GRC 100 Project - ConEdison

By

Matthew Robinson

Students Cohort Start Date: 1/9/203

Submitted to: Eric Keith

TABLE OF CONTENTS

Organizational Abstract

ConEdison is one of the largest publicly traded US energy delivery systems found within the Utilities industry. They provide, "renewable energy, sustainability services, cost-effective energy solutions, demand response, and energy performance contracting" ("Consolidated Edison"). They have grown exponentially since their start. As a result, it is critical for an organized GRC plan to be in place.

As a primary business driver in terms of the company's overall structure ConEdison operates as a corporation. Within a corporation shareholders value will drive corporate governance and activities. ConEd has charted, "…$12 billion in annual revenues and $62 billion in assets" ("Consolidated Edison"). Acting as a legal entity separate from the owners it is the responsibility of the Board to make decisions in the best interest of their investors.

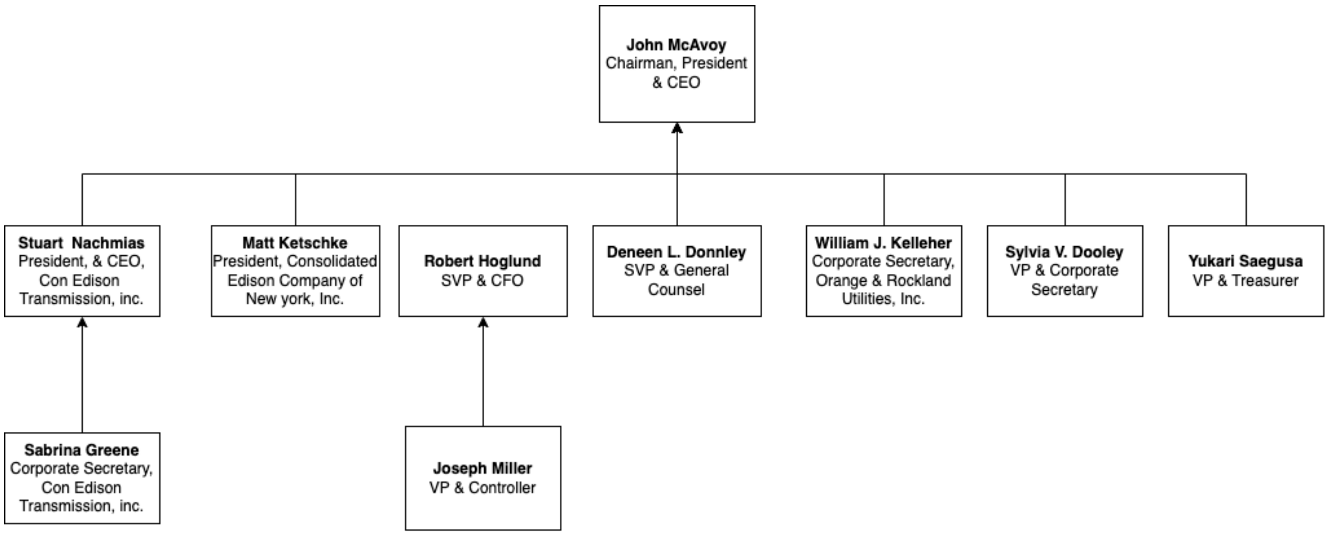
A common business driver across all organizations that affects modern governance is maturity. A company like ConEd becomes mature when it's firmly established, trusted, and continues to hold a high market share in their industries. To optimize the companies maturity the focus must be on processing improvement and enhancing the existing processes. This can be defined within the Corporate Governance Guidelines ("Consolidated Edison"). The best practices ConEd has found for organization and enhancement include:

- Defining the **frequency of meetings** and their **agenda**
- Allowing the Directors **access to management**
- Allowing the Directors **access to auditors**
- An **evaluation** plan for both CEOs and Board Members
- **Confidentiality**
- Management speaks as a **central head with constituencies**

M1-1 – Organizational Defined Governance

ConEdison is a business that relies heavily on its Board Members to structure their Governance, Risk, and Compliance goals. Within this structure is a hierarchy in which tasks are associated and overall decisions are made. Under the Corporate Government Guidelines for ConEdison the board is comprised of 16 members, voted in by the current Board, who's primary goal is to, "…(i) evaluate the performance of the Company and its management; (ii) elect the CEO and other members of senior management; (iii) review the Company's strategic plans, objectives and risks, including with respect to sustainability, environmental, social and governance ("ESG") matters; (iv) provide advice and counsel to the Company's management; (v) exercise oversight of compliance by the Company with applicable laws and regulations, including the Company's public reporting obligations; (vi) evaluate the overall effectiveness of the Board and its committees and (vii) select and recommend for approval by the shareholders a suitable slate of candidates for Board membership" ("Consolidated Edison"). Board Members will elect members to leadership, as well as associate tasks to different members through each of their six standing committees. The current committees as of February 16th, 2023 include:

