# GRC 100 Project - Phase 1

By

David Pierre

01/09/2023

Submitted to: Eric Keith

TABLE OF CONTENTS

[**Organizational Abstract 3**](#_heading=h.z1k98w2gothw)

[**M1-1 – Organizational Defined Governance 4**](#_heading=h.gjdgxs)

[**M1-2 – GRC and Organizational Objectives Alignment 5**](#_heading=h.1fob9te)

[**M2-1 – Organizational Regulatory Privacy Policy 6**](#_heading=h.3znysh7)

[**M2-2 – Corporate Governance 7**](#_heading=h.2et92p0)

[**M3-1 – Business Continuity Planning 8**](#_heading=h.tyjcwt)

[**M3-2 – Roles and Responsibilities 9**](#_heading=h.3dy6vkm)

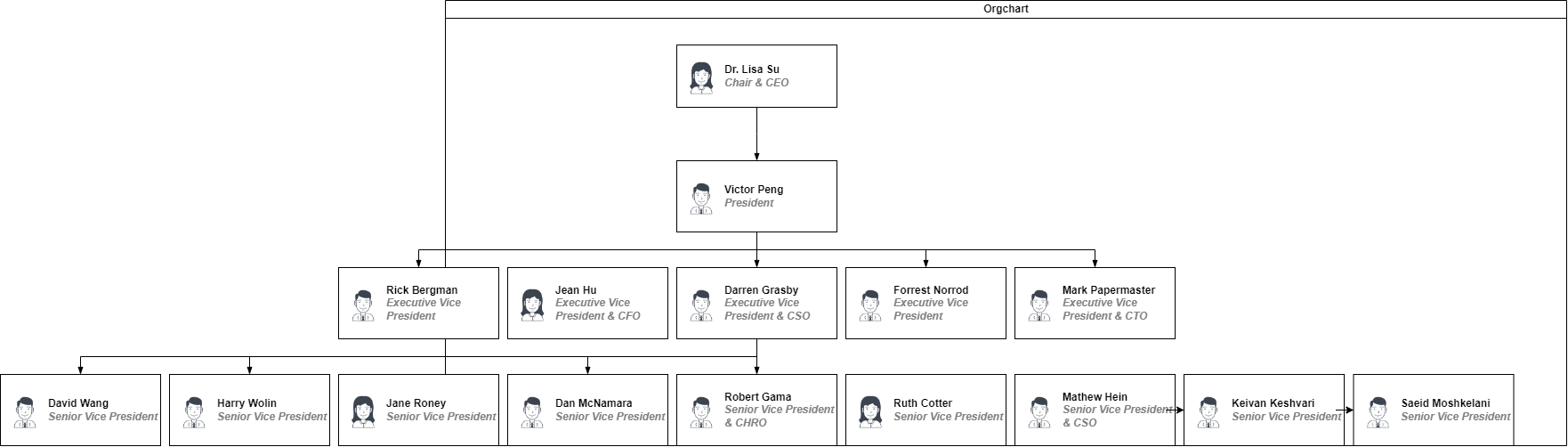
[**References 10**](#_heading=h.4d34og8)

## Organizational Abstract

Technology has become one of the most important creations of mankind. It has to lead to the spread of knowledge, information, and the improvement of the quality of life. Whether it's transporting resources or saving lives, it has made the process much easier. This paper aims to explore how AMD has been a leader in the advancement of technology and innovation. AMD has structured its company in a manner that aligns with its vision, mission, and objectives. The company operates in more than 35 countries across the world including its corporate offices, engineering facilities, and service sites. They are currently operated by their CEO Dr. Lisa Su, president Victor Peng, and several executives and senior vice presidents. The vision of AMD is adaptive, high-performing computing technology. Their mission is to improve the experiences within the entertainment, hyperconnectivity, health care, automotive, aerospace, and data center industries.

## M1-1 – Organizational Defined Governance

AMD would be best suited to operate with proactive governance due to their need to improve the experience of their customers. Companies that operate under this type of governance usually have a specific set of priorities. Some of these priorities may include quality delivery of products or services, strategic alignment, performance management, resource management, and risk management. These priorities are necessary in order of making sure the company is keeping up with and abiding by the set rules and standards of information security and privacy governance. AMD has administered its corporate responsibility to approach it considering environmental, social, and governance issues. Their governance objectives include digital impact, environmental sustainability, supply chain sustainability, and diversity. Proactive governance will allow AMD to improve its performance while taking other people and ideas into consideration.



