NETZ INFORMATIONS SYSTEME

NIS AG
Buchenstrasse 8
CH-6210 Sursee
Tel. +41 41 267 05 05
info@nis.ch
www.nis.ch

Whitepaper

IKT-Minimalstandard Audit 2025

Professionelles Hosting des Netzinformationssystems – sicher, performant und umfassend betreut.

Ziel und Einordnung

Als Anbieterin von Fullservice Angeboten für Kunden mit erhöhten Anforderungen an Informationssicherheit, Verfügbarkeit und Resilienz lässt die NIS AG ihre Sicherheitsorganisation und Angebote regelmässig durch unabhängige externe Stellen überprüfen.

Im Jahr 2025 wurde ein externes Audit gemäss dem **IKT-Minimalstandard des Bundes**[1] durchgeführt. Ziel dieses Audits war es, den aktuellen Reifegrad der organisatorischen und technischen Sicherheitsmassnahmen transparent zu bewerten, Stärken und Verbesserungspotenziale aufzuzeigen und eine belastbare Grundlage für die Weiterentwicklung des Informationssicherheits-Managementsystems (ISMS) zu schaffen.

Was ist der IKT-Minimalstandard?

Der IKT-Minimalstandard ist ein vom Bund definierter Referenzrahmen zur Erhöhung der Cyber-Resilienz von Organisationen, insbesondere im Umfeld kritischer Infrastrukturen und deren Lieferketten. Er orientiert sich konzeptionell am **NIST Cybersecurity Framework**[2] und gliedert die insgesamt 108 Sicherheitskontrollen entlang der fünf Funktionen:

Dabei wird für jede Sicherheitskontrolle ein Maturity Rating vergeben, das von 0 (nicht umgesetzt) bis 4 (dynamisch umgesetzt, kontinuierlich überprüft und verbessert) reicht. Pro Funktion und insgesamt ergibt sich anschliessend ein durchschnittliches Maturity Rating.

Der Standard adressiert dabei nicht nur technische Kontrollen, sondern explizit auch Governance, Prozesse, Rollen, Übungen und organisatorische Massnahmen. Er eignet sich daher besonders zur Beurteilung der operativen Sicherheitsreife von SaaS- und Cloud-Anbietern.

Umfang und Methodik des Audits

Das Audit wurde durch die **Swiss Infosec AG**[3] als unabhängige, spezialisierte Sicherheitsberatung durchgeführt.

Bewertet wurden sämtliche organisatorischen und technischen Massnahmen und Prozesse der NIS AG, sowie der operative Betrieb der SaaS Angebote in den Cloud-Umgebungen.

Als Referenzrahmen dienten der IKT-Minimalstandard (Version Mai 2023), das NIST Cybersecurity Framework (v1.1) sowie der **ISO/IEC 27001:2022 Standard**[4] (Annex A, Mapping).

Die Bewertung erfolgte anhand von Dokumentenanalysen, Interviews mit Schlüsselrollen sowie stichprobenartigen Nachweisen. Ziel war eine realistische Einordnung des tatsächlichen Umsetzungsgrads, nicht eine formale Zertifizierung.

---

[1] BACS, Bundesamt für Cybersicherheit, *„Empfehlungen IKT-Minimalstandards“* 29 07 2025. [Online]. Available: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html. [Zugriff am 09 02 2026].

[2] NIST, National Institute of Standards and Technology, *„Cybersecurity Framework“* [Online]. Available: https://www.nist.gov/cyberframework. [Zugriff am 09 02 2026].

[3] Swiss Infosec AG, *„SWISS INFOSEC“* [Online]. Available: https://www.infosec.ch/. [Zugriff am 09 02 2026].

[4] ISO, *„ISO/IEC 27001:2022“* 10 2022. [Online]. Available: https://www.iso.org/standard/27001.

Zusammenfassung der Ergebnisse

Das Audit bestätigt insgesamt ein **sehr solides Sicherheitsniveau** der NIS AG.

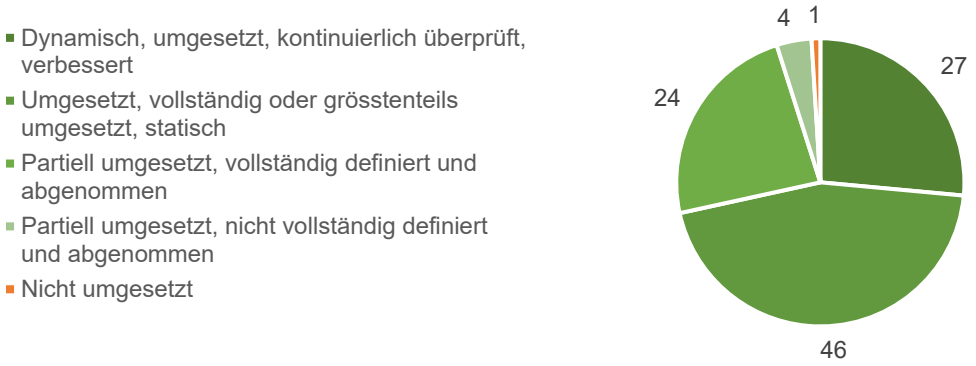

Abbildung 1: Anzahl Sicherheitskontrollen pro Maturity Rating

Der über alle Funktionen aggregierte Reifegrad beträgt **3.1** auf der Bewertungsskala von 0 bis 4 und wird von den Auditoren als **sehr gut** eingestuft.

