***NIST CSF 1.1 assessment report for 'Verizon Telecommunications', a global telecommunication company***

**1. Identify - Asset Management (ID.AM):**

Verizon manages a large number of physical and digital assets spread across the globe, with several stakeholders (customers, employees, partners, and regulators) depending on their reliability, availability, and security. There is, however, a lack of total comprehension and management of these assets, particularly when it comes to recognizing and preserving sensitive data and resources.

Failure to identify and manage critical assets could expose sensitive data, increasing the chance of data breaches, service interruptions, and harming the company’s reputation. Moreover, an unstructured asset management approach could affect the company’s capacity to respond to security incidents or regulatory inquiries effectively.

The Information Technology and Network Operations functions are urged to review and enhance asset management practices, with particular attention to the following controls:

* ID.AM-1: Keeping control of all physical devices, systems, and networks. This that means every server, network gadget, and mobile device must be accounted for. Thus, the chances of unauthorized access or disruption are reduced.
* ID.AM-2: Keeping a thorough list of all software platforms and applications within the company (apps our customers use, backend systems and third-party software), allowing us to spot any vulnerabilities and keep everything updated.

**2. Protect – Access Control (PR.AC):**

Verizon’s access management currently lacks a well-defined workflow, exposing the organization to potential risks of unauthorized access and internal abuse, which could damage the company's data confidentiality and integrity.

Some users had incompatible or unnecessary access privileges that did not match the tasks or roles that they had to complete, raising concerns about the effectiveness of Verizon's access management controls.

The Information Technology and Human Resources departments are requested to create and enforce a policy that defines user activation workflows and strengthens password policies, with particular attention to the following controls:

* PR.AC-1: The goal is ensuring that users are assigned the appropriate access rights based on their roles and responsibilities, helping decrease the risk of unauthorized access and potential misuse of data.
* PR.AC-4: Managing access permissions is crucial for maintaining security, guided by the principles of least privilege and separation of duties and will lead to a decreased risk of unauthorized access due to vulnerable or stolen credentials. Regular updates and reviews of these permissions limit the damage that can be caused.

**3. Protect – Awareness and Training (PR.AT):**

Verizon lacks a comprehensive cybersecurity training program that addresses the risks and challenges that the company faces. A lack of training among employees may lead to a better chance of cybersecurity incidents caused by human errors. An effective cybersecurity training program is important for educating the employees about the best practices in cybersecurity and reducing the risks of cybersecurity incidents caused by human errors.

The Human Resources function, together with the Information Security function and the Chief Technology Officer need to organize and deliver information security training to meet the following subcategory requirements:

* PR.AT-1: Providing a comprehensive cybersecurity training program to all employees is essential in helping raise awareness and educating them about security risks and best practices in cybersecurity. This makes them protect the company's sensitive assets (customer data and intellectual property) and helps identify potential threats (phishing attempts, suspicious attachments or malicious links), thereby reducing the risk of fraudulent activities.
* PR.AT-3: External stakeholders (partners, vendors and customers) can adopt appropriate security measures if cybersecurity measures and protocols are presented to them. The increased degree of awareness reduces the risk of socially engineered attacks, in which the external stakeholders can be tricked into performing insecure actions or disclosing sensitive information.

**4. Detect – Anomalies and Events (DE.AE):**

Verizon, being a telecommunications company highly prioritizes the stability and reliability of its network operations and systems. Spotting oddities or unusual events is critical, as they are the antecedents or signs of potential cybersecurity issues.

Currently, there may not be a complete plan in place that tracks normal network operations and predicted data flows. Without a proper plan, it becomes harder to spot unusual events until it is too late. Similarly, an inexperienced team might struggle to understand and respond to detected events. A lack of skills and plan can lead to an ineffective response, that can cause potential damage to the organization's systems and reputation.

Under the guidance of the Chief Technology Officer and with the Information Technology and Network Operations departments, a more effective approach to detect these anomalies and events can be found, with particular attention to the following controls:

* DE.AE-1: It is crucial that the organization maintains a solid understanding of its network operations and data flows, by keeping an inventory of network devices and understanding how traffic usually behaves. By implementing this control, it will be easier to detect and stop potential issues.
* DE.AE-2: To understand what the attackers are targeting and how they are doing it, the spotted events need to be carefully studied. It is required to examine the incident, understanding its origin, goal, possible impact, and then drawing conclusions in order to improve the organization's defensive mechanisms. Having a specialized team within the IT department focused on this task can help increase the organization’s capacity to react quickly and effectively to cybersecurity threats.

**5. Recover – Recovery Planning (RC.RP):**

Verizon can not afford to have its services to go down due to a cyber issue because it can lead to substantial financial, operational, and reputational impacts. Therefore, it is mandatory to have an effective recovery plan that quickly gets systems or assets back online affected by a cyber incident.

Currently, there might be a lack of a solid recovery plan, that can lead to a lot more damage caused by a cyber incident. How the recovery plan is integrated into the process of handling a cyber incident is important, as it can lead to gaps in how the company responses.

The CEO and the Chief Technology Officer must ensure that Verizon is able to have a strong recovery plan. This requires a multi-departmental approach, especially IT, Network Operations, and the Finance and Accounting departments, as they have a big role in disaster recovery and business running. They should focus on the following:

* RC.RP-1: A structured and regularly tested recovery plan ensures quick system restoration post-cyber incidents, by developing recovery time objectives and recovery point objectives, as well as periodically reviewing and updating the plan based on testing outcomes and evolving risk scenarios.
* RC.RP-2: The incorporation of recovery planning into the incident management process allows an effective transition from incident response to recovery, implying the need of incorporating lessons learned from past incidents into recovery strategies, safeguarding recovery efforts from being compromised by incident response activities and using the recovery phase to improve system resilience against future incidents.

