NIST Cybersecurity Framework (CSF) 2.0

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Revol: Financial technology company

Eshagh Shafaei

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS
May 25, 2024

Contents

1 | Introduction

Overview: Revol is a leading financial technology company dedicated to providing innovative solutions for digital banking needs. With a focus on simplifying financial transactions and enhancing user experience, Revol offers a range of digital banking services to individuals and businesses.
Mission Statement: To Revolionize the way people manage their finances by providing accessible, efficient, and secure digital banking solutions.

2 | Organization Chart

Executive Leadership:

- CEO: Oversees the overall strategic direction and operations of Revol
- CFO: Responsible for financial management, budgeting, and strategic investments.
- CTO: Leads technology development, infrastructure, and cybersecurity initiatives.
- CISO: Chief Information Security Officer responsible for overseeing the cybersecurity program.
- Chief Compliance Officer: Ensures compliance with regulatory requirements and industry standards.
- Chief Risk Officer: Manages enterprise risk management, including cybersecurity risks.

Functional Departments:

- Technology and Engineering: Develops and maintains Revol's digital banking platform, mobile applications, and backend systems.
- Operations: Manages day-to-day operations, customer support, and service delivery.
- Compliance and Legal: Ensures compliance with regulatory requirements, manages legal affairs, and oversees regulatory relationships.
- Risk Management: Identifies, assesses, and mitigates risks to Revol's business operations and assets.
- Marketing and Communications: Manages branding, marketing campaigns, and public relations initiatives.
- Finance and Accounting: Handles financial planning, accounting, and reporting functions.

Stakeholders:

- Internal Stakeholders:
- Executive Leadership Team: Sets strategic direction, allocates resources, and oversees operations.
- Employees: Contribute to Revol's success through their roles in technology development, customer support, compliance, and other functions.
- Shareholders: Have a vested interest in Revol's financial performance and long-term growth.
- External Stakeholders:
- Customers: Utilize Revol's digital banking services and rely on the platform for managing their finances.
- Regulators: Regulate and oversee Revol's operations to ensure compliance with financial regulations and consumer protection laws.
- Partners and Suppliers: Collaborate with Revol to provide services, technology solutions, and infrastructure support.

Assets:

- Digital Banking Platform:

- Core digital banking platform and mobile applications.
- Customer data, including personal and financial information.
- Intellectual property, including proprietary algorithms, software code, and technology patents.
- Brand reputation and customer trust.
- Infrastructure:
- Data centers, servers, and networking equipment supporting Revol's operations.
- Cloud computing resources and third-party service providers.
- Financial Resources:
- Capital investments, funding rounds, and financial reserves.
- Revenue streams, including subscription fees, transaction fees, and premium services.

Risks:

- Cybersecurity Risks:
- Data breaches, unauthorized access, and cyber attacks targeting customer data and financial assets.
- Malware infections, phishing attacks, and social engineering tactics aimed at compromising Revol's systems and applications.
- Compliance Risks:
- Non-compliance with financial regulations, consumer protection laws, and data privacy regulations.
- Regulatory fines, penalties, and legal liabilities resulting from compliance failures.
- Operational Risks:
- Service disruptions, system failures, and technical outages impacting customer experience and satisfaction.
- Operational errors, internal fraud, and employee misconduct affecting business operations and financial integrity.

Opportunities:

- Market Expansion:
- Expand into new geographic markets and regions to reach a broader customer base and drive growth.
- Introduce innovative financial products and services tailored to specific market segments and customer needs.
- Technology Innovation:
- Leverage emerging technologies such as artificial intelligence, machine learning, and blockchain to enhance Revol's digital banking platform and user experience.
- Develop partnerships with technology startups and fintech companies to accelerate innovation and product development.
- Regulatory Compliance:
- Invest in robust compliance programs and governance frameworks to maintain regulatory compliance and foster trust with regulators and customers.
- Proactively engage with regulators to shape regulatory policies and standards that support innovation and responsible financial services.

