Security and Risk: Management and Certifications

Cybersecurity Assessment Report

University of Padova

Lorenzo D'Antoni
Student Number: 2073767

June 3, 2024

Contents

1 Introduction

The aim of this document is to perform a cybersecurity assessment report using generative AI that complies with the NIST Cybersecurity Framework (CSF) 2.0 [6]. Then, in the final section, I will analyze and critically examine what the AI model has produced. To do so, a fictitious use case on which to write the report is necessary. The next paragraphs will provide some context about the chosen use case, the methodology used to construct the assessment, and how the risk was measured.

1.1 Use Case

It's important to highlight that the use case is fictitious and not complete by any means but the aim is to make it as real as possible. I decided to analyze *Emax*, a newly launched fintech startup in Italy, out to disrupt traditional banking with its fully virtual model. This small, approximately 50-person company provides core banking services such as deposits, withdrawals (both at ATMs and peer-to-peer), transfers, and basic budgeting tools. Their roadmap includes bill payments, while cryptocurrency and investment services are considered longer-term goals. *Emax*'s primary focus lies in delivering essential banking services with unparalleled ease of use and efficiency.

To achieve their goals, *Emax* relies heavily on cloud-based solutions. They have adopted a Banking-as-a-Service (BaaS) platform, specifically *Solarisbank*, for their core banking system. This choice streamlines their operations and reduces compliance overhead. A popular CRM, *Salesforce*, is used for customer relationship management. Identity and Access Management (IAM) is handled through *Okta*, enforcing strict Multi-Factor Authentication (MFA) policies for all user access. Data analytics relies on a managed data lake service within *AWS*, along with *Power BI* for business intelligence visualizations.

This approach reduces upfront investments, enables scaling as needed, offloads management and security responsibilities to the providers, facilitates potential market expansion, and allows them to benefit from the generally superior security capabilities of major cloud vendors. Recognizing the Italian market's preference for debit cards, *Emax* currently focuses on providing a streamlined debit card program, simplifying their initial compliance journey.

Emax carefully manages a range of sensitive customer data, including Personally Identifiable Information (PII), financial account information, debit card details (handled by a PCI-DSS [11] compliant processor), and behavioral and login patterns.

Customers can apply for an *Emax* account through the mobile app or web portal, with E-KYC (Electronic Know Your Customer) procedures, including ID scans and video identity checks, ensuring compliance.

They partner with an established external card issuer, handling the technical and financial aspects of debit card production, payment processing, fraud management, and compliance with card industry standards. This allows *Emax* to focus entirely on customer acquisition and building best-in-class user experiences.

Emax provides customer support through in-app chat, email, and a limited call center. Due to their startup nature and budget realities, they prioritize cloud-based fraud detection solutions, utilizing a vendor like *Kount*, which com-

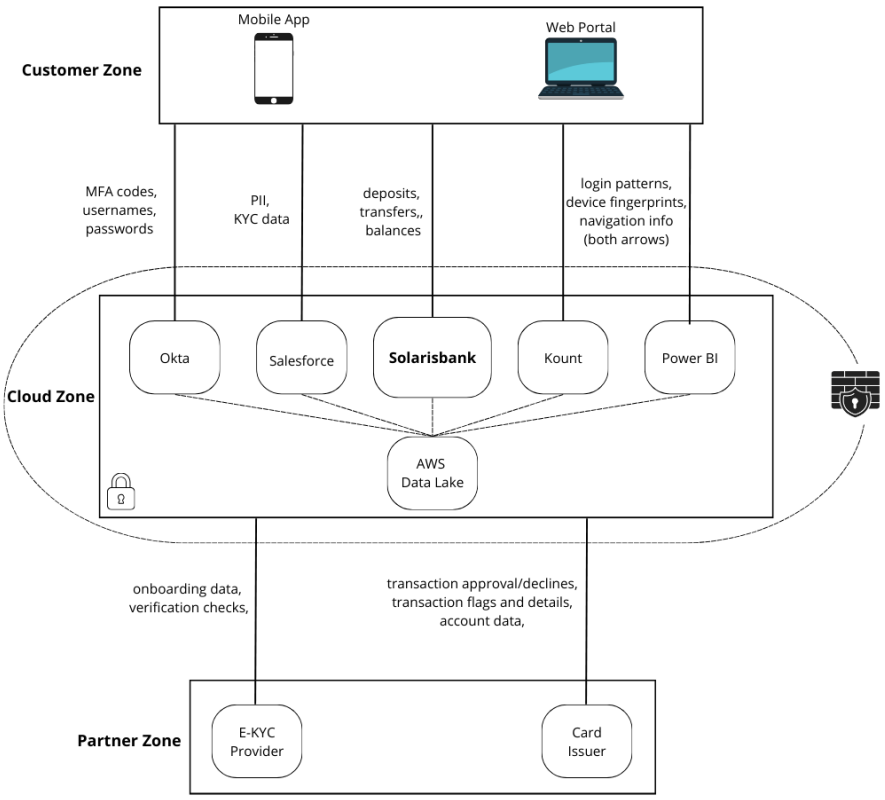

Figure 1: A basic diagram depicting the IT system architecture of the small bank. All arrows indicate bidirectional connections. The Cloud Zone is safeguarded by a firewall, and data exchanges between other zones and the Cloud Zone are secured through encryption.