## M1-2 – GRC and Organizational Objectives Alignment

**Business Driver: Maturity**

AMD strives to lead the world in technological innovation. To continuously maintain that level of success, they must decide what are the main factors that will influence this. Based on their objectives, it would be most suitable if they implemented a level 4 CMMI. The CMMI is used to improve the organization at hand through appraisal and training programs. Plenty of U.S. government contracts require the use of a CMMI to guide the process. AMD has managed the governance of its organization through its Enterprise Information Security team, Business Information Security Officers program, and Audit and Finance committee.

**Organizational Alignment**

AMD has established a code of ethics, a supplier code of conduct, worldwide standards of business conduct, and several policies that describe the governance of its organization. Some of these policies discuss topics such as anti-bribery, anti-corruption, climate change, conflict minerals, environmental health and safety, exports, human rights, and product quality.

AMD understands the importance of having a secure infrastructure, which is why they are constantly updating and testing the system they have in place. Their Business Information Security Officers work with the cybersecurity team to communicate to their clients what strategies and policies would best be suited for the governance. The Audit and Finance committee works together with the Enterprise Information Security team by providing reviews and feedback on information security risks.

**GRC Objectives**

* Global Policy 1102: The protection of confidential information
* Global Policy 1707: Ethics and Compliance in working with U.S. public sector contracts
* Finance Policy 1150: The authorization for employees to sign written agreements on behalf of the company
* Global Policy for Management of Worker & Third Party Personal Data: The protection of personal and third party data

## M2-1 – Organizational Regulatory Privacy Policy

**Governance Drivers: Privacy Compliance**

The privacy drivers that will be influencing how AMD complies with privacy include:

* Core - communication from the executives to the rest of the organization on critical privacy protection practices and desired outcomes
* Profiles - the prioritization of the practices and results
* Implementation Tiers - levels of supporting the organization’s practices and results

There are several issues at the forefront of challenges posed to privacy. Some of these issues include the different approaches based on geographical location, complex contractual agreements, dilapidated laws, and the increased need for awareness based on country-specific requirements. AMD’s teams make sure that they are operating their organization in a way where their practices are not to the detriment of people or society. They are strongly against using any type of method that would violate any environmental factors, ethics, or human rights, a method used by many companies currently. AMD provides public reports on the use of many minerals to create their products.

**Organizational Regulatory Privacy Policy**

Any time of information provided to us from our customers will not be sold nor shared with outside companies or organizations. All information is used to create best practices for our customers and stakeholders.

## M2-2 – Corporate Governance

**Corporate Governance**

The AMD Board of Directors works together with the Board Committee for Nominating and Corporate Governance and management to discuss their environmental, social, and governance practices, issues, and reporting. AMD meets at least once every quarter to update its findings. They make their reportings public to be transparent with their stakeholders.

The control and management of risks regarding cyber and information security are essential in governance. Organizations need to have a team, strategy, and policies in place to be able to mitigate and limit infiltration. Assets are a major component of a company’s value and should be protected by best practices. AMD has a cross-functional team that focuses on product energy efficiency. They meet biweekly to discuss standards and regulatory developments that could pose opportunities or harm short-term or long term.

The Enterprise Architecture is responsible for identifying the organization’s rules, requirements, and case of activities. The organization is analyzed through different scopes to decide what framework would work best. AMD’s Enterprise Information Security team was designed to plan and execute the best framework within cybersecurity. The team is constantly educating and testing their employees on what practices work best to protect their assets.

