



Sicherheit. Steuerbar. Prüfbar.

- ✓ Security Consulting
- ✓ Regulatorische Anforderungen
- ✓ Awareness Schulungen
- ✓ CISO-as-a-Service
- ✓ Cyber Security Check

UNSERE LEISTUNGEN PASSGENAU FÜR IHRE RISIKEN



Wir helfen, Risiken transparent zu machen, wirksame Schutzmassnahmen zu etablieren, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, koordiniert auf Vorfälle zu reagieren und den Geschäftsbetrieb nach Störungen schnell und kontrolliert wiederherzustellen.

UNSERE LEISTUNGEN IN DER ÜBERSICHT

Einhaltung FINMA-Vorgaben

Übersetzung von regulatorischen Anforderungen in klare Prozesse, Rollen und Kontrollen sowie strukturierte Vorbereitung auf Vor-Ort-Kontrollen.

Informationssicherheitsstrategie

Entwicklung und Umsetzung einer auf Ihr Geschäftsmodell passenden Sicherheitsroadmap.

Governance, Risk & Compliance

Aufbau klarer Verantwortlichkeiten, Richtlinien und Kontrollen zur wirksamen Steuerung von Cyber- und IKT-Risiken

Sicherheitsarchitektur & -design

Konzeption und Weiterentwicklung sicherer IT- und Applikationsarchitekturen entlang bewährter Sicherheitsprinzipien.

Menschzentrierte Sicherheit

Sensibilisierung, Schulung und Einbindung der Mitarbeitenden, damit Sicherheit im Alltag gelebt wird.

Cybersicherheitsbewertungen

Strukturierte Assessments zur Beurteilung des Reifegrads, Identifikation von Schwachstellen und Priorisierung von Massnahmen.

GOVERNANCE & STRATEGIE

Governance, Risk & Compliance

Eine wirksame Steuerung von Informationssicherheit beginnt bei einer klaren Governance-Struktur. Governance, Risk & Compliance stellt sicher, dass Verantwortlichkeiten, Entscheidungswege und Richtlinien verbindlich festgelegt sind und Informationssicherheit als Managementaufgabe verstanden wird. Durch klare Rollen, Gremien und Berichtswege erhalten Geschäftsleitung und Verwaltungsrat die Transparenz, die sie für fundierte Entscheidungen zu Cyber- und IKT-Risiken benötigen.

GoodIT unterstützt beim Aufbau und der Weiterentwicklung dieser Strukturen: von der Definition von Richtlinien und Standards über Risiko- und Kontrollprozesse bis hin zu Reporting, KPIs und der Einbindung interner Revision. So entsteht ein konsistenter Rahmen, der regulatorische Vorgaben ebenso berücksichtigt wie das individuelle Risikoprofil und die strategischen Ziele Ihres Unternehmens.



Informationssicherheitsstrategie

Eine Informationssicherheitsstrategie verbindet Geschäftszwecke, Risiken und Massnahmen zu einem kohärenten Zielbild. Sie definiert, welches Sicherheitsniveau angestrebt wird, wie es erreicht werden soll und welche Prioritäten gesetzt werden.

Gemeinsam mit Ihnen entwickelt GoodIT eine auf Ihr Geschäftsmodell passende Sicherheitsroadmap, die sowohl kurz- als auch mittelfristige Massnahmen umfasst. Dazu gehören unter anderem Zielbilder für Organisation, Prozesse und Technologie, abgestimmte Programme und Projekte sowie Kriterien für die Erfolgskontrolle der umgesetzten Massnahmen.

SICHERHEITSARCHITEKTUR & -DESIGN

Governance, Risk & Compliance

Sicherheitsarchitektur & -design sorgen dafür, dass Sicherheit nicht nachträglich „aufgesetzt“, sondern von Anfang an in Systeme und Prozesse integriert wird. Eine gute Architektur schafft klare Zonen, definierte Schnittstellen und nachvollziehbare Schutzmechanismen, die den Geschäftsbetrieb unterstützen statt behindern.

GoodIT begleitet Sie bei der Konzeption und Weiterentwicklung sicherer IT- und Applikationsarchitekturen. Von Netzwerk- und Cloud-Architekturen über Identitäts- und Zugriffsmanagement bis hin zu Logging, Monitoring und Resilienz. Dabei werden bewährte Sicherheitsprinzipien wie Least Privilege, Defense in Depth und Segregation of Duties konsequent berücksichtigt.