Organization Chart (Quick View):

1. CEO/President
2. Board of Directors
3. Chief Financial Officer (CFO)
4. Chief Operating Officer (COO)
5. Chief Information Security Officer (CISO)
6. Compliance Manager
7. Risk Management
8. Director of Information Technology (IT)
9. Director of Marketing and Sales
10. Director of Human Resources (HR)
11. Customer Service Manager
12. SOC Manager
13. Security Analysts
14. Network Security Manager
15. Cloud Security Architect
16. Incident Response Manager
17. Security Awareness Manager
18. General Counsel
19. Vendor Risk Manager

3 | Govern

Revol ensures robust cybersecurity risk management through the establishment, communication, and monitoring of cybersecurity policies and strategies.

3.0.1 | Organizational Context (GV.OC):

Revol understands the organizational context surrounding cybersecurity risk management decisions, including mission, stakeholder expectations, and legal requirements.

Ex1: Revol regularly reviews its mission statement and ensures that it aligns with the cybersecurity risk management approach, identifying potential risks that may hinder achieving its mission.

3.0.2 | Risk Management Strategy (GV.RM):

Revol establishes risk management objectives, risk tolerance, and risk appetite statements to support operational risk decisions.

Ex1: Revol updates its risk management objectives annually during strategic planning sessions, considering major changes in the operating environment.

Ex2: The company sets measurable objectives for cybersecurity risk management, such as enhancing user training quality and ensuring robust protection for critical systems.

3.0.3 | Roles, Responsibilities, and Authorities (GV.RR):

Revol establishes cybersecurity roles, responsibilities, and authorities to foster accountability and continuous improvement.

Ex1: Revol's leaders define their roles and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy.

Ex2: The company includes cybersecurity responsibilities and performance requirements in personnel descriptions and periodically measures performance for improvement.

3.0.4 | Policy (GV.PO):

Revol establishes, communicates, and enforces organizational cybersecurity policies.

Ex1: Revol creates an understandable and usable risk management policy, including statements of management intent, expectations, and direction.

Ex2: The company requires personnel to acknowledge receipt of policy when first hired, annually, and whenever policy is updated.

3.0.5 | Oversight (GV.OV):

Revol uses results from organization-wide cybersecurity risk management activities to inform and improve risk management strategies.

Ex1: Revol measures the effectiveness of risk management strategies and uses the results to inform decision-making processes and achieve organizational objectives.

Ex2: The company examines cybersecurity risk strategies that impede operations or innovation and adjusts them accordingly.

4 | Identify (ID)

Identify (ID): Revol systematically identifies and understands cybersecurity risks to manage them effectively and efficiently.

- **Asset Management (ID.AM):** Revol identifies and manages various assets, such as customer data, hardware, software, systems, facilities, services, and personnel, in alignment with organizational objectives and risk strategies.

  Example: Revol maintains a centralized asset inventory system that tracks all digital and physical assets across the organization. Automated asset discovery tools continuously update this inventory, ensuring accurate asset management.

- **Risk Assessment (ID.RA):** Revol comprehensively assesses cybersecurity risks to the organization, its assets, and individuals. This includes understanding the nature and impact of potential threats, vulnerabilities, and risks.

  Example: Revol conducts regular penetration testing and vulnerability scans to identify and assess potential security weaknesses in its systems and infrastructure. Threat intelligence feeds and analysis are also utilized to stay informed about emerging cybersecurity threats.

- **Improvement (ID.IM):** Revol continually seeks opportunities for improvement in its cybersecurity risk management processes, procedures, and activities across all Critical Security Framework (CSF) functions.

  Example: After identifying a gap in its incident response procedures during a tabletop exercise, Revol implemented a series of enhancements to streamline communication channels and response protocols, ensuring more effective incident management in the future.

This concise report outlines Revol's approach to identifying cybersecurity risks and highlights its commitment to maintaining robust risk management practices.

5 | PROTECT (PR)

Identity Management, Authentication, and Access Control (PR.AA)

- PR.AA-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
  - Current State: Basic identity management practices.
  - Target State: Comprehensive identity and access management.
  - Recommendations: Implement multi-factor authentication (MFA) and advanced IAM solutions.
  - Example: Deploying MFA for all employee logins to critical systems.
- PR.AA-3: Remote access is managed.
  - Current State: Remote access controls exist but need enhancement.
  - Target State: Secure and controlled remote access.
  - Recommendations: Implement VPNs and strict remote access policies.
  - Example: Requiring VPN access for all remote work and monitoring remote sessions.

