ISD FENIQS

Cybersecurity Readiness Assessment

Results Report

Organization: acme GmbH
Email: max.mustermann@acme.com
Date: April 22, 2026

Overall Score

39 / 51 (76%)

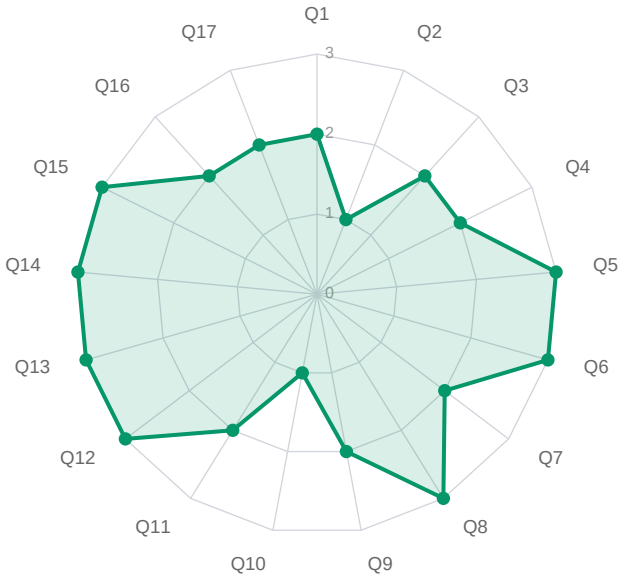
Good Posture – Keep Maturing

You’re on the right track — your security maturity is ahead of many peers.

You’ve clearly invested in core security measures and risk management practices. That said, cybersecurity is never "done": new threats, tools, and compliance requirements evolve constantly.

Now is the time to look at advanced services like threat hunting, zero-trust architecture, and continuous cloud security.

Results Overview



About This Assessment

The ISD FENIQS Cybersecurity Readiness Assessment evaluates an organization's security posture across 17 key domains, aligned with industry-leading frameworks including the NIST Cybersecurity Framework (CSF) 2.0, CIS Controls, ISO 27001, and the EU NIS2 Directive. Each question maps to one or more of the six NIST CSF core functions: Govern, Identify, Protect, Detect, Respond, and Recover.

For each question, participants select the response that best describes their current state. Each response corresponds to a maturity level from 0 (no capability) to 3 (advanced, proactive capability). The assessment produces a total score out of a maximum of 51 points, categorizing the organization into one of three risk tiers.

The following pages contain the assessment content for each answered question. For the selected response level, three sections are provided: an **Assessment** explaining the current state and its implications, a **Risk Implications** analysis detailing specific threats and exposures, and a **Recommendation** providing actionable next steps for improvement.

Score Range	Risk Tier	Description
0 – 20	High Risk – Immediate Action Required	Significant gaps exposing the organization to serious threats. Foundational protections may be missing.
21 – 36	Medium Risk – Room for Improvement	Decent foundation with key areas requiring attention. Missing deeper visibility, automation, or proactive detection.
37 – 51	Good Posture – Keep Maturing	Strong security maturity ahead of many peers. Focus on advanced services, threat hunting, and continuous improvement.

SECTION 1 — GOVERNANCE

Cybersecurity Policy & Awareness Training

NIST CSF: Govern (GV.AT), Protect (PR.AT)

Do you have a cybersecurity policy and regular awareness training for employees?

Score: 2

Policy + annual training

Assessment

Your organization has established both a formal cybersecurity policy and annual training. This places you above the majority of organizations in terms of security awareness maturity. Annual training provides a structured foundation, and the combination with a policy demonstrates organizational commitment to cybersecurity governance. However, once-a-year training alone may not be sufficient to address the rapidly evolving threat landscape, as employees tend to forget training content within weeks.

Risk Implications

Annual training provides baseline coverage but creates gaps between sessions where emerging threats (e.g., new phishing techniques, deepfake-enabled social engineering, AI-generated attacks) are not addressed. Employees may develop a compliance-oriented mindset, completing training as a checkbox exercise rather than genuinely improving their security awareness. The forgetting curve means that after 30 days, most people retain only a fraction of what they learned in a training session.

Recommendation

Evolve your program toward more frequent touchpoints: quarterly refresher sessions, monthly security tips, and continuous phishing simulations. Implement gamification elements to increase engagement. Tailor training content to role-specific risks (e.g., finance teams face different threats than IT staff). Track metrics like phishing simulation click rates, training completion rates, and incident reports to measure effectiveness and justify further investment.

SECTION 2 — GOVERNANCE

Multi-Factor Authentication (MFA)

NIST CSF: Protect (PR.AA)

Do you have Multi-Factor Authentication (MFA) enabled across critical systems?