bines rule-based flags and Machine Learning models to identify suspicious transactions and evolving fraud patterns. *Emax* lacks a dedicated CSIRT (Computer Security Incident Response Team). Incident response actions would fall under the responsibility of their existing but small security team.

Beyond GDPR [2] and PSD2 [1], *Emax* must adhere to Italian-specific regulations. These include the Legislative Decree No. 231/2007 (Anti-Money Laundering) [5], which requires robust customer identification, transaction monitoring, and suspicious activity reporting. They must also comply with Bank of Italy Regulations, which outline specific guidelines for financial institutions within the Italian context.

A simple diagram illustrating the bank's IT system architecture is presented in Figure 1.

1.2 Cybersecurity framework

All security risk-related terms (asset, impact, threat, vulnerability, risk, likelihood, risk assessment, etc.) adhere to the definitions established by ISO 27005 [3].

The cybersecurity assessment report will be based on the NIST Cybersecurity Framework (CSF) 2.0 [6]. The framework is structured around a hierarchy of functions, including Govern, Identify, Protect, Detect, Respond, and Recover. These functions outline high-level cybersecurity outcomes that can help any organization effectively manage its cybersecurity risks. Furthermore, the framework introduces the concept of Organizational Profiles and Tiers. Organizational Profiles allow an organization to describe its current and/or target cybersecurity posture in terms of the outcomes defined by the framework's functions. Tiers, on the other hand, can be applied to these Organizational Profiles to characterize the rigor of an organization's cybersecurity governance and management practices.

Since this report cannot go much beyond the 10 pages, it will be based on the NIST Cybersecurity Framework (CSF) 2.0 Small Business Quick-Start Guide [8]. This Guide provides a concise summary of the most important actions to consider for each of the six high-level functions defined by the NIST CSF 2.0 [6], based on the framework's subcategories (outcomes).

By focusing on the key actions for each function, the Guide offers a good starting point for small organizations to enhance their cybersecurity posture. This is a more effective approach than manually selecting only some outcomes from the functions or analyzing only some functions from the framework.

1.3 Structure of the AI-based assessment

The cybersecurity assessment report will begin with a dedicated section focusing on asset identification and risk assessment. One crucial asset will be analyzed to show how risk assessment can be done systematically. The analysis spanned several pages due to the chosen format and structure, which I believe is the best for clarity and simplicity. However, if there were no limitations on space, incorporating a summary table would be preferable.

This will be followed by an analysis of the key actions to consider for each function of the NIST CSF 2.0 [6], as provided in the Small Business Quick-Start Guide [8].

The analysis will highlight the organization's current cybersecurity profile, which characterizes the extent to which each outcome defined by the NIST CSF 2.0 [6] is being achieved. For each function, the report will identify areas of improvement and outline specific actions the organization can take to enhance its cybersecurity posture.

By following this structured approach, the report will provide a comprehensive assessment of the organization's cybersecurity state and a clear roadmap for improving its overall cybersecurity resilience.

1.4 How the risk was measured?

Conducting a thorough risk assessment is a complex but crucial step in an organization's cybersecurity strategy.

The risk assessment process begins with developing an inventory of the organization's assets and assigning a value to each asset. Next, the organization must identify the relevant threats to each asset and determine the level of vulnerability to those threats. Additionally, the organization should assess the security controls currently in place to mitigate the identified threats.

For each asset, the organization must then determine the potential impact on the business, in terms of cost, if a threat were to materialize. The company must also assess the likelihood of a threat occurring, based on the effectiveness of the existing security controls. The level of risk will be determined as the combination of the impact and likelihood of the threat occurring.

However, accurately estimating all these factors and assessing the entire range of threats can be challenging. Therefore, an iterative risk management life cycle, as outlined in the NIST SP 800-37 [10], is necessary. This approach involves continuously monitoring and evaluating the effectiveness of risk treatment measures, with the results feeding back into the next iteration of the risk management process.

Given the difficulty in quantifying impact and likelihood, especially for a small organization like *Emax*, a qualitative assessment approach may be more practical.

