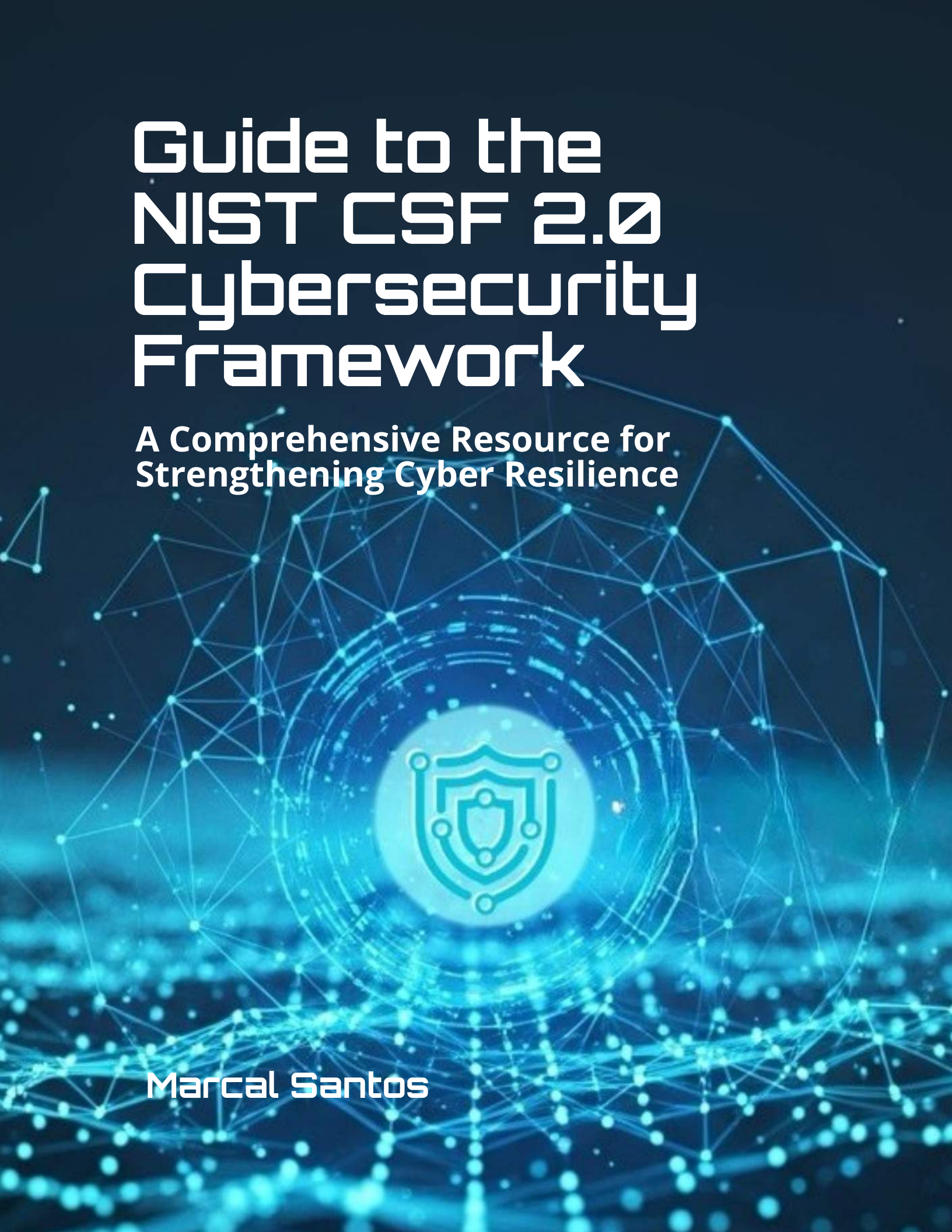
Guide to the NIST CSF 2.0 Cybersecurity Framework

A Comprehensive Resource for Strengthening Cyber Resilience



Marcal Santos

Table Of Contents

Guide to the NIST CFS 2.0 Cybersecurity Framework

A Foundational Checklist for Business Resilience

Introduction:

The NIST Cybersecurity Framework (CSF) 2.0 provides a clear, strategic path for organizations of all sizes to manage and reduce cybersecurity risk. It is not a rigid set of rules, but a flexible framework designed to align with your specific business needs.

At Trescudo, we use the NIST CSF 2.0 as the foundation for building resilient security programs. This checklist is designed to help you begin assessing your organization's posture against the six core functions of the framework. Use these high-level questions to identify strengths and uncover areas for improvement.