Score: 1 **Partial (admin accounts only)**

Assessment

MFA is enabled for administrative accounts, which protects the most privileged access paths. This is a reasonable starting point, as compromised admin credentials can cause the most widespread damage. However, limiting MFA to administrators leaves the majority of your user base and their associated data unprotected. Attackers frequently target regular user accounts as an entry point, then escalate privileges laterally through the network.

Risk Implications

While admin accounts are protected, regular user accounts remain vulnerable to credential-based attacks. A compromised user account can serve as an initial foothold for lateral movement, data exfiltration, or ransomware deployment. Business email compromise (BEC) attacks, which cause billions in losses annually, specifically target non-admin email accounts. Additionally, inconsistent MFA coverage creates confusion and resistance to adoption when you eventually expand the rollout.

Recommendation

Develop a phased rollout plan to extend MFA to all employees, starting with users who handle sensitive data (finance, HR, legal) and external-facing roles. Prioritize coverage of email accounts, cloud applications, and VPN connections. Use Conditional Access policies (e.g., in Microsoft Entra ID) to enforce MFA based on risk signals such as unfamiliar locations or devices. Communicate the rollout clearly to employees and provide support to minimize friction.

SECTION 3 — GOVERNANCE

Security Controls Review & Architecture

NIST CSF: Govern (GV.RM), Identify (ID.IM)

Do you regularly review and update your cybersecurity controls and architecture?

Score: 2 **Annual or reactive reviews**

Assessment

Your organization conducts annual reviews of cybersecurity controls, supplemented by reactive reviews when issues arise. This demonstrates a structured approach to security governance and provides regular checkpoints for identifying and addressing gaps. Annual reviews are aligned with common compliance requirements and provide a consistent cadence for security improvement.

Risk Implications

Annual reviews, while structured, may not keep pace with the speed of threat evolution. A full year between reviews creates windows where new vulnerabilities, configuration changes, or infrastructure modifications may go unexamined. Additionally, annual reviews can become formulaic over time, focusing on the same areas without adapting to changing risk profiles or emerging attack vectors.

Recommendation

Increase review frequency to semi-annual or quarterly for high-risk areas (e.g., cloud configurations, identity and access management, internet-facing systems). Implement continuous monitoring for critical controls where possible, and use the annual review as a comprehensive strategic assessment rather than the sole review mechanism. Integrate threat intelligence into your review process to ensure reviews address current, relevant risks.

SECTION 4 — VULNERABILITY MANAGEMENT

Endpoint Protection (AV, EDR, XDR)

NIST CSF: Protect (PR.DS), Detect (DE.CM)

Do you have endpoint protection in place (AV, EDR, XDR)?

Score: 2 **Basic EDR or AV with cloud console**

Assessment

You have deployed a basic EDR solution or cloud-managed antivirus, providing improved visibility and detection capabilities over traditional AV. Cloud-based management enables centralized monitoring, policy enforcement, and remote remediation. This is a meaningful step forward in endpoint security maturity, offering behavioral detection and better telemetry compared to signature-only approaches.

Risk Implications

Basic EDR or cloud-managed AV provides detection capabilities but may lack the depth of correlation, automated response, and threat hunting that advanced EDR/XDR platforms offer. Without a Security Operations Center (SOC) or dedicated security team monitoring alerts, detections may go uninvestigated or unresolved. Alert fatigue can become an issue if the volume of alerts exceeds the team's capacity to triage effectively. Coverage gaps may also exist for non-standard endpoints (e.g., Linux servers, IoT devices).

Recommendation

Evaluate upgrading to an advanced EDR/XDR platform with centralized management and consider augmenting with a managed detection and response (MDR) service if internal SOC resources are limited. Ensure that alerts are actively monitored and triaged, and that detection rules are tuned to reduce false positives. Extend coverage to all endpoint types in your environment and integrate endpoint telemetry with your broader security monitoring infrastructure.

SECTION 5 — VULNERABILITY MANAGEMENT

Vulnerability Scanning

NIST CSF: Identify (ID.RA), Protect (PR.PS)

How often do you scan for vulnerabilities in your environment?

Score: 3 **Continuous scanning and remediation process**

Assessment

Your organization has implemented continuous vulnerability scanning paired with a structured remediation process. This represents a mature vulnerability management program that provides near-real-time visibility into your attack surface and enables rapid response to newly disclosed vulnerabilities. Continuous scanning ensures that no significant window exists between vulnerability emergence and detection.