Nevertheless, it is important to acknowledge that a qualitative approach may result in insufficient differentiation between important risks. This inherent subjectivity is a limitation that should be considered when interpreting the results of the risk assessment. To address this challenge, small organizations may need to explore additional risk analysis methods or seek guidance from experts to supplement the qualitative assessment.

FIPS 199 [9] provides three security impact categories (Low, Medium, and High) and describes them in detail. Additionally, NIST SP 800-100 [7] assigns qualitative likelihood ranges to these categories. According to this standard, the Low likelihood range is defined as less than or equal to 0.1, the Medium likelihood range is between 0.1 and 0.5, and the High likelihood range is between 0.5 and 1.0.

The vulnerability, likelihood, impact, and overall level of risk will be determined using a series of risk assessment matrices provided by [13] (Figure 3).

1.5 How the AI-based assessment was generated

For generating the cybersecurity assessment report, I've chosen the *Gemini 1.0 Ultra* AI model, with a $32,000$-token context window, bridging the gap between OpenAI's *gpt-3.5-turbo* and GPT-4 models. While Google has been reticent about *Gemini*'s technical details, we know it employs a Mixture-of-Experts architecture, selecting the most pertinent expert module to address queries, ensuring specialized responses.

Although *Microsoft Copilot* and *Perplexity* are viable free options, *Copilot*'s input/output capabilities and conversational memory are limited, while *Perplexity*, despite enhancing the GPT-3.5 OpenAI model with various improvements like web search integration, source-linked answers, and image/document analysis, lacks the technical precision required for generating a comprehensive cybersecurity assessment directly from an attached document.

Therefore, I opted for a potentially more robust AI model and broke down the task of creating the entire report into smaller segments, submitting them individually to the model.

In particular, I adopted a consistent method: I presented the small virtual bank scenario to the model, outlined the structure of the input for analysis (always a subsection of a problem, such as one asset or one NIST function at a time), and clarified the expected response format. Before proceeding, I

confirmed the model's comprehension of the task and whether it required additional information to respond unambiguously. I then began submitting the topic's subsections (e.g. Govern function) and continued until the entire topic was addressed (e.g. all the NIST functions).

2 AI-based Assessment

2.1 Asset Identification

Emax does not have a structured way to identify and assess the assets. Figure 2 provides a uniform and simple way of documenting the assets. As the company matures and grows, a more sophisticated and formal method must be used.

The **Asset Classification** categorizes the assets based on value and sensitivity (Critical, High, Moderate, Low). The **Exposure Level** assesses the vulnerability of the assets to cyber threats, compliance risks, or disruptions (High, Medium, Low). The **Disaster Recovery Priority** indicates the urgency of restoring the asset in a disaster (Tier 1 - immediate, Tier 2 - within $24 - 48$ hours, Tier 3 - lower priority).

All the services in the Cloud Zone are classified as Medium regarding the level of exposure. This is because they are provided by very reputable and known vendors with very high and proved security measures. However, they cannot be classified as Low since they remain core breach entry points and the provider reliability and trust is still a factor.

The mobile app and the web portal provide a way to interact with *Emax*'s services. They present a significant attack surface for social engineering attacks, phishing attempts, and malware distribution. However, they can be patched, updated and redeployed relatively quickly compared to the other services. This mitigates the long term impact of a security breach. Moreover, the use of secure communication protocols (HTTPS) and proper data encryption should minimize the exposure of sensitive data in transit. *Emax*'s also employs authentication and authorization mechanisms to restrict access to sensitive features and data. This justifies the Moderate and Medium ratings in the asset classification and exposure level columns.

The services in the Partner Zone (Card Issuer and E-KYC provider) are vital for the small bank and *Emax* should rely on their security measures. This and the impact of some violations in these services justify their High markings in both Asset Classification and Exposure Level.

This inventory is NOT exhaustive. Collaborate with different departments to ensure completeness and identify additional assets as they grow, add services, and onboard new vendors.

Next, a crucial asset will be analyzed to demonstrate the application of the risk management life cycle, as defined by X.1055 [4]. This will serve as a framework for analyzing all assets not reported here due to page restrictions.

2.2 Risk management life cycle

2.2.1 Customer Data

Threats:

Asset Name	Asset Description	Asset Classification	Exposure Level	Disaster Recovery Priority
Core Banking System	Cloud-based BaaS Platform (SW)	Critical	Medium	TIer 1
Customer Data	PII, Account Balances, Transaction History, Behavioral Data (Data)	Critical	High	Tier 1
CRM System	Customer Data, Interactions, Marketing Data (SaaS)	High	Medium	Tier 2
Employee Worstations	Company-issued laptops and desktops (HW)	Moderate	Low	Tier 3
Mobile App & Web Portal	Frontend code, API connections (SW)	Moderate	Medium	Tier 1
IAM	User Accounts, Authentication Credentials, Authorization Policies (SaaS)	Critical	Medium	Tier 1
E-KYC Integration	API connection and Data Exchange with the KYC Provider (SaaS)	High	High	Tier 2
Card Issuer Integration	API connection and Data Exchange with the Card Issuer (SaaS)	High	High	Tier 2

Figure 2: Asset Register.