- Audit
- Corporate Governance and Nominating
- Executive
- Finance
- Management Development and Compensation
- Safety, Environment, Operations and Sustainability [1]


John McAvoy
Chairman, President & CEO
Stuart Nachmias
President, & CEO, Con Edison Transmission, inc.
Matt Ketschke
President, Consolidated Edison Company of New york, Inc.
Robert Hoglund
SVP & CFO
Deneen L. Donnley
SVP & General Counsel
William J. Kelleher
Corporate Secretary, Orange & Rockland Utilities, Inc.
Sylvia V. Dooley
VP & Corporate Secretary
Yukari Saegusa
VP & Treasurer
Sabrina Greene
Corporate Secretary, Con Edison Transmission, inc.
Joseph Miller
VP & Controller

M1-2 – GRC and Organizational Objectives Alignment

The CMMI Model is a model for optimizing development processes. The goal of this process is to help organizations improve by encouraging, "…productive, efficient behaviors that decrease risks in software, product, and service development" (White).The main advantages of using a CMMI Model would be its:

- **Consistency**
- **Cost Saving**
- **Self Improvement**
- **Market Demand** - many competing companies are utilizing CMMI
- **Performance Demand** - consistently and predictably deliver the products their customers want
- **Process Demand** - framework to standardize process ("CMMI-Focus")

In relation to the CMMI Model, ConEd aligns its business processes in a similar fashion. Each member of the board and its committees has a clear defined role, with final decisions and communications held under the responsibility of the CEO. By defining roles in an organized hierarchy the company is able to reach optimal efficiency. ConEd keeps an up to date Corporate Governance Guidelines to accurately define the company's leadership style, philosophy, values, standards, and policies.

While the CMMI model has many benefits it may not be the right fit for all organizations. CMMI may not take in account all requirements some organizations may have. In other instances not every organization is at the same stage of growth. Perhaps the CMMI model may be better suited for larger, more established companies ("Pros and Cons").

Information security governance is important in this scenario to protect the privacy of its shareholders. As an investor owned company it is critical the shareholders are being protected against unauthorized use of information.

In the hierarchy of ConEd's current structure security leaders must work with the Board to develop a security strategy to be successful.

GRC compliance guidelines, standards, and laws that directly influence the industry include Compliance, PCI-DSS, FISMA.

M2-1 – Organizational Regulatory Privacy Policy

Privacy defines the state or condition of freedom from observation of being disturbed by other people. It is important to understand the drivers that influence governance privacy to ensure all information is secure.

Organization for Economic Co-Operation and Development (OECD) privacy principles provide a framework for conEdison's privacy and data protection. This framework consists of eight principles:

- **Collection Limitation Principle**
- **Data Quality Principle**
- **Purpose Specification Principle**
- **Use Limitation Principle**
- **Security Safeguards Principle**
- **Openness Principle**
- **Individual Participation Principle**

Accountability Principle

*****The article, "OECD Privacy Principles" can be utilized for a detailed breakdown of how each principle is acted out.

The cybersecurity program is aligned with the NIST Cybersecurity Framework. This framework is composed of three parts:

- **Implementation Tiers** - communication about resources for privacy risk
- **Core** - enables dialogue between executive level to implementation level
- **Profiles** - prioritizing outcomes that best meet privacy value, mission, risks

The NIST Privacy Framework is a tool intended to help organizations, "… identify and manage privacy risk to build innovative products and services while protecting individuals' privacy" ("Privacy Framework"). Each comppnet reinforces privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities.

Privacy is defined in the Generally Accepted Privacy Principles (GAPP) as the, "…rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information" ("The 10 Generally"). After collecting personal information like a customer's telephone, email, address, social media, etc. is is important to disclose certain rights to the customer. These ten principles include:

- **Management**
- **Notice**
- **Choice and Consent**
- **Implementation Tiers**
- **Use, Retention and Disposal**
- **Access**
- **Disclosure to 3rd Parties**
- **Security for Privacy**
- **Quality**
- **Monitoring and Enforcement**

*****Please refer to, “The 10 Generally Accepted Privacy Principles” to understand the principles in more detail.

Beyond ensuring customer’s personal information is secure it is critical that conEdsion navigates through fragmented laws and pays special attention to the current complex contractual requirements and country specific requirements.