Risk Implications

Continuous scanning generates large volumes of data that must be effectively triaged and prioritized. Without robust risk-based prioritization and clear remediation workflows, the volume of findings can overwhelm teams and lead to important vulnerabilities being lost in the noise. Scanning tools also have limitations: they may not detect all vulnerability types, especially in custom applications or complex configurations.

Recommendation

Maintain your continuous scanning program and focus on optimizing the remediation workflow. Leverage risk-based prioritization that considers asset criticality, exploit availability, and threat intelligence. Integrate vulnerability management with your broader security operations for coordinated response. Regularly review and validate that remediation actions are effective and that vulnerabilities are truly resolved.

SECTION 6 — VULNERABILITY MANAGEMENT

Asset Discovery & Integration

NIST CSF: Identify (ID.AM)

Is asset discovery automated and integrated with your scanning tools?

Score: 3 **Fully automated**

Assessment

Asset discovery is fully automated and integrated with your scanning and security tools. This ensures that your security team has a continuously updated, accurate picture of all assets in the environment. New devices and systems are automatically discovered, inventoried, and enrolled in security coverage. This level of automation is essential for maintaining security in dynamic, cloud-enabled environments.

Risk Implications

Fully automated discovery must be regularly validated to ensure accuracy and completeness. Automated tools may have blind spots in certain network architectures, encrypted environments, or non-standard device types. The quality of your security posture depends not just on discovering assets but on ensuring that each discovered asset is properly classified, owned, and protected.

Recommendation

Maintain your automated discovery and focus on enriching asset data with business context: criticality classification, data sensitivity, ownership, and compliance requirements. Use this enriched asset inventory as the foundation for risk-based security decisions. Regularly validate discovery coverage through manual spot checks and penetration testing that specifically targets asset visibility.

SECTION 7 — VULNERABILITY MANAGEMENT

Compliance & Configuration Checks

NIST CSF: Protect (PR.PS), Identify (ID.GV)

Do you perform compliance and configuration checks (e.g., CIS benchmarks)?

Score: 2 **Regularly, using scripts/tools**

Assessment

Regular configuration checks are performed using scripts or tools, providing consistent, repeatable assessments against defined baselines. This structured approach enables tracking of configuration compliance over time and supports systematic remediation of deviations.

Risk Implications

Script-based and tool-assisted checks are effective but may cover only a subset of your environment or configuration parameters. Custom scripts require ongoing maintenance to stay current with new benchmarks and system changes. Without centralized reporting, it can be difficult to aggregate compliance status across the environment and communicate it to stakeholders.

Recommendation

Consider upgrading to enterprise-grade configuration management and compliance tools that provide comprehensive coverage, centralized reporting, and automated remediation. Integrate configuration checks with your change management process to validate that changes do not introduce security deviations. Extend coverage to cloud configurations, which are increasingly a source of breaches.

SECTION 8 — DETECTION & RESPONSE

Log Collection & Storage

NIST CSF: Detect (DE.AE), Identify (ID.AM)

Do you collect and store logs from your critical infrastructure (servers, network, endpoints)?

Score: 3 **Centralized log collection (e.g., SIEM) with retention policy**

Assessment

Centralized log collection through a SIEM or equivalent platform is in place, with a defined retention policy. This is a best-practice approach that provides comprehensive visibility, efficient search and analysis capabilities, and compliance-ready documentation. Centralized logging is the foundation upon which effective threat detection, incident response, and security analytics are built.

Risk Implications

SIEM deployments require ongoing tuning, maintenance, and expertise to remain effective. Un-tuned SIEMs can generate excessive noise, leading to alert fatigue and missed detections. Log ingestion costs can escalate as data volumes grow. Ensure that your retention policy meets both regulatory requirements and operational needs for incident investigation.

Recommendation

Focus on optimizing your SIEM deployment: tune detection rules to reduce false positives, implement use cases aligned with your threat model, and ensure analysts have the training to effectively investigate alerts. Consider integrating threat intelligence feeds to enrich log data. Regularly review and test your ability to search and retrieve historical log data for incident investigation purposes.

SECTION 9 — DETECTION & RESPONSE

Threat Detection & Alerting

NIST CSF: Detect (DE.CM, DE.AE)

Do you have active threat detection and alerting in place?

Score: 2 **Alerts on some key events only**

Assessment

Alerting is configured for some key events, providing automated detection of specific high-priority security incidents. This is a meaningful improvement over manual review, as it enables faster response to known threat patterns and reduces reliance on human log analysis for common scenarios.

Risk Implications

Limited alerting coverage means that sophisticated attacks, which may not trigger the specific rules in place, can still go undetected. Attackers who understand common detection rules can deliberately avoid triggering them. Without comprehensive coverage and correlation across multiple data sources, attacks that span multiple systems or stages may be missed. Alerts without a defined response process may also go uninvestigated.