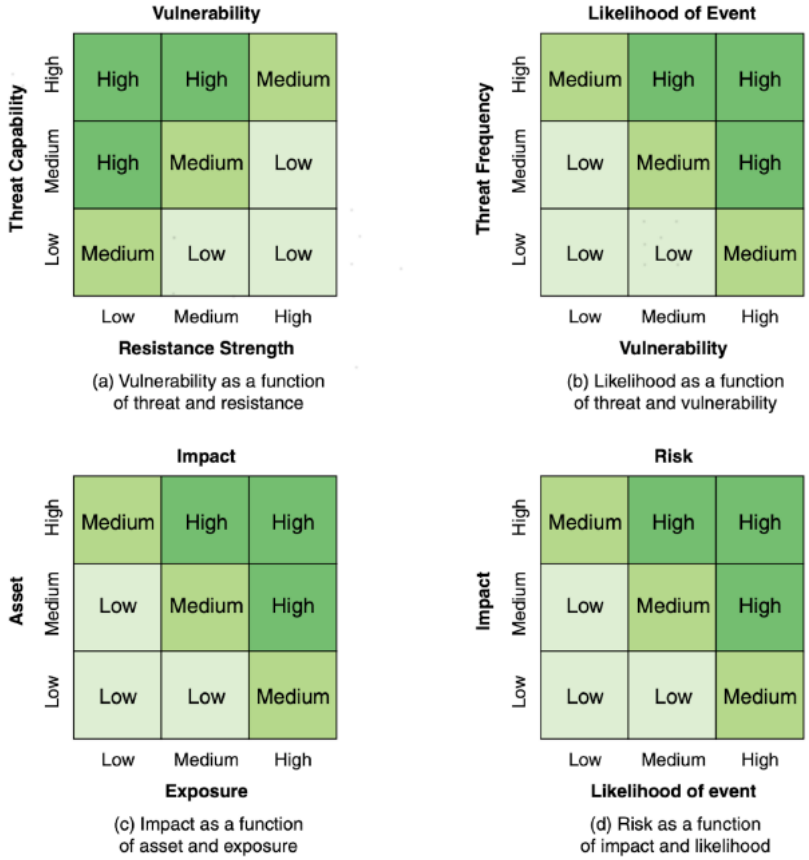

Figure 3: Matrices provided by [13] used to assess the level of risk.

- *Data Breach*: unauthorized access to data through hacking, phishing, or social engineering.
- *Accidental Exposure*: human error or system misconfigurations could lead to sensitive data being accidentally exposed to unauthorized users.
- *Ransomware*: encryption of data for extortion.

Vulnerability Assessment (as a function of the capability of the threat and the resistance strength of an asset to that particular threat):

- *Data Breach*: High.

  Resistance strength: Medium. *Emax* has some defenses in place but cloud systems are complex to protect.

  Threat capability: High. Software vulnerabilities or phishing techniques can be exploited.

- *Accidental Exposure*: Medium.

Resistance strength: Medium. Technical safeguards can help, but data is often moved and handled by employees, creating opportunities for mistakes.

Threat capability: Medium. It often doesn't require advanced technical skills.

- *Ransomware*: High.

  Resistance strength: Medium. *Emax* has some defenses, but ransomware often exploits unpatched systems or leverages phishing attacks to gain a foothold.

  Threat capability: High. Ransomware groups range from opportunistic attackers to sophisticated actors capable of customized attacks.

Existing Controls:

- *Firewalls and Intrusion Detection*: provides basic network-level protection (managed by BaaS).
- *Encryption*: employed to protect data at rest and in transit.
- *Access Controls (Okta)*: limit access and reduce the impact of credential compromises.
- *Data Handling Policies:*: these outline safe practices, but enforcement and employee awareness are key.
- *Data Loss Prevention (DLP) Tools*: these can detect and block accidental data transfers in some cases.
- *Data Backups*: while not prevention, good backups minimize the impact of a ransomware attack.
- *System Patching*: keeping software updated reduces known vulnerabilities that ransomware exploits.

Impact Assessment (as a function of the asset class and the exposure to loss that a particular threat could cause):

- *Data Breach*: High.

  Exposure: High. Could cause direct financial loss, severe reputation damage, regulatory penalties.

  Asset: High.

- *Accidental Exposure*: High.

