPR as a main directive for everyone in the EU to follow, the US has category specific data protection that works in cohesion with state laws to ensure data protection for Americans. These ‘categories’ consist of the Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST), the Gramm-Leach-Bliley Act (GLBA), and Federal Information Security Management Act (FISMA). While states like California have a security breach notification law, not all states have something similar in effect which creates issues within this separated approach since not all US citizens have equal data protection. There are some government bodies that help to mitigate this such as the Federal Trade Commission (FTC) or the Federal Communication Committee (FCC) but this creates a lot of ‘hands in the pot’ instead of the more cohesive GDPR approach.

# Enterprise Architecture

The means by which an organization regulates and normalizes its IT framework to align with its business goals is commonly referred to as enterprise architecture (EA). EA requires analysis, outlining, planning and application of enterprise analysis in order to successfully implement business strategies. This will help a business construct IT projects and policies so that they may achieve their desired results and stay ahead of their industry’s trends or disruptions. EA as a structure can be vague since it encompasses an organization, so several methodologies exist to assist businesses.

The Open Group Architectural Framework (TOGAF) states that it has been embraced by more than 80% of the world’s leading enterprises. TOGAF supplies principles for creating, planning, applying and governing enterprise IT architecture. This framework assists organizations in creating a standardized method to EA with common terminology, suggested standards, compliance techniques, and recommended tools and software.

Federal Enterprise Architecture Framework (FEAF) introduced mandates regarding IT efficiency to ensure a high degree of integration between federal agencies. FEAF provides a specialized approach for EA practice as well as a complete classification for it. While designed for the US Government, it can also be practiced by private companies.

The NATO Architecture Framework (NAF) supplies rules, advice, and templates to establish a common denominator for comprehending, analyzing, and incorporating architectures in NATO. Applying NAF is supposed to give architectures the ability to contribute most effectively to procuring and handling cost-effective and interoperable military capabilities. NAF has a Version 4 available whose goal is to supply a norm for creating and detailing architectures for both military and business use.

The Unified Modeling Language (UML) characterizes rules and notations for distinguishing business and software systems. It isn’t a tool for creating software systems, but rather a visual language for corresponding, designing, indicating, and defining systems. There is also no method or process, UML is simply a language and is therefore flexible and useable in many ways. The UML system is generic yet comprehensive enough to serve as the building blocks for all system design necessities.

The Sherwood Applied Business Security Architecture (SABSA) focuses on both enterprise and solution levels to help develop business-driven, risk and opportunity centered Security Architectures. This seamlessly aligns and meshes security and risk management into an IT Architecture’s method and structure. SABSA ensures that the demands of your enterprise are met fully and that security services are constructed, delivered and supported as an elemental part of your business and IT management framework.

Based off the research that I have done regarding EA; I would have to choose SABSA. Since 1995, they have developed and sustained the design and certify and accredit the qualified Architects who use it in roughly 50 countries around the globe and became the ‘approach of choice’. This method is used in many diverse professions such as Banking, Nuclear Power, Information Services, Manufacturing, and Government.

# References

Aiim. (2021). *Governance vs compliance.* Retrieved from: <https://community.aiim.org/blogs/brandon-burke/2019/04/03/governance-vs-compliance>

Burgess, Matt. (2020, March 24th). *What is GDPR? The summary guide to GDPR compliance in the UK.* Retrieved from: <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>

The Chartered Governance Institute. (2021). *What is corporate governance?* Retrieved from: <https://www.cgi.org.uk/about-us/policy/what-is-corporate-governance#:~:text=Corporate%20governance%20is%20the%20system,accountability%2C%20and%20who%20makes%20decisions>

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

Coos, Andrada. (2018, January 17th). *EU vs US: What are the differences between their data privacy laws?* Retrieved from: <https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/>

EA Principals. *What is FEAF?* Retrieved from: <https://www.eaprincipals.com/content/what-feaf>

Geoviz, Inc. (2013, July 12th). *Top 6 benefits of adopting capability maturity model – CMMI – focus software companies.* Retrieved from: <https://geo-viz.com/blog/top-6-benefits-of-adopting-capability-maturity-model-cmmi-focus-software-companies/>

Lord, Nate. (2020, October 6th). *What is a data protection officer (DPO)? Learn about the new role required for GDPR compliance in 2019.* Retrieved from: <https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance>

OCEG. (2002-2021). *Ultimate resource for governance, risk and compliance (GRC).* Retrieved from: <https://www.oceg.org/>

The SABSA Institute C.I.C. (2020). *SABSA Executive Summary.* Retrieved from: <https://sabsa.org/sabsa-executive-summary/>

SecureSet Academy, Inc. (2018). *SecureSet cybersecurity analyst: GRC 100* [Powerpoint slides]*.* Retrieved from: <https://learning.flatironschool.com/courses/4771/pages/grc100-m1-2-grc-definitions-and-drivers-3-videos-total-time-7-10?module_item_id=300746>

SecureSet Academy, Inc. (2018). *SecureSet cybersecurity analyst: GRC 100* [Powerpoint slides]*.* Retrieved from: <https://learning.flatironschool.com/courses/4771/pages/grc100-m1-4-regulations-standards-and-best-practices-2-videos-total-time-8-04?module_item_id=300748>

Sparx Systems Pty Ltd. (2000-2021). *Unified modeling language (UML).* Retrieved from: <https://sparxsystems.com/enterprise_architect_user_guide/15.2/model_domains/whatisuml.html>

Techopedia Inc. (2021). *Data custodian.* Retrieved from: <https://www.techopedia.com/definition/1004/data-custodian>

Visual Paradigm. (2021). *What is NATO architecture framework (NAF).* Retrieved from: <https://www.visual-paradigm.com/guide/enterprise-architecture/what-is-nato-architecture-framework/>

White, Sarah K. (2018, October 16). *What is enterprise architecture? A framework for transformation.* Retrieved from: <https://www.cio.com/article/3313657/what-is-enterprise-architecture-a-framework-for-transformation.html>

White, S.K. (2021, June 1st). *What is CMMI? A model for optimizing development processes.* Retrieved from: <https://www.cio.com/article/2437864/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html>

Wolford, Ben. (2020). *What is GDPR, the EU’s new data protection law?* Retrieved from: <https://gdpr.eu/what-is-gdpr/>

Woollven, C. (2021, June 10th). *List of mandatory documents required by the GDPR.* Retrieved from: <https://www.itgovernance.co.uk/blog/the-documents-you-need-to-comply-with-the-gdpr>