Recommendation

Expand your detection coverage by adding alerting rules aligned with common attack frameworks (e.g., MITRE ATT&CK). Implement correlation rules that combine signals from multiple sources to detect complex attack patterns. Define and document response procedures for each alert type. Consider adopting a managed SOC service for comprehensive monitoring or invest in building internal detection engineering capabilities.

SECTION 10 — OT SECURITY

Operational Technology (OT) Security

NIST CSF: Identify (ID.AM), Detect (DE.CM)

Do you have Operational Technology (OT) or industrial control systems in your environment?

Score: 1 **Occasional scanning / limited visibility**

Assessment

Some scanning or visibility into OT security exists, but it is limited and inconsistent. Occasional scanning provides snapshots but cannot keep pace with the evolving threat landscape targeting industrial systems.

Risk Implications

Limited visibility means that changes in the OT environment, including unauthorized devices, configuration changes, or anomalous communication patterns, may go undetected. The gap between scans creates windows where threats can establish and persist. OT environments change slowly, but when they are compromised, the impact can be severe and immediate.

Recommendation

Increase the frequency and coverage of OT scanning. Deploy passive monitoring tools that can observe OT network traffic without impacting operational systems. Implement network segmentation and access controls between IT and OT zones. Develop OT-specific incident response procedures and ensure IT security staff understand the unique constraints of OT environments.

SECTION 11 — CLOUD SECURITY

Cloud Security Posture

NIST CSF: Protect (PR.DS, PR.PS)

Do you use public cloud platforms (e.g., Azure, AWS, GCP)?

Score: 2 **Basic tooling in place**

Assessment

Basic cloud security tooling is deployed, providing some level of automated visibility and protection for your cloud environment. This may include native security services, basic monitoring, or third-party tools that provide configuration assessment.

Risk Implications

Basic tooling may cover common misconfigurations but may lack the depth to detect complex attack patterns, runtime threats, or sophisticated data exfiltration attempts. Without centralized monitoring and alerting, security findings from cloud tools may not receive timely attention.

Recommendation

Enhance your cloud security tooling with a comprehensive CSPM solution and integrate it with your centralized security monitoring (SIEM/SOC). Implement cloud workload protection for runtime security. Establish cloud-specific incident response procedures and ensure your security team has cloud security training and certifications.

SECTION 12 — CLOUD SECURITY

Cloud Monitoring & Protection

NIST CSF: Detect (DE.CM), Protect (PR.DS)

Is your cloud monitored and protected (e.g. Defender, Sentinel, CSPM tools)?

Score: 3 **Managed detection and protection (e.g., Defender + SOC)**

Assessment

Cloud security is actively managed with both detection and protection tools, integrated with SOC monitoring. This comprehensive approach provides continuous, expert-driven security coverage for your cloud environment, combining automated detection with human analysis and response.

Risk Implications

Even with managed cloud security, the shared responsibility model requires ongoing attention to your own configurations, identities, and data. Ensure that managed service providers have appropriate access and visibility, and that their detection coverage is regularly reviewed and validated against your specific cloud architecture and threat model.

Recommendation

Continue your mature approach and focus on advanced cloud security capabilities: threat hunting in cloud environments, detection and response for container and serverless workloads, and integration of cloud security with your broader Zero Trust architecture. Regularly test your cloud security through red team exercises that specifically target cloud misconfigurations and weaknesses.

SECTION 13 — NETWORK & ACCESS

Remote & Branch Office Access Security

NIST CSF: Protect (PR.AA, PR.DS)

How do you secure remote and branch office access?

Score: 3

Full ZTNA and security stack with features like IPS, DNS filtering, RBI, MDR

Assessment

A comprehensive Zero Trust Network Access solution is deployed with advanced security features including Intrusion Prevention (IPS), DNS filtering, Remote Browser Isolation (RBI), and Managed Detection and Response (MDR). This represents a mature, defense-in-depth approach to securing remote and branch office access that operates on the principle of never trust, always verify.

Risk Implications

Complex security stacks require careful management, monitoring, and maintenance. Ensure that all components are actively managed, policies are regularly reviewed, and the user experience remains acceptable. Overly restrictive policies can drive users to find workarounds that undermine security.

Recommendation

Maintain your comprehensive posture and focus on continuous improvement: refine ZTNA policies based on usage patterns and risk signals, implement continuous device compliance monitoring, and integrate access telemetry with your SIEM for threat detection. Regularly assess the user experience to ensure security controls do not create unacceptable friction.