  Exposure: Medium to High. It depends heavily on the specific data exposed and to whom.

  Asset: High.

- *Ransomware*: High.

  Exposure: High. The potential for financial loss (ransom and recovery), reputational damage, and downtime is very severe.

  Asset: High.

Likelihood Assessment (as a function of the frequency of the threat and the vulnerability to that threat):

- *Data Breach*: High.

  Vulnerability: High. The attack surface includes their frontend applications, partner integrations and the cloud systems they rely on.

  Threat frequency: Medium. Data breaches are frequent in the financial sector.

- *Accidental Exposure*: Medium.

  Vulnerability: Medium. Technical safeguards can help but misconfigurations or bypassing procedures by employees remains a concern.

  Threat frequency: Medium. Human error is inevitable in any organization.

- *Ransomware*: High.

  Vulnerability: High. *Emax*'s reliance on cloud systems and connected devices makes them a potential target.

  Threat frequency: Medium. Ransomware is rampant, and attackers frequently target businesses of all sizes.

Risk Level (as a function of impact and likelihood):

- *Data Breach*: High.

  Impact: High.

  Likelihood: High.

- *Accidental Exposure*: High.

  Impact: High.

  Likelihood: Medium.

- *Ransomware*: High.

  Impact: High.

  Likelihood: High.

Potential Additional Controls & Prioritization:

- *Data Classification*: classify customer data based on sensitivity to prioritize protection efforts.
- *Penetration Testing*: Regularly test *Emax*'s systems for vulnerabilities to identify and address weaknesses before attackers exploit them.
- *Data Backups and Disaster Recovery*: Implement robust backups and disaster recovery procedures to ensure data availability in case of incidents.

Monitoring & Evaluation:

- Regularly monitor system logs for suspicious activity and security events.
- Conduct periodic risk assessments to identify and address emerging threats.
- Review and update security policies and procedures as needed.
- Measure the effectiveness of existing controls and make adjustments as necessary.

2.3 Cybersecurity Report

2.3.1 Govern

To assess *Emax*'s posture with respect to the NIST CSF's Govern function, a selection of actions from the Small Business Quick-Start Guide [8] was considered (Figure 4). Actions were prioritized based on their relevance and criticality for a small fintech startup like *Emax*.

Action to consider	Current cybersecurity profile
Understand how cybersecurity risks can disrupt the achievement of your business's mission **(GV.OC-01)**	The company understands that cybersecurity is crucial. Data breaches, ransomware, and downtime would be detrimental to their core mission of providing reliable banking services. However, they lack a formal process to tie specific cyber threats to quantifiable business impacts. Due to limited resources and staff, it prioritizes daily operations over strategic risk analysis.
Understand who within your business will be responsible for developing and executing the cybersecurity strategy **(GV.RR-02)**	Emax, being a small company, doesn't have a dedicated CISO. Cybersecurity responsibility may be split between their small IT/security team, with management providing overall direction and outsourcing some aspects. Roles and responsibilities for cybersecurity seem informal. While suitable at their current scale, this creates ambiguity and may hinder scaling up security as they grow.
Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships **(GV.SC-06)**	Emax relies heavily on cloud providers and has partner integrations, so the vendor's security significantly affects Emax's risk profile. They do some level of due diligence when selecting these vendors but don't have a consistent process for ongoing risk assessment. Emax requires a more formalized approach to assess third-party risks to safeguard themselves and their customers.

Figure 4: *Emax*'s Govern function assessment.

Overall Govern assessment. *Emax* appears to have foundational awareness of governance elements but lacks the formal structures and processes that would be expected of a larger organization. The CSF Tier for Govern is Tier 2 (Risk Informed).

Target profile enhancements. To reach CSF Tier 3 (Repeatable), the company should implement the following measures: establish a risk register (linking cybersecurity risks to business impact), implement compliance mapping (aligning regulations with specific controls and security practices), establish a governance structure (documenting roles, responsibilities, and escalation paths for cybersecurity decisions) and develop a vendor risk framework (with defined procedures for assessing vendor risk during onboarding and regularly thereafter).

2.3.2 Identify

To assess *Emax*'s posture with respect to the NIST CSF's Identify function, a selection of actions from the Small Business Quick-Start Guide [8] was considered (Figure 5). Actions were prioritized based on their relevance and criticality for a small fintech startup like *Emax*.

