



ICT-Audits. *Sicherheit, Datenschutz, Compliance & Funktionalitäten.*

ICT-Revision mit ganzheitlichem Ansatz.

Klarheit und Transparenz gewinnen, wo Ihr Unternehmen steht.

Das ICT-Audit liefert wertvolle Fakten in den Bereichen Cyber-Sicherheit, Cyber-Abwehr und Datenschutz. Darüber hinaus liefert das Audit faktenbasierte Erkenntnisse über Schwachstellen in Ihren Systemen, konzeptionelle und strategische Risiken sowie die Bewertung von Notfallszenarien. Mögliches Einsparungspotential aufgrund eines überdimensionierten ICT-Environments, ohne Sicherheits- und Datenschutzrisikoverlust, kann ebenfalls ermittelt werden.

Sicherheit

- Sicherheits- & Risiko-Assessment
- Prüfen von Schwachstellen & Verwundbarkeiten
- Einstufen von Cyber-Bedrohungen
- Bewerten von Cyber-Defense-Konfigurationen
- Auswerten von Assets & Eintrittswahrscheinlichkeiten

Datenschutz

- Verifizieren der Backupkonzepte/-systeme & Wiederherstellungsabläufe
- Bewertung Zugriffsschutz & Datensicherheit
- Überprüfung Datenschutz & technisch-organisatorische Massnahmen

Compliance

- Bewertung Compliance, Richtlinien & Reglemente
- Überprüfung Dokumentationen
- Kontrolle Disaster Recovery & Incident-Response-Fähigkeiten

ICT

- Erstellung IST-Situationsanalyse ICT-Environment
- Prüfen ICT-Strategie/-Konzeption, Arbeitsweise & Funktionalität
- Prüfung Business Continuity & Lifecycle-Management
- Prüfung Schulungskonzept & Awareness der Mitarbeitenden



«Gewissheit und Klarheit erhalten, von unabhängiger Stelle, verhilft allen Entscheidungsgremien dabei, richtige Massnahmen zu treffen und die Aufsichtspflichten und Führungsverantwortung wahrzunehmen.»

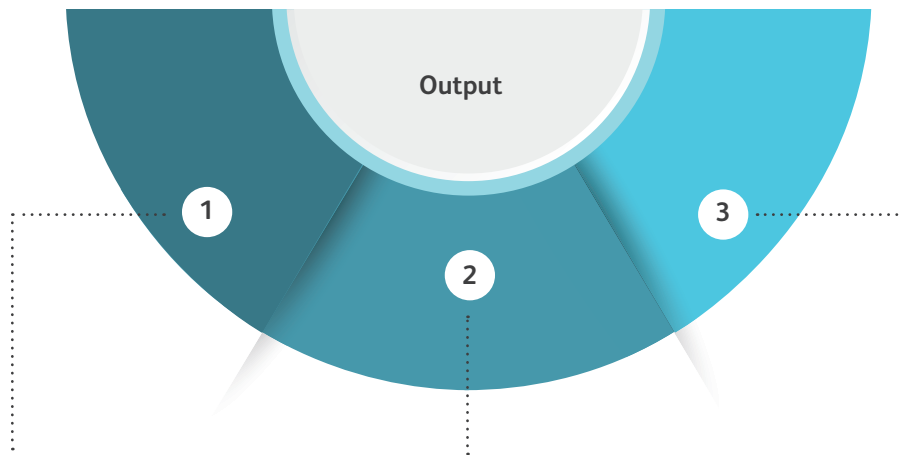
Jörg Strebel

CSO / Mitglied der Geschäftsleitung



Output.

Fakten, Ablauf & Wissenswertes.



Audit & Analyse

Durchführung, Überprüfung & Begutachtung

- Infrastruktur-, Netzwerk-, Client- & Cloudanalyse
- Veraltete Komponenten, nicht aktualisierte Systeme
- Fehlkonfigurationen von Diensten, Betriebssystemen & Virtualisierungen
- Standard-Programme, Hardware-Komponenten und Firmware
- Schwachstellen, Eintrittswahrscheinlichkeiten & Schadenspotential
- Sicherheitssysteme, Netzwerksegmentierung, SOC & Monitoring
- Firewalllösung, SSL-Inspection, Webfilter, Mailsecurity, Verschlüsselung
- Profilkonfigurationen, Endpoint-protection, Zugriffsschutz
- Klassifizierung, Authentifizierungsvorgaben, Passwort-Policy
- Backup, Retention Policy, Überwachung & Wiederherstellung
- Dokumentationen, Datenschutz & Lizenzkonformität
- ICT-Organisation & RACI (Responsible, Accountable, Consulted & Informed)