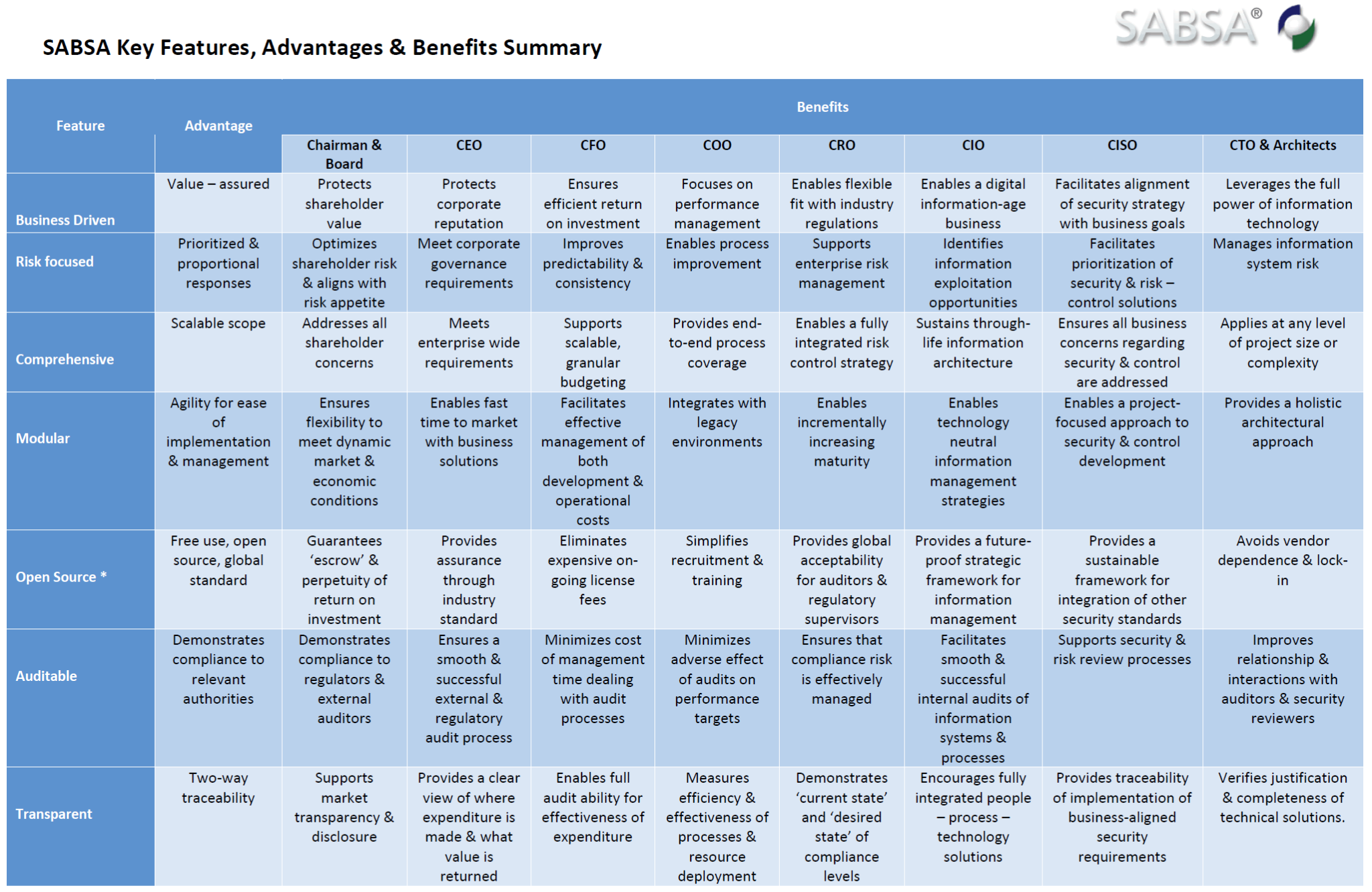
The management of assets should be one of many top priorities in any organization. There should typically be an owner to these assets that manage them by defining their classification, inventory, value, and protection. They would receive and execute the strategy the governance team implemented and be responsible for any compromises. AMD has Business Information Security Officers that work together with the cybersecurity team to implement Cyber Operations, Incident Command and Response, and Insider Threat functions. These functions are monitored 24/7 to ensure the protection of their assets.

Managing changes in an organization are required to ensure that everyone understands what will take place moving forward. AMD’s executive team receives regular updates every month on current requirements and suggestions. Their Executive Steering Committee oversees the progress being made in the organization. The Corporate Responsibility team monitors day-to-day activities, policies, infrastructure, reporting, and communication. These teams work together so that AMD is up to date with all needs and reporting.

Business Continuity planning is necessary when operations of the organization are altered or halted. AMD has incorporated this factor into its risk management by having its Environmental, Health and Safety, Finance, Human Resources, Global Operations, Information Technology, and other teams identify and create plans to prepare for such events.

**Enterprise Architecture Framework**

Given the nature of its organization, AMD would be best suited under the Sherwood Applied Business Security Architecture. This framework is composed of Risk Management, Governance, Information Assurance, and Continuity Management. These areas of focus are already incorporated into AMD’s governance.



## M3-1 – Business Continuity Planning

**NIST SP 800-34**

The purpose of this guide is to identify the processes of a mission or business. These processes will determine how much time can be afforded by the organization to not be in operation in the case of an attack or breach. The relationships between different interdependencies are measured to identify the requirements of the resources involved.