Action to consider	Current cybersecurity profile
Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services **(ID.AM-01/02/04)**	Emax has a basic inventory of major components, but it lacks granularity and overlooks many third-party integrations. Its focus is primarily on IT components rather than data assets.
Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement **(ID.IM-01)**	Emax conducts informal or ad-hoc assessments as issues arise. They might rely on vendors for some security assessments but lack a structured internal review process. They need a more proactive and consistent approach to identifying weaknesses and gaps in their controls.
Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register **(ID.RA)**	Emax has a general awareness of cyber threats but does not have a formal risk register that documents them systematically, including potential impacts and response plans.
Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties **(ID.IM-04)**	Formal communication of security plans beyond basic acceptable use policies for staff is limited. Vendors are not fully aware of Emax's expectations. Implementing a more structured communication and training program for both employees and partners would enhance overall security awareness.

Figure 5: *Emax*'s Identify function assessment.

Overall Identify assessment. *Emax* has a rudimentary understanding of identifying assets and risks but lacks the formal processes and documentation expected in a more mature state. The CSF Tier for Identify is between Tier 1 (Partial) and Tier 2 (Risk Informed).

Target profile enhancements. To achieve CSF Tier 3 (Repeatable), the company should focus on several key areas. This includes establishing a Comprehensive Asset Inventory covering hardware, software, and classified data, implementing Regular Risk Assessments such as vulnerability scans and penetration testing, documenting threat scenarios in a Formal Risk Register, and instituting a Security Awareness Program with regular staff training and vendor communication protocols.

2.3.3 Protect

To assess *Emax*'s posture with respect to the NIST CSF's Protect function, a selection of actions from the Small Business Quick-Start Guide [8] was consid-

ered (Figure 6). Actions were prioritized based on their relevance and criticality for a small fintech startup like *Emax*.

Action to consider	Current cybersecurity profile
Understand what information employees should or do have access to. Restrict sensitive information access to only those employees who need it to do their jobs **(PR.AA-05)**	Emax uses Okta, indicating at least some level of role-based access control (RBAC). RBAC is foundational, but Emax might benefit from a more refined model based on the principle of least privilege to reduce their risk profile.
Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords **(PR.AA-03)**	Emax mandates MFA and password managers.
Prioritize regularly backing up your data and testing your backups **(PR.DS-11)**	Their core data resides in the BaaS platform (Solarisbank), which handles backups. However, Emax should know their vendor's backup procedures and have a plan in case local data (even temporary) is lost. Emax needs clarity on vendor responsibilities and should have their own procedures for any data they manage directly.
Prioritize configuring your tablets and laptops to enable full-disk encryption to protect data **(PR.DS-01)**	Encryption is in place for all company-issued devices. Personal devices are not permitted.
Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks **(PR.AT-01/02)**	Beyond basic training, there's limited ongoing communication about recognizing attacks, reporting incidents, and practicing good cyber hygiene. A formalized program would mitigate this risk.

Figure 6: *Emax*'s Protect function assessment.

Overall Protect assessment. *Emax* has a decent foundation but needs a more consistent approach to access controls, data protection, and proactive staff training. The CSF Tier for Protect is Tier 2 (Risk Informed).

Target profile enhancements. To achieve CSF Tier 3 (Repeatable), the company should focus on several key areas. This includes implementing fine-grained Role-Based Access Control (RBAC) to closely align access controls with job functions, establishing a comprehensive Backup and Recovery Plan with clear vendor responsibilities and supplementary data backup strategies and instituting a formal Security Awareness Training program with regular sessions for all staff.

2.3.4 Detect

To assess *Emax*'s posture with respect to the NIST CSF's Detect function, a selection of actions from the Small Business Quick-Start Guide [8] was considered (Figure 7). Actions were prioritized based on their relevance and criticality for a small fintech startup like *Emax*.

Action to consider	Current cybersecurity profile
Understand how to identify common indicators of a cybersecurity incident **(DE.CM)**	Emax has a basic understanding of common attack indicators but lacks the knowledge to identify sophisticated attack techniques. Lack of staff-wide awareness of incident indicators creates delays in detection and response, escalating potential harm.
Assess your computing technologies and external services for deviations from expected or typical behavior **(DE.CM-06/09)**	Emax relies heavily on their vendors for primary threat detection. They have some basic log monitoring but may not have a sophisticated system for anomaly detection. Their reliance on vendor security leaves them potentially blind to unusual activity within their own portions of the system or in how data interacts with partner services.
Assess your physical environment for signs of tampering or suspicious activity **(DE.CM-02)**	As a virtual bank, their physical footprint is small. However, they lack formal processes for monitoring and reporting anomalies in their physical workspace, which creates vulnerabilities.
Communicate with your authorized incident responder, such as an MSSP, about the relevant details from the incident to help them analyze and mitigate it **(DE.AE-06/07)**	Emax lacks a dedicated CSIRT and does not have a contract with an MSSP (Managed Security Service Provider). Their incident response likely involves escalating to vendors and potentially ad-hoc improvisation.

Figure 7: *Emax*'s Detect function assessment.