SECTION 14 — COMPLIANCE

Regulatory Compliance (ISO 27001, NIS2)

NIST CSF: Govern (GV.OC, GV.RM)

Are you required to comply with ISO27001, NIS2, or other regulatory frameworks?

Score: 3 **Fully compliant, reviewed regularly**

Assessment

Full compliance has been achieved and is regularly reviewed and maintained. This represents the highest level of compliance maturity, demonstrating not just adherence to regulatory requirements but ongoing commitment to maintaining and improving security governance. Regular reviews ensure that compliance keeps pace with regulatory updates and evolving threats.

Risk Implications

Compliance maturity can lead to complacency if the focus shifts from security outcomes to audit readiness. Ensure that compliance activities are aligned with actual risk reduction, not just documentation. Regulatory requirements may change (e.g., NIS2 amendments proposed in January 2026), requiring updates to your compliance program.

Recommendation

Maintain your strong compliance posture and use it as a foundation for broader security maturity. Stay engaged with regulatory developments and industry groups to anticipate changes. Share your compliance experience through industry communities and consider using your compliance maturity as a competitive differentiator in client and partner relationships.

SECTION 15 — TESTING & RESILIENCE

Risk Assessment & Treatment Planning

NIST CSF: Govern (GV.RM), Identify (ID.RA)

Do you have a process for risk assessment and treatment planning?

Score: 3 **Ongoing risk management framework in place**

Assessment

An ongoing, structured risk management framework is in place, providing continuous assessment, treatment, and monitoring of cybersecurity risks. This mature approach ensures that risk management is not a periodic event but an integral part of organizational decision-making and operations.

Risk Implications

Even mature risk management frameworks require regular validation and refinement. Ensure that risk assessments are grounded in reality by incorporating threat intelligence, incident data, and vulnerability findings. Risk appetite and tolerance should be periodically re-evaluated by leadership as the business and threat landscape evolve.

Recommendation

Continue to strengthen your risk management framework by integrating quantitative risk analysis alongside qualitative methods. Use risk data to drive strategic security investments and communicate risk in business terms to executive leadership and the board. Share risk insights across the organization to build a risk-aware culture.

SECTION 16 — TESTING & RESILIENCE

Security Testing

NIST CSF: Identify (ID.RA), Detect (DE.AE)

Do you test your security controls (e.g., penetration tests, red/blue teaming)?

Score: 2 **Biannually or per major change**

Assessment

Security testing occurs biannually or is triggered by major changes, providing more frequent validation than annual testing alone. Testing after major changes ensures that new systems, configurations, or architectures are validated before or shortly after deployment.

Risk Implications

While more frequent, biannual testing still leaves gaps where changes between tests may introduce undetected vulnerabilities. Change-triggered testing requires disciplined change management processes to ensure that all security-relevant changes are flagged for testing. There is a risk that smaller changes accumulate without triggering a test.

Recommendation

Consider adopting continuous security testing and validation practices. Implement automated attack simulation tools that test specific controls on a regular basis. Incorporate security testing into your CI/CD pipeline for application changes. Evolve toward a purple team approach where offensive and defensive teams collaborate continuously.

SECTION 17 — TESTING & RESILIENCE

Incident Response Plan

NIST CSF: Respond (RS.MA, RS.AN), Recover (RC.RP)

Do you have an incident response plan?

Score: 2 **Formal plan tested annually**

Assessment

A formal, approved incident response plan is in place and tested annually through tabletop exercises or simulations. This demonstrates organizational commitment to incident preparedness and ensures that the plan is validated, team members are familiar with their roles, and gaps are identified before a real incident occurs.

Risk Implications

Annual testing may not be sufficient to maintain readiness, particularly in organizations with high staff turnover or rapidly changing infrastructure. The time between tests may allow skills to atrophy and new team members to be unfamiliar with the plan. If the plan is not updated between tests to reflect organizational changes, it may become outdated.

Recommendation

Increase testing frequency to at least semi-annual, with different scenarios for each exercise. Supplement formal exercises with informal drills and awareness activities. Ensure the plan is updated after every significant organizational change, technology change, or real incident. Include post-incident reviews as a formal part of the plan to capture and incorporate lessons learned.

Next Steps

76%

39 / 51 points

Good Posture – Keep Maturing

Discuss Your Results with Our Experts

Our cybersecurity specialists can help you translate the findings of this assessment into a concrete action plan. Visit isdfeniqs.com or contact us at contact@isdfeniqs.com.

Disclaimer: This assessment provides a general evaluation based on the responses given and does not constitute a formal security audit or certification. For a comprehensive security analysis, we recommend professional consultation.