Besonders starke Ausprägungen zeigen sich unter anderem in:

- der sicheren Ausgestaltung des Cloud-Betriebs in AWS
- Netzwerk- und Perimeterschutz (WAF, DDoS-Mitigation)
- Transportverschlüsselung (TLS v1.3)
- Rollen- und Berechtigungskonzepten
- Backup- und Wiederherstellungsmechanismen inklusive Off-Region Redundanz

Diese Ergebnisse bestätigen, dass zentrale Schutz-, Reaktions- und Wiederherstellungsmechanismen wirksam implementiert sind.

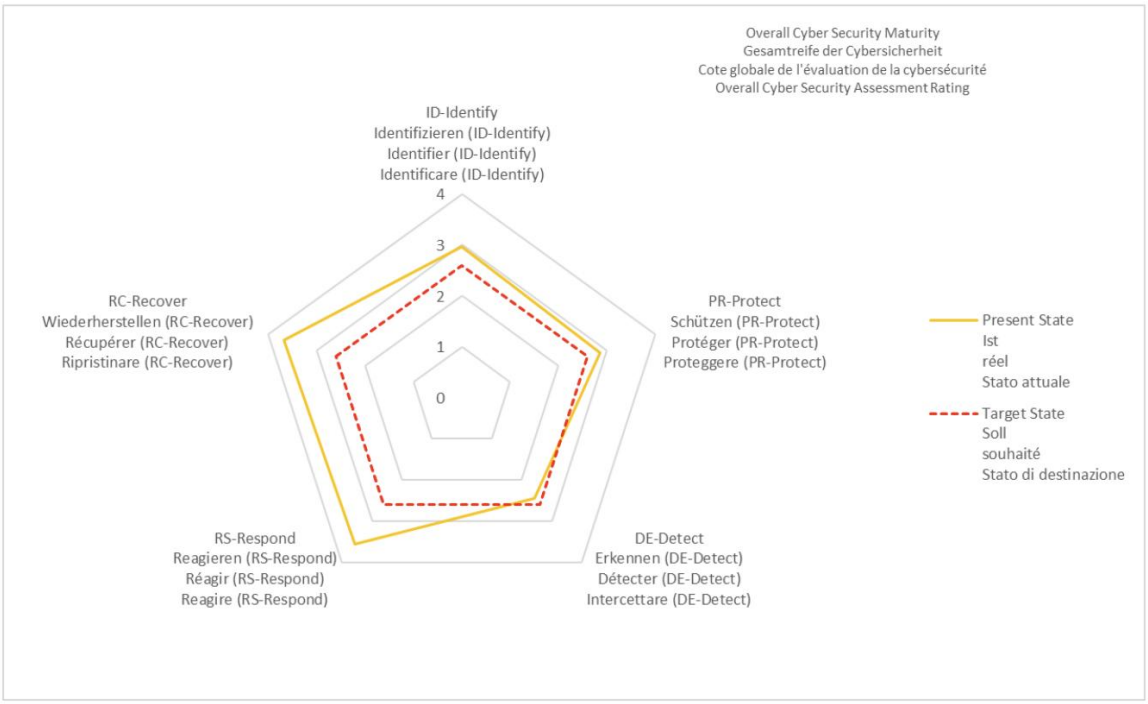

Abbildung 2: Übersicht der Maturity Ratings aller Funktionen

Bedeutung für Kunden und Lieferkette

Für die Kunden der NIS AG im Umfeld kritischer Infrastrukturen ist Informationssicherheit ein zentraler Bestandteil der Lieferketten-Verantwortung. Das durchgeführte Audit zeigt, dass die NIS AG diese Verantwortung ernst nimmt und ihre Sicherheitsorganisation regelmässig extern überprüfen lässt.

Das Audit unterstützt Kunden insbesondere bei der Bewertung von Lieferantenrisiken, regulatorischen Nachweisen, der Einschätzung von Betriebs- und Ausfallrisiken, sowie von Due-Diligence-Prüfungen im Rahmen von Beschaffungsprozessen.

Transparenz und weitere Informationen

Dieses Whitepaper stellt eine bewusst verdichtete Darstellung der Audit Ergebnisse dar. Detailberichte, Bewertungsmatrizen und weiterführende Nachweise können auf Anfrage und unter NDA zur Verfügung gestellt werden.

Kontakt

NIS AG

Buchenstrasse 8

CH-6210 Sursee

Tel. 041 267 05 05

info@nis.ch · www.nis.ch

Literaturverzeichnis

[1] BACS, Bundesamt für Cybersicherheit, *„Empfehlungen IKT-Minimalstandards“* 29 07 2025. [Online]. Available: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html. [Zugriff am 09 02 2026].

[2] NIST, National Institute of Standards and Technology, *„Cybersecurity Framework“* [Online]. Available: https://www.nist.gov/cyberframework. [Zugriff am 09 02 2026].

[3] Swiss Infosec AG, *„SWISS INFOSEC“* [Online]. Available: https://www.infosec.ch/. [Zugriff am 09 02 2026].

[4] ISO, *„ISO/IEC 27001:2022“* 10 2022. [Online]. Available: https://www.iso.org/standard/27001.