Overall Detect assessment. *Emax* appears to have very rudimentary detection capabilities, relying heavily on their vendors and lacking proactive monitoring of their own environment. The CSF Tier for Detect is Tier 1 (Partial).

Target profile enhancements. To attain CSF Tier 3 (Repeatable), the company should focus on several key areas. This includes providing Incident Indicator Training to staff to recognize common signs of compromise like phishing emails and unusual system behavior, implementing a centralized log collection tool or service for SIEM or Log Analysis to detect unusual patterns, establishing basic Physical Security Procedures for reporting unusual activity at office spaces, and developing an Incident Response Plan outlining contact procedures, vendor escalation, and communication chains. Consideration should also be given to retaining a Managed Security Service Provider (MSSP) for serious incidents.

2.3.5 Respond

To assess *Emax*'s posture with respect to the NIST CSF's Respond function, a selection of actions from the Small Business Quick-Start Guide [8] was considered (Figure 8). Actions were prioritized based on their relevance and criticality for a small fintech startup like *Emax*.

Action to consider	Current cybersecurity profile
Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan **(RS.MA-01)**	Emax lacks a formal Incident Response (IR) plan. Roles and responsibilities for response are ad-hoc and based on the nature of the perceived threat. A significant incident would likely lead to confusion and delays without a structured plan and decision-making hierarchy.
Assess the incident to determine its severity, what happened, and its root cause **(RS.AN-03, RS.MA-03)**	Their analysis capabilities are limited. They rely heavily on vendors for root-cause analysis if the issue is on the vendor's side, hindering their ability to learn and improve their own defenses.
Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies **(RS.CO-02/03)**	Emax is obligated to communicate due to regulations like GDPR. However, they lack predefined communication templates and a clear process for escalating to the right authorities or notifying affected customers.

Figure 8: *Emax*'s Respond function assessment.

Overall Respond assessment. *Emax* appears very unprepared for incident response. They lack the structured planning and processes needed to effectively handle a cyber incident. The CSF Tier for Respond is Tier 1 (Partial).

Target profile enhancements. To achieve CSF Tier 3 (Repeatable), the company should prioritize several key measures. This includes establishing a Basic Incident Response (IR) Plan, which outlines incident types, severity levels, communication channels, reporting obligations, and escalation paths both internally and to vendors or authorities. Additionally, it's essential to develop Forensic Capabilities by retaining logs for analysis and establishing a relationship with an external forensics provider for serious incidents. Furthermore, implementing Communication Templates for timely and compliant notifications to customers, regulators, and partners is crucial.

2.3.6 Recover

To assess *Emax*'s posture with respect to the NIST CSF's Recover function, a selection of actions from the Small Business Quick-Start Guide [8] was considered (Figure 9). Actions were prioritized based on their relevance and criticality for a small fintech startup like *Emax*.

Action to consider	Current cybersecurity profile
Understand who within and outside your business has recovery responsibilities **(RC.RP-01)**	Emax lacks clearly defined roles for who leads recovery internally. Emax relies heavily on vendors in case of a major outage but lacks a plan for how they'd recover their own data, configurations, or customer communications if compromised.
Assess what happened by preparing an after-action report (on your own or in consultation with a vendor/partner) that documents the incident, the response and recovery actions taken, and lessons learned **(RC.RP-06)**	Post-incident analysis is informal, focusing on fixing the immediate issue without a structured approach to root cause determination or capturing lessons learned to inform future improvements.
Assess the integrity of your backed-up data and assets before using them for restoration **(RC.RP-03)**	While they have backups via the vendor, their backup testing for internal systems and data might be infrequent and lacks a formal verification process.
Prioritize your recovery actions based on organizational needs, resources, and assets impacted **(RC.RP-02)**	Emax would struggle to prioritize which systems need restoration first without a predefined plan aligned with business continuity needs.

Figure 9: *Emax*'s Recover function assessment.

Overall Recover assessment. *Emax* appears very unprepared in the area of recovery. Lack of planning, backup procedures, and post-incident analysis pose significant risks to their business continuity. The CSF Tier for Recover is Tier 1 (Partial).

Target profile enhancements. To achieve CSF Tier 3 (Repeatable), the company should focus on several critical areas. Firstly, it should develop a Recovery Plan integrated with the Incident Response (IR) plan, outlining vendor dependencies, communication channels, and priorities for restoration efforts based on criticality. Additionally, regular testing and verification of backup integrity, both vendor-owned and internally managed, through Backup Testing is essential. Lastly, implementing a structured process for Post-Incident Reviews is crucial for documenting incidents, evaluating response effectiveness, identifying root causes, and identifying areas for improvement.