Please view the organizational regulatory privacy policy at the link below:

https://www.privacypolicies.com/live/df46c1cc-217b-4698-a82a-0aeb963871ba

M2-2 – Corporate Governance

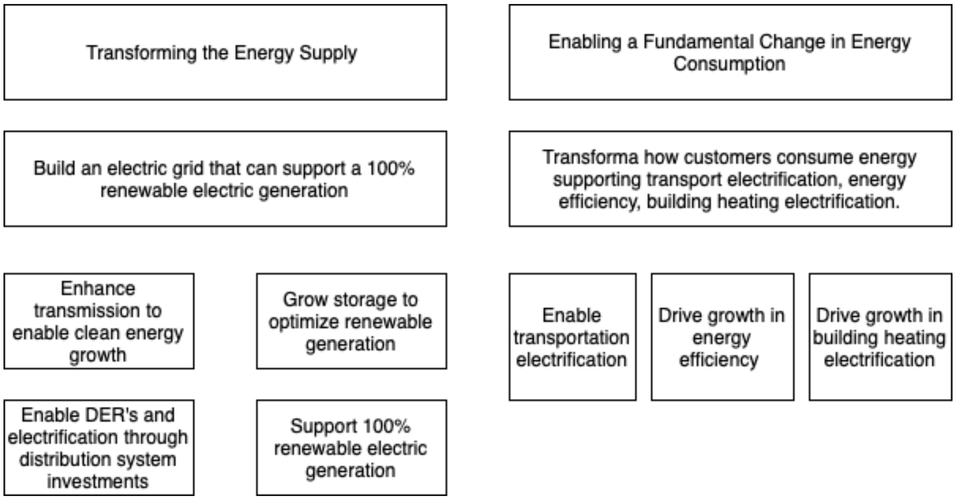
Corporate governance defines the framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in an organization’s relationship with its stakeholders.

The Board of Directors distribute responsibilities between five corporate governance activities to insure all needs are met. These include:

- **Risk Oversight:** How company prepares/responds to major disruptive events
  Ex) Improving managerial skills through coaching
- **Enterprise Architecture:** Decision making through documentation provides abstract view of an enterprise
  Ex) Building a Business Development Model to define how company resources will be used to create sales and revenue
- **Asset Management:** Policies and procedures for managing assets
  Ex) An asset is any item of value for an organization. ConEd collects customer’s personal information, data, such as telephone numbers, addresses, phone numbers, etc. which are high valued assets.
- **Change Management:** Provides structure for the activities that occur after the organization approves a change
  Ex) A team has 12 months to complete a project; however, one month in, the timeline was cut to 8 months
- **Business Continuity:** Planning and preparation of an organization to maintaining business functions
  Ex) It is important conEd prepares for outages with essential suppliers or services. In the case of an outage, conEd first makes sure critical buildings like hospitals, police and fire stations, nursing homes, and water treatment plants get power on.

*Below is an Enterprise Architecture example for conEdison (“A Comprehensive”).

Electric Clean Energy Strategies


Transforming the Energy Supply
Enabling a Fundamental Change in Energy Consumption
Build an electric grid that can support a 100% renewable electric generation
Transforma how customers consume energy supporting transport electrification, energy efficiency, building heating electrification.
Enhance transmission to enable clean energy growth
Grow storage to optimize renewable generation
Enable transportation electrification
Drive growth in energy efficiency
Drive growth in building heating electrification
Enable DER's and electrification through distribution system investments
Support 100% renewable electric generation

M3-1 – Business Continuity Planning

The Business Impact Analysis (BIA) predicts consequences of disruption of business functions and gathers information needed to develop recovery strategies. The purpose of NIST SP 800-34 is to identify the **three** steps typically involved in accomplishing the BIA:

- **Determine mission/business process and recover critically** that reflects maximum downtime can tolerate while staying aligned to mission
- **Identify resource requirements** to resume business processes as quickly as possible
- **Identify recovery priorities** based upon results from previous activities

ConEdison's mission is to, "…provide energy to our customers safely, reliably, and sustainably" ("About Our Company"). Looking further it is in the best interest to provide a fair return to investors and improve the quality of life for the communities they serve.

While identifying what areas require priority amidst a crisis, it is equally as important to ensure the right resources are required to recover quickly. A method in which conEdison has found success is to centralize their work primarily within New York State and to employ a large number of people within this area. CECONY directly employs, "…over 12,300 people, while its spending generates an additional 20,500 jobs in NYS" ("ConEdison Impact"). A large quantity of workers within a centralized area has resulted in, "…seven times fewer electricity interruptions and a four times faster response rate compared to national averages" ("ConEdison Impact").