After assessing Verizon’s current cybersecurity measures and understanding the strengths and weaknesses better, the next step is to set the minimum levels for each control area using the NIST CSF 1.1 scale, which highlights the gaps that have to be addressed, setting goals for improved security:

**1. Identify - Asset Management (ID.AM)**

ID.AM-1: Currently the Tier is 1 (Partial): tracking of physical devices in the network is not accurate, leading to unclear visibility of the network structure. The target is to achieve Tier 3 (Repeatable), where all devices are inventoried and their statuses are consistently tracked. To progress to the desired tier, Verizon should implement a systematic inventory management system for physical devices, that should be constantly updated and audited.

ID.AM-2: The current Tier is 2 (Risk Informed): software platforms and applications inventory is not properly maintained or updated, also the target is to reach Tier 3 (Repeatable), by setting up regular updates that help avoid vulnerabilities related to outdated software.

**2. Protect – Access Control (PR.AC)**

PR.AC-1: At the moment the Tier is 1 (Partial), meaning that the organization lacks a robust system for managing credentials of devices and users. The desired level is Tier 4 (Adaptive) and can be reached by allowing dynamic access management of credentials and response to changes in real-time.

PR.AC-4: The current Tier is 2 (Risk Informed), where access permissions are managed without a systematic approach or proper guidelines, the target being achieving Tier 3 (Repeatable) to reduce the risk of unauthorized access and internal abuse, by establishing clear access control policies.

**3. Protect – Awareness and Training (PR.AT)**

PR.AT-1: Currently the Tier level is 2 (Risk Informed), as the provided training to employees is limited, to achieve the desired level, Tier 4 (Adaptive), it needs to keep the employees informed of current threats and best practices frequently, by providing comprehensive and regular cybersecurity training.

PR.AT-3: At the moment the current Tier is 1 (Partial), as the communication about the cybersecurity responsibilities with third-party stakeholders is limited, to get to the desired level, Tier 3 (Repeatable) it is needed to have regular discussions with external partners to help them understand their cybersecurity responsibilities, minimizing breach risks.

**4. Detect – Anomalies and Events (DE.AE)**

DE.AE-1: Currently the Tier level is 1 (Partial): Verizon’s baseline for network operations lacks clarity and consistency. The target level is Tier 3 (Repeatable), aiming for an improved detection of oddities and potential attacks through stable network baselines. Moving to the desired tier can be achieved by creating clear baselines for network operations.

DE.AE-2: Also the Tier level is 1 (Partial): current analysis of the detected events lacks structure, making it difficult to understand attack targets and strategies. The target level is also Tier 3 (Repeatable), systematic event analysis allowing to learn from previous incidents and improve defense mechanisms, this can be achieved by implementing advanced analysis tools and protocols for regular views.

**5. Recover – Recovery Planning (RC.RP)**

RC.RP-1: At the moment the Tier level is 2 (Risk Informed), as longer system downtimes are due to the fact that the recovery processes and procedures are not well-maintained or executed. The goal is to reach Tier 3 (Repeatable), ensuring that implementing repeatable recovery processes leads to timely restoration of systems after an incident, this can be done by revising and improving the recovery processes and procedures.

RC.RP-2: The current Tier level is 1 (Partial), as the recovery planning is not effectively incorporated into incident management. The goal is also to reach Tier 3 (Repeatable), minimizing the impact of cybersecurity incidents by integrating recovery planning into incident management. This can be done setting clear recovery objectives and strategies in the incident response plan.

Verizon's defensive approach relies heavily on understanding the threat landscape. It is non-negotiable to identify important risks and take the appropriate procedures to minimize these threats. Failure to follow these suggestions might result in serious cybersecurity consequences such as illegal data access, halts in operational flow and harm to the company's reputation.

After going through Verizon's cybersecurity measures across the five categories and considering the nature of the sensitive activities the organization is dealing with, it appears that the company should aim for Framework Implementation Tier 3 (Repeatable). Getting to this level means that the organization has put in place a solid framework of risk management procedures and keeps a regular check on its cybersecurity defenses. This can be achieved through a step-by-step process, each carefully executed and reviewed to guarantee proper implementation and integration.

The company should begin by focusing on the core parts of its cybersecurity architecture, by gaining better control over its IT infrastructure (ID.AM-1) and improving activation operations and password regulations (PR.AC-1) and focus on strengthening its management of access permissions (PR.AC-4).

Secondly, the company should enhance its operational aspects, by improving the inventory management process for all software platforms and applications (ID.AM-2) and implementing efficient detection processes (DE.AE-2 and DE.AE-3).

Lastly, Verizon should concentrate on the advanced aspects of its cybersecurity setup, by developing a comprehensive cybersecurity program for it its employees and external stakeholders (PR.AT-1 and PR.AT-3) and prioritize regular testing of recovery processes and procedures (RC.RP-1 and RC.RP-2).

Verizon has the opportunity to dramatically strengthen its cybersecurity framework by strategically focusing on the indicated areas, lowering exposure to cyber attacks and assuring the dependable and flawless flow of its operations.