Awareness and Training (PR.AT)
PR.AT-1: All users are informed and trained.

- Current State: Basic awareness training programs.
- Target State: Comprehensive and ongoing training.
- Recommendations: Develop a detailed training schedule covering all security policies.
- Example: Monthly phishing simulation exercises to train employees on recognizing threats.

Data Security (PR.DS)

- PR.DS-1: Data-at-rest is protected.
  - Current State: Basic protection measures.
  - Target State: Strong encryption and access controls.
  - Recommendations: Implement advanced encryption techniques.
  - Example: Encrypting all sensitive data stored on company servers.
- PR.DS-2: Data-in-transit is protected.
  - Current State: Encryption for data-in-transit.
  - Target State: Robust protection for data-in-transit.
  - Recommendations: Use advanced encryption protocols and secure data transmission channels.
  - Example: Enforcing TLS for all web-based communications.
- PR.DS-5: Protections against data leaks are implemented.
  - Current State: Basic data leak protection measures.
  - Target State: Advanced data leak prevention (DLP) solutions.
  - Recommendations: Deploy DLP solutions and regularly monitor for potential data leaks.
  - Example: Using DLP software to monitor and prevent unauthorized sharing of sensitive information.

Platform Security (PR.PS)

- PR.PS-1: Baseline configurations are established and maintained.
  - Current State: Baseline configurations are defined but need regular updates.
  - Target State: Regularly updated and enforced baseline configurations.
  - Recommendations: Establish a process for regular configuration updates and enforcement.
  - Example: Maintaining and auditing a baseline configuration for all servers.
- PR.PS-2: Security vulnerabilities are identified and managed.
  - Current State: Basic vulnerability management.
  - Target State: Comprehensive vulnerability management.
  - Recommendations: Implement regular vulnerability scanning and management practices.
  - Example: Conducting weekly vulnerability scans and applying patches promptly.

Technology Infrastructure Resilience (PR.IR)

- PR.IR-1: Redundancy and availability measures are implemented to ensure resilience.
  - Current State: Basic redundancy measures.
  - Target State: Comprehensive redundancy and high availability.
  - Recommendations: Implement advanced redundancy and failover mechanisms.
  - Example: Using a multi-region cloud setup to ensure high availability and disaster recovery.
- PR.IR-3: Recovery plans are in place and tested.
  - Current State: Recovery plans exist but need regular testing.
  - Target State: Regularly tested and updated recovery plans.
  - Recommendations: Conduct regular recovery plan tests and updates.
  - Example: Performing annual disaster recovery drills to ensure readiness.

6 | DETECT (DE)

involves continuous monitoring and analysis of cybersecurity events to identify anomalies and potential threats swiftly. By establishing baseline operations and employing advanced monitoring tools, organizations can enhance their ability to detect and respond to security incidents effectively.

Continuous Monitoring (DE.CM)
DE.CM-1: Monitor networks for events.

- Current State: Continuous monitoring tools deployed, but effectiveness can be improved.
- Target State: Advanced, real-time monitoring across all network layers.
- Recommendations: Enhance monitoring tools with behavior analytics and threat intelligence integration.
- Example: Implementing SIEM solutions coupled with intrusion detection systems (IDS) to monitor network traffic patterns, detect anomalies, and respond to threats promptly.

Adverse Event Analysis (DE.AE)
DE.AE-1: Establish baseline operations.

- Current State: Baselines established but not regularly updated.
- Target State: Dynamic baselines updated in real-time to reflect evolving network environments.
- Recommendations: Implement automated baseline generation and continuous adjustment mechanisms.
- Example: Utilizing machine learning algorithms to analyze network traffic and automatically adjust baselines based on normal behavior, thus facilitating anomaly detection.