3 Discussion

Current AI models lack the capability to conduct a comprehensive cybersecurity assessment directly from the NIST CSF 2.0 [6] document. To address this, the assessment was broken down into smaller, easier tasks. Each task comes with clear, detailed instructions for the AI model to help create sections of the report.

The *Gemini 1.0 Ultra*, with its huge question input size and context window, easily accommodated the use case description of the small bank, allowing for subsequent references with ease.

In the creation of the Asset Register (Figure 2), the model effectively identified the company's key assets. Additional prompts were necessary to extract the reasoning behind the model's selections and responses. While a more comprehensive list would have been preferred, space limitations allowed for only the most important assets to be included.

Afterwards, the model was asked to choose an asset for in-depth analysis. Initially, its responses were broad and lacked technical detail. With clarifying prompts, a technically accurate response was obtained. The model then carried out a more comprehensive risk assessment for the selected asset, but had to be concise due to page constraints.

For similar reasons, the model was directed to briefly analyze the actions related to each of the six CSF functions. Although lacking detailed technical data, the responses captured the company's current cybersecurity profile informally yet accurately. On the other hand, the suggested improvements for the target profile were clearly expressed, providing strong actions and measures to narrow the gap between the current and desired cybersecurity postures.

In summary, the responses were helpful but occasionally informal and imprecise. Notably, references to standards, guidelines, or technical reports were missing. For instance, in the Protect function, the model could have cited the SANS Institute's article "Auditing and Securing Multifunction Devices" [12] which provides a security measures checklist for multifunction devices (network-attached document production devices that combine two or more of these functions: copy, print, scan, and fax).

It was observed that when asking about standards and regulations relevant to a particular sector, the model's responses were accurate but sometimes outdated. Therefore, it's recommended to verify the AI model's suggestions to ensure the recommended regulations and standards are current and valid.

Furthermore, in real-world situations, disclosing the company's technical specifics to an external AI model, especially for a bank, presents significant risks. The preferred approach is to create a customized AI model, utilizing top existing models and fine-tuning them with documentation outlining the company's structure and IT systems. While this model should be kept confidential, it can serve as a valuable internal resource, providing foundational information to employees.

Nowadays, AI models face challenges in autonomously generating detailed cybersecurity reports. However, by breaking down complex problems, standards, or guidelines into smaller parts, the models can quickly generate a solid starting point for an elaborate risk assessment report.

References

[1] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*. 2015. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20151223 (visited on 04/14/2024).

[2] European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council*. of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). May 4, 2016. URL: https://data.europa.eu/eli/reg/2016/679/oj (visited on 04/14/2024).

[3] *Information security, cybersecurity and privacy protection*. International Organization for Standardization (ISO), 2022. URL: https://www.iso.org/standard/80585.html.

[4] International Telecommunication Union. *Risk management and risk profile guidelines for telecommunication organizations*. ITU-T Recommendation X.1055. 2008. URL: https://www.itu.int/rec/T-REC-X.1055 (visited on 04/14/2024).

[5] *Legislative Decree No. 231 of 8 June 2007 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica)*. 2007. URL: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2007-06-08;231 (visited on 04/14/2024).

[6] National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

[7] National Institute of Standards and Technology (NIST). *Information Security Handbook: A Guide for Managers*. Special Publication (SP) 800-100. 2006. URL: https://doi.org/10.6028/NIST.SP.800-100B (visited on 04/14/2024).

[8] National Institute of Standards and Technology (NIST). *NIST Cybersecurity Framework 2.0: Small Business Quick Start Guide*. Tech. rep. U.S. Department of Commerce, 2024. URL: https://doi.org/10.6028/NIST.SP.1300 (visited on 04/14/2024).

[9] National Institute of Standards and Technology (NIST). *Standards for Security Categorization of Federal Information and Information Systems*. Federal Information Processing Standard (FIPS) 199. 2004. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf (visited on 04/14/2024).

[10] *NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Special Publication (SP) 800-37 Rev. 2. National Institute of Standards and Technology (NIST), 2021. URL: https://doi.org/10.6028/NIST.SP.800-37r2.

[11] PCI Security Standards Council. *Payment Card Industry (PCI) Security Standards Council – Data Security Standard, Version 4.0*. Tech. rep. 2022. URL: https://www.pcisecuritystandards.org/document_library (visited on 04/14/2024).

[12] SANS Institute. "Auditing and Securing Multifunction Devices". In: (2007). URL: https://www.sans.org/white-papers/1921/ (visited on 04/14/2024).

[13] W. Stallings. *Effective Cybersecurity: Understanding and Using Standards and Best Practices*. Addison-Wesley, 2019. ISBN: 9780134772929. URL: https://books.google.it/books?id=qBLFuQEACAAJ (visited on 04/14/2024).