Bewerten & Dokumentieren

Verifizieren, Auswerten & Beurteilen

- Zusammenführen Auditdaten
- Verifizierung Erkenntnisse
- Beurteilung Fakten
- Bewerten Risiken & Assets
- Erstellung Risiko-Cockpit
- Definition Handlungsfelder
- Beschreibungen Kausalitäten
- Berichterstellung
- Management-Zusammenfassung
- Qualitätskontrollen

Präsentieren & Informieren

Erläutern, Aufzeigen & Aufklären

- Outputs & Erkenntnisse
- Kritikalitäts- & Risikostufen
- Befunde & Handlungsempfehlungen
- Risikominimierung
- Interventionsmassnahmen
- Massnahmenkatalog
- Generelle Optimierungen
- Optimierungsmassnahmen
- Strategische ICT-Empfehlungen
- Ganzheitliche ICT-Konzeption



Unsere ICT-Audits.

Klarheit, Sicherheit, Orientierung.

ICT-Audit Elite –
ganzheitliche Sicherheit
mit Compliance-Fokus

Elite bietet eine ganzheitliche Analyse der gesamten ICT-Landschaft.

Infrastruktur, Sicherheit, Prozesse und Dokumentation werden im Zusammenspiel betrachtet, um Risiken und Schwachstellen transparent aufzuzeigen. Ein Schwerpunkt liegt auf der technischen Unterstützung von Compliance-Anforderungen, insbesondere im Kontext des revDSG. Die Variante richtet sich an Organisationen mit hohen Anforderungen an Sicherheit, Verfügbarkeit und Governance.

ICT-Audit Advanced –
Strukturierte Sicherheit
und Transparenz

Advanced verbindet technische Sicherheit mit organisatorischer Reife.

Neben der Infrastruktur werden Sicherheitsarchitektur, Berechtigungen und Lifecycle-Themen bewertet. Der Fokus liegt auf dem Schutz kritischer Systeme, der Widerstandsfähigkeit gegen Ausfälle und Angriffe sowie auf konsistenten Sicherheitsmassnahmen. Advanced schafft Transparenz über Risiken und unterstützt die gezielte Weiterentwicklung der ICT.

ICT-Audit Essentials –
der kompakte Überblick

Essentials bietet eine pragmatische Gesamtsicht auf die grundlegende Sicherheit und Stabilität der ICT-Umgebung.

Im Fokus stehen technische Basis, zentrale Sicherheitsmechanismen sowie die Absicherung von Infrastruktur, Zugriffen, Netzwerken und Datensicherung. Ziel ist es, Schwachstellen frühzeitig zu erkennen und eine verlässliche Grundlage für weitere ICT-Entscheidungen zu schaffen. Essentials eignet sich ideal als Einstieg oder zur periodischen Standortbestimmung.

ICT-Audit – Leistungsumfang & Abstufungen

Bereich	Essentials	Advanced	Elite
ICT-Umgebung (Räumlichkeiten, USV, Basis-Infrastruktur)	✓	✓	✓
Security (Grundsicherheit & Sicherheitsarchitektur)	✓	✓	✓
Zugriffsschutz & Berechtigungen	✓	✓	✓
Serverinfrastruktur & Virtualisierung	Δ	✓	✓
Microsoft 365-Umgebung	Δ	✓	✓
Datensicherung & Wiederherstellung	✓	✓	✓
Compliance (Datenschutz, Disaster Recovery, Reglemente)	X	X	✓
Individuelle Risikobeurteilung pro Feststellung	X	✓	✓
Kundenspezifische Massnahmeempfehlungen	X	✓	✓
Schwachstellenscan	○	○	✓
Phishing-Kampagne (2–3 Mails)	○	○	✓

✓ enthalten | Δ wahlweise | X nicht enthalten | ○ optional

ICT-Lösungen am Puls der Zeit.

Hauptsitz/Postadresse

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

Standort Luzern
Schnydermatt 1
6210 Sursee

+41 43 233 30 30
hello@neo-one.ch
www.neo-one.ch