7 | RESPOND (RS)

Addressing cybersecurity incidents effectively is crucial for maintaining the security and integrity of Revol's systems and data. The Respond phase focuses on promptly and effectively managing, analyzing, reporting, and mitigating incidents to minimize their impact on operations and customers.
Incident Management (RS.MA) RS.MA-1: Efficiently manage incidents.

- Current State: Revol efficiently manages incidents.
- Target State: Continuously improve incident management processes.
- Recommendations: Implement automated incident response workflows.
- Example: Utilizing incident response platforms to streamline incident handling and resolution.

Incident Analysis (RS.AN)
RS.AN-1: Analyze incidents to understand attack vectors and techniques.

- Current State: Incident analysis is conducted, but with limited depth.
- Target State: Conduct thorough incident analysis to understand attack techniques and improve defenses.
- Recommendations: Enhance incident analysis capabilities with threat intelligence integration.
- Example: Leveraging advanced forensic tools to dissect incidents and identify root causes effectively.

Incident Response Reporting and Communication (RS.CO)
RS.CO-1: Report incidents promptly and accurately.

- Current State: Incidents are reported but with room for improvement in accuracy and timeliness.
- Target State: Ensure prompt and accurate incident reporting to facilitate swift response.
- Recommendations: Implement incident reporting protocols and channels for streamlined communication.
- Example: Utilizing incident response platforms to automate incident reporting and communication processes.

Incident Mitigation (RS.MI)
RS.MI-1: Implement measures to mitigate incidents.

- Current State: Revol implements measures to mitigate incidents.
- Target State: Enhance incident mitigation capabilities to minimize impact.
- Recommendations: Develop and test incident response playbooks for various scenarios.
- Example: Conducting regular tabletop exercises to simulate incident response scenarios and refine mitigation strategies at Revol.

8 | RECOVER (RC)

Recover from cybersecurity incidents swiftly and effectively to minimize disruption to operations and restore normal business functions.

Incident Recovery Plan Execution (RC.RP)
RC.RP-1: Execute incident recovery plans efficiently.

- Current State: Incident recovery plans are established but may need optimization.
- Target State: Streamlined and systematic execution of incident recovery plans.

- Recommendations: Regularly test and update incident recovery plans to ensure effectiveness.
- Example: Conducting regular tabletop exercises to simulate incident recovery scenarios and refine execution strategies.

Incident Recovery Communication (RC.CO)
RC.CO-1: Communicate incident recovery progress and expectations.

- Current State: Incident recovery communication processes exist but may need improvement.
- Target State: Clear and timely communication of incident recovery status and expectations.
- Recommendations: Establish communication channels and protocols for incident recovery updates.
- Example: Providing regular updates to stakeholders through designated communication channels regarding incident recovery progress and expected timelines.

9 | Implementation Tiers

Assess Revol's current cybersecurity posture across four tiers:

- Tier 1 (Partial): Risk management practices are not formalized.
- Tier 2 (Risk Informed): Risk management practices are approved but not established organization-wide.
- Tier 3 (Repeatable): Risk management practices are formally approved and established organization-wide.
- Tier 4 (Adaptive): Risk management practices are continually improved based on lessons learned and predictive indicators.

Provide an assessment of where Revol currently stands and recommendations for improvement.

10 | 4. Profiles

Develop a current profile and a target profile for Revol:

- Current Profile: Document the current state of cybersecurity practices.
- Target Profile: Define the desired state of cybersecurity practices.

Highlight gaps and outline steps to move from the current profile to the target profile.

11 | 5. Recommendations

Provide specific, actionable recommendations to improve Revol's cybersecurity posture. Include short-term, medium-term, and long-term actions.

12 | 6. Conclusion

In conclusion, Revol's cybersecurity approach, aligned with NIST guidelines, emphasizes proactive measures such as asset management, risk mitigation, and robust identity controls. Continuous monitoring and thorough incident analysis enhance their ability to detect and respond to threats promptly. Streamlined incident management processes, coupled with clear communication channels for recovery updates, ensure efficient recovery from cybersecurity incidents. By prioritizing these strategies, Revol aims to safeguard its operations, mitigate risks effectively, and maintain the trust of its customers in an ever-evolving threat landscape.