In the case of a major outage the priority of conEdison is to ensure critical buildings get power first. Some elements of the mission may be effected after severe conditions, for example, "*providing a return to investors."* However, conEdison is confident in their plan of action during a downtime. It is vital they put the needs of their customers first.

A further advantage of remaining centralized is the money accrued for the state. ConEdison has contributed, "…$3.8 billion of taxes and fees in New York State in 2021, of which $2.9 billion went to the City of New York" ("ConEdison Impact"). The impact conEdison has on New York is drastic. Likely, in a crisis situation, NY would quickly come to conEdison's aid as they provide energy for so many residents and they provide a large return for the state. As a result this acts as a long term security blanket for conEdison's investors - even in the face of a crisis.

The **MTD** represents the total amount of time leaders are willing to accept for a business process outage and includes all impact considerations.

RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources.

The **RPO** represents the point in time to which business processes data must be recovered after an outage.

Preemptively conEdison has mapped out their plan in the chance of a crisis so there is a plan of attack before the fact. In alignment with the definitions above the key recovery activities include:

- Field reports are received and assessed for severity of damage
- Repair crews are dispatched, including those not normally assigned to the storm-damaged area
- Local officials are notified of any special problems in their communities
- Our liaison employees are deployed to county Emergency Management offices and other key locations to help coordinate public safety measures
- Contractors and crews from neighboring utilities are given safety briefings and assigned repairs in communities with a lot of damage
- Our Community Response Team members are sent to municipal offices in severely affected communities to provide direct assistance to government officials and customers
- The news media are kept updated on damage reports, restoration progress, and safety advisories
- After every major event or outage, we hold a "lessons-learned" meeting to further improve our plans (“Our Outage”)

M3-2 – Roles and Responsibilities

<u>Organizationalm Roles:</u>

- **CEO**
- **CFO**
- **SVP**
- **General Counsel**
- **Corporate Secretary**
- **Treasurer**
- **Controller**

The responsibilities of the CEO is to make major corporate decisions, managing overall operations, and setting the company's strategic direction. They are accountable to the board of Directors or stakeholders of the company.

CFO responsibilities include internal and external financial reporting, stewardship of company's assets, and ownership of cash management.

SVP responsibilities include setting business goals and solving internal issues as needed. They ensure employee compliance with company policies.

The General Counsel reviews, researches, interprets, and prepares both written and oral opinions on a wide variety of legal issues. Drafts, reviews, and approves policies and procedures, regulations, bylaws, and other legal documents.

The Corporate Secretary prepares reports, conducts searches, and collects data for upper management. They manage logistics of board and committee meetings.

The Treasurer oversees the financial administration, reviews procedures and financial reporting, advises the board on financial strategy, and advises on fundraising.

The Controller guides financial decisions by establishing, monitoring, and enforcing policies and procedures. They protect assets by establishing, monitoring, and enforcing internal controls.

References

"About Our Company." *Coned.com*, www.coned.com/en/about-us/careers/about-our-company.

"CMMI – Focus Software Companies." *Geo-viz.com*, 12 July 2013, geo-viz.com/blog/top-6-benefits-of-adopting-capability-maturity-model-cmmi-focus-software-companies/. Accessed 1 Mar. 2023.

"A Comprehensive View of Our Electric System through 2050." *Coned.com*, www.coned.com/-/media/files/coned/documents/our-energy-future/our-energy-projects/electric-long-range-plan.pdf.

"ConEdison Impact Study." *Coned.com*, www.coned.com/-/media/files/coned/documents/about-us/economic-impact-report.

"Consolidated Edison, Inc. Corporate Governance Guidelines." *Conedison.com*, 16 Feb. 2023, www.conedison.com/-/media/files/conedison/about-us/corp-governance/corp-governance-guidelines.pdf. Accessed 1 Mar. 2023.

"OECD Privacy Principles." *Oecdprivacy.org*, oecdprivacy.org.

"Our Outage Recovery Plan." *Coned.com*, www.coned.com/en/community-affairs/our-storm-recovery-plan.

"Privacy Framework." *Nist.gov*, www.nist.gov/privacy-framework.

"Pros and Cons of the CMMI Model." *Digital Adoption*, 16 Sept. 2022, www.digital-adoption.com/cmmi/. Accessed 1 Mar. 2023.

"The 10 Generally Accepted Privacy Principles." *linfordco.com*, linfordco.com/blog/the-10-generally-accepted-privacy-principles/.

White, Sarah K. "What is CMMI? A model for optimizing development processes." *CIo.com*, 1 June 2021, www.cio.com/article/274530/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html#:~:text=The%20Capability%20Maturity%20Model%20Integration,%2C%20product%2C%20and%20service%20development. Accessed 1 Mar. 2023.