CybelAngel

Recommendations for implementing NIST CSF 2.0

ICT risk management

- [ ] Follow an ICT cybersecurity risk management framework.
- [ ] Conduct a comprehensive risk assessment to identify vulnerabilities in ICT systems.
- [ ] Map critical ICT assets and their dependencies to business functions.
- [ ] Assign clear roles and responsibilities for managing ICT risks.

Third-Party risk management

- [ ] Vet all third-party ICT service providers to ensure they meet standards before entering contracts.
- [ ] Update contracts to include detailed provisions on data security, storage locations, and incident response protocols.
- [ ] Develop robust exit strategies to mitigate risks when terminating contracts with non-compliant providers.
- [ ] Conduct regular audits and require third-party providers to participate in cyber resilience training programs, while leveraging CybelAngel's capabilities to continuously assess and monitor your key vendors. This ensures ongoing compliance, strengthening cyber defenses, and reducing risk through actionable intelligence and rapid exposure detection.

Incident reporting

- [ ] Set up standardized templates for incident response and communication with relevant internal and external stakeholders.
- [ ] Notify clients promptly about incidents and outline mitigation measures.
- [ ] Perform root-cause analyses for all incidents to prevent recurrence.

Resilience testing

- [ ] Schedule regular penetration testing, red teaming, and risk-based security assessments to simulate real-world cyberattacks in line with NIST guidance.
- [ ] Use the results of these tests to refine operational resilience strategies.

Businesses without an existing cybersecurity strategy can start with templates and information provided by NIST, such as the Small Business Quick Start Guide, which makes suggestions for each of the core functions.

To protect critical infrastructure as cyber threats continue to evolve, organizations must take an adaptive approach to their cybersecurity posture. NIST CSF 2.0 represents a vital advancement in cybersecurity practices with a proactive approach to managing risks and ensuring compliance.