GOVERN (GV): Establish and Monitor Your Strategy

This function is the foundation. It ensures cybersecurity is aligned with business objectives and managed as a core enterprise risk.

- [ ] **Strategy:** Do we have a clearly defined and documented cybersecurity strategy that is understood and supported by executive leadership?
- [ ] **Roles & Responsibilities:** Are cybersecurity roles and responsibilities clearly defined across the organization, from the board level to technical staff?
- [ ] **Risk Management:** Is our cybersecurity risk management program integrated into our broader enterprise risk management (ERM) strategy?
- [ ] **Policy:** Are our cybersecurity policies established, communicated, and regularly reviewed?
- [ ] **Supply Chain:** Do we have a process for identifying and managing cybersecurity risks associated with our suppliers and third-party partners?

IDENTIFY (ID): Understand Your Assets and Risks

You cannot protect what you do not know. This function is about understanding your environment and the risks it faces.

- [ ] **Asset Management:** Do we maintain a comprehensive inventory of our physical and digital assets (devices, systems, applications, data)?
- [ ] **Vulnerability Management:** Do we have a program to continuously identify and assess vulnerabilities within our systems?
- [A] **Risk Assessment:** Do we regularly conduct risk assessments to understand the potential impact of threats to our operations?
- [ ] **Attack Surface:** Do we have a clear understanding of our internal and external attack surface?

PROTECT (PR): Implement Safeguards to Limit Impact

This function focuses on implementing proactive security controls to defend against cyber threats.

- [ ] **Access Control:** Do we enforce the principle of least privilege, ensuring users only have access to what they need to perform their jobs?
- [ ] **MFA:** Is multi-factor authentication (MFA) implemented for all critical systems, remote access, and privileged accounts?
- [ ] **Data Security:** Is our sensitive data identified, classified, and protected both at rest and in transit (e.g., via encryption, DLP)?
- [ ] **Protective Technology:** Are our networks and endpoints protected with modern security solutions (e.g., NGFW, EDR/XDR) that can block advanced threats?
- [ ] **Awareness & Training:** Are employees regularly trained on cybersecurity best practices, including phishing and social engineering recognition?

DETECT (DE): Identify Incidents in a Timely Manner

Even with strong protections, incidents can occur. This function is about timely discovery.

- [ ] **Continuous Monitoring:** Are our networks, systems, and cloud environments continuously monitored for anomalous activity and potential threats?
- [ ] **SIEM/XDR:** Do we have a centralized logging and detection platform (e.g., SIEM, XDR) to correlate events and identify indicators of compromise?
- [ ] **Detection Processes:** Do we have established processes to analyze and triage security alerts effectively?

RESPOND (RS): Take Action When an Incident Occurs

A swift, coordinated response can significantly minimize the damage of an incident.

- [ ] **Response Plan:** Do we have a formal incident response plan that is tested regularly through tabletop exercises or simulations?
- [ ] **Communication:** Does the plan include clear communication protocols for internal stakeholders, leadership, and external parties (e.g., customers, regulators)?
- [ ] **Analysis & Containment:** Do we have the capability to analyze the scope of an incident and effectively contain it to prevent further spread?

RECOVER (RC): Restore Operations and Build Resilience

This function focuses on restoring services and learning from incidents to improve future resilience.

- [ ] **Recovery Plan:** Do we have a documented plan to restore systems and data to normal operations in a timely manner?
- [ ] **Backups:** Are our critical systems and data regularly backed up, and are these backups tested to ensure they can be restored?
- [ ] **Lessons Learned:** Do we conduct a post-incident review to identify the root cause and implement improvements to our security posture?

Your Next Step: From Checklist to Strategy

This checklist is the first step. A truly resilient cybersecurity posture requires a deep understanding of your unique environment, a tailored strategy, and expert implementation.

At **Trescudo**, we specialize in guiding businesses in the Benelux region through this entire process. We help you move from questions to answers, building a robust security program that protects your business and builds confidence.

Ready to turn this checklist into an actionable strategy?

Contact Trescudo today for a no-obligation consultation with our cybersecurity experts.

TRESCUDO

The Trescudo Guide

The Trescudo Guide to the NIST Cybersecurity Framework 2.0 offers a practical checklist designed to help organizations assess and enhance their cybersecurity posture across the framework's six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. By providing targeted questions and strategies, this guide empowers businesses to align their cybersecurity efforts with their specific needs, ensuring resilience against evolving threats. Transform your approach to cybersecurity with Trescudo's expert insights and tailored strategies that build confidence and robust protection for your organization.

TRESCUDO