**Three Steps for a Business Impact Analysis**

The Business Impact Analysis serves three different purposes. The first is to provide an understanding of all practices and activities. Second, it identifies the infrastructure and essential processes. Finally, it allows the development of a plan to resume the processes after an event has occurred. There are three steps designated to the creation of the analysis which is listed below:

1. **Mission/Business Processes & Recovery Criticality**

Several steps should be taken to properly secure any organization from outside threats. These are some of the steps AMD believes are the most suitable:

* Adopt a zero-trust security and framework mindset
* Conduct several audits and assessments
* Establish end-to-end encryption
* Maintain and develop tight access controls
* Provide a shared-responsibility model of cloud computing
* Ensure the infrastructure supports the Trusted Boot/Trusted Platform Module (TPM)
* Establish Multi-Factor Authentication (MFA)
* Develop comprehensive end-user programs
* Use machine learning and artificial intelligence algorithms

1. **Resource Requirements**

AMD believes that the future of securing organizations should be done by having data centers in place. The modernization of these centers includes many aspects such as having numerous small facilities, switching to a software-defined infrastructure model, administering infrastructure upgrades, and adopting a cloud-centric or hybrid cloud architecture. These data centers allow for a high level of security. Having a data center with a focus on cybersecurity will better prepare organizations for unforeseen events.

1. **Recovery Priorities**

| Category | High Level | Medium Level | Low Level |
| --- | --- | --- | --- |
| Corporate | Restricted | Confidential | Public |
| Defense | Top Secret | Secret | Confidential |
| Qualitative | High | Moderate | Low |

**Organization Backup and Recovery**

* MTD: Maximum Tolerable Downtime (MTD) is the number of time managers and leaders are willing to allow for the business or organization to be after a disruption or outage has taken place
* RTO: Recovery Time Objective (RTO) is the maximum amount of time a resource of a business or organization can be unavailable before it affects the processes of other processes and resources
* RPO: Recovery Point Objective (RPO) is the point in time to which process data must be recovered after an outage or disruption has occurred

AMD utilizes cloud backups to ensure that its data is protected and stored away in case of any unwarranted events take place. In the event of a disruption, a cloud backup can be used to restore the data in use, preventing processes from being halted. The only way processes or activities would be stopped is if everything is centralized in one location.

Duplicate, redundant facilities would be the best fit for recovery facilities. It allows for multiple locations that can operate at the same time. This would prevent any processes or activities to be halted due to the fact the business or organization is running through numerous locations as opposed to one central facility.

## M3-2 – Roles and Responsibilities

**Organizational Roles**

* Chief Executive Officer (CEO)
* Chief Financial Officer (CFO)
* Chief Security Officer (CSO)
* Chief Technology Officer (CTO)
* Chief Information Officer (CIO)
* Chief Information Security Officer (CISO)

**Responsibilities of each Role**

The CEO is the person in charge or would come second to the business or organization owners. They have to support all information security motives and hold the business accountable for complying with the policies and procedures of the business or organization. They also ensure that funding is provided for these processes and activities.

The CIO is responsible for the governance of IT and the service delivery that supports the processes that drive the organization or business. This includes overseeing customer data and the technology budget.

The CFO is in charge of mitigating the enterprise risk management including information security and financial, reputational, operational, and strategic risks. This involves analyzing strengths/weaknesses in the company's finances and overseeing all aspects of its financial status.

The CSO is in command of the security initiatives and strategies of the business or organization. They develop and implement the best plans suited for optimal security.

The CTO is responsible for the system administrators and provides the direct link between information security policies and the systems, data, and network. They ensure the efficiency of the technology being used in the organization or business.

The CISO develops and administers information security plans that ensure the protection and security of the organization or business. They are the people that determine the best policies and procedures that protect communications, assets, and systems involved.

## References

*About AMD | AMD*. (n.d.). Retrieved February 9, 2023, from https://www.amd.com/en/corporate.html

*Cybersecurity | AMD* (no date) *AMD*. Available at: https://www.amd.com/en/corporate-responsibility/governance-cybersecurity (Accessed: February 9, 2023).

*Governance Documents* (no date) *Advanced Micro Devices, Inc.* Available at: https://ir.amd.com/leadership-governance/governance-documents (Accessed: February 9, 2023).

*Advanced Micro Devices, Inc. (“AMD”)* (no date) *AMD*. Available at: https://www.amd.com/system/files/documents/human-rights-policy.pdf (Accessed: March 12, 2023).

*AMD Supplier code of conduct | AMD* (no date) *AMD*. Available at: https://www.amd.com/en/corporate-responsibility/amd-supplier-code-of-conduct (Accessed: March 12, 2023).

*Cybersecurity | AMD* (no date) *AMD*. Available at: https://www.amd.com/en/corporate-

responsibility/governance-cybersecurity (Accessed: March 11, 2023).

*SABSA Executive Summary - The SABSA Institute* (no date) *SABSA*. Available at: https://sabsa.org/sabsa-executive-summary/ (Accessed: March 11, 2023).

*Providing Proper Cybersecurity and Risk Management for Your Data ... - AMD* (no date) *AMD*. Available at: https://www.amd.com/system/files/documents/amd-cybersecurity-and-risk-management.pdf (Accessed: March 26, 2023).