Menschzentrierte Sicherheit

Menschen sind als Stärke wie auch als mögliche Schwachstelle ein zentraler Faktor jeder Sicherheitsstrategie. Menschzentrierte Sicherheit zielt darauf ab, Mitarbeitende zu befähigen, Risiken zu erkennen, verantwortungsvoll zu handeln und Sicherheitsvorgaben im Alltag pragmatisch umzusetzen.

GoodIT entwickelt zielgruppenorientierte Awareness- und Schulungskonzepte, die Fachbereiche, Management und technische Teams jeweils dort abholen, wo sie stehen. Ergänzend werden Prozesse und Werkzeuge so gestaltet, dass sich sichere Verhaltensweisen möglichst intuitiv in den Arbeitsalltag integrieren lassen und damit dauerhaft verankert werden.

STANDORTBESTIMMUNG

Einhaltung FINMA-Vorgaben

Die Einhaltung aufsichtsrechtlicher Anforderungen ist für Finanzinstitute und weitere regulierte Unternehmen geschäftskritisch. Vorgaben zur Beherrschung von IKT- und Cyberrisiken dienen nicht nur der formalen Compliance, sondern sichern Stabilität, Reputation und Vertrauenswürdigkeit gegenüber Kunden, Partnern und Aufsicht.

GoodIT übersetzt die relevanten FINMA-Vorgaben in klare Prozesse, Rollen und Kontrollen und unterstützt beim Aufbau der dafür notwendigen Dokumentation und Nachweise. Dazu gehört auch die strukturierte Vorbereitung auf Vor-Ort-Kontrollen. Von der Identifikation prüfungsrelevanter Unterlagen über die Organisation von Interviews bis hin zu Management-Briefings oder der Begleitung während der Prüfung.



Cybersicherheitsbewertungen

Cybersicherheitsbewertungen liefern eine objektive Grundlage für Entscheidungen, anstatt sich auf Bauchgefühl oder Einzelereignisse zu stützen. Sie zeigen auf, wo Organisation, Prozesse und Technik bereits gut aufgestellt sind und wo kritische Lücken oder ineffiziente Doppelstrukturen bestehen.

GoodIT führt strukturierte Assessments durch – etwa Reifegradanalysen, Risiko- und Kontrollenbewertungen oder Architektur-Reviews. Die Ergebnisse werden in verständlicher Form aufbereitet und in konkrete, priorisierte Maßnahmen überführt, sodass Führung und Fachbereiche wissen, wo sie mit welchem Nutzen ansetzen sollen.

Dein Security Partner in Nidwalden

Cyber- und Informationssicherheit ist längst kein optionales Extra mehr, sondern ein zentraler Bestandteil moderner Unternehmensführung. Sie beeinflusst direkt die Geschäftskontinuität, die Einhaltung gesetzlicher Vorgaben und das Vertrauen von Kunden, Partnern und Mitarbeitenden. Angesichts der steigenden Bedrohungslage durch Ransomware, gezielte Phishing-Kampagnen oder gezielten Angriffe auf Lieferketten kann es sich kein Unternehmen mehr leisten, Sicherheit nur punktuell zu betrachten.

Für regulierte Finanzinstitute kommt hinzu, dass Cyber- und IKT-Risiken explizit als Teil der operationellen Risiken und der operativen Resilienz adressiert werden müssen und damit zentrale Prüf- und Aufsichtsthemen der FINMA sind. Vorgaben zu Cyberrisiken, zum Schutz kritischer Daten, zu Meldepflichten bei schwerwiegenden Vorfällen sowie zu Governance, Risiko-Management und internen Kontrollen machen Informationssicherheit zu einem wesentlichen Bestandteil der regulatorischen Compliance.

GoodIT unterstützt Unternehmen als verlässlicher Security Partner dabei, diese Herausforderungen strukturiert und effizient zu meistern. Im Fokus steht ein ganzheitlicher Ansatz, der organisatorische und technische Aspekte der Informationssicherheit miteinander verbindet und sich an anerkannten Standards und regulatorischen Anforderungen, wie etwa den FINMA-Rundschreiben zu operationellen Risiken und Cyberrisiken, orientiert. Dazu gehört unter anderem die systematische Identifikation und Bewertung von Risiken, die Definition geeigneter Schutzmassnahmen sowie die Etablierung klarer Verantwortlichkeiten und Prozesse.



GoodIT
Allmendstrasse 22
6373 Ennetbürgen
www.goodit.ch
info@goodit.ch

