Vorstellung
CSP Cyber Security made easy

Passion für
Transformation

Agenda

1. Vorstellungsrunde
2. Kurzvorstellung CSP
3. Dienstleistungen Cyber- und Informationssicherheit
4. Wieso Cybersecurity mit CSP?
5. Einige konkrete Themen, Leistungen und Services (ja nach Interesse)

IHRE ANSPRECHPARTNER



Peter Flütsch

Expert Security Consultant / Partner
Dipl. Ing. FH / EMBA IT-Management
CISSP / CISM / ISO 27001 Lead Auditor
peter.fluetsch@csp-ag.ch
+41 71 508 09 72

IHRE ANSPRECHPARTNER



Martin Kalberer

Partner

martin.kalberer@csp-ag.ch

+41 44 520 33 61

IHRE ANSPRECHPARTNER



Jens Albrecht

Senior Security Consultant
Dipl. El.-Ing. FH / NDS Wirtschaftsing. FH
CISSP / CISM / CRISC
jens.albrecht@csp-ag.ch
+41 44 520 33 68

IHRE ANSPRECHPARTNER



Stephan Riesen

Senior Security Consultant
CAS Information Security-Technology HSLU
CISSP / CISM / HERMES 2022 Advanced
stephan.riesen@csp-ag.ch
+41 31 512 86 07

IHRE ANSPRECHPARTNER



Reto Fausch

Projektleiter / Berater
BSc Wirtschaftsinformatik
IPMA Level D / CPRE IREB
reto.fausch@csp-ag.ch
+41 71 231 10 83

Agenda

1. Vorstellungsrunde
2. Kurzvorstellung CSP
3. Dienstleistungen Cyber- und Informationssicherheit
4. Wieso Cybersecurity mit CSP?
5. Einige konkrete Themen, Leistungen und Services (ja nach Interesse)

WIR SIND





Dienstleistungsportfolio (Auszug)

Strategie

Eignerstrategie

Unternehmens- oder Bereichs-strategie

Entwicklung Leitbild

ICT-/Digitalisierungsstrategie

Sourcing-Strategie

Informationssicherheits-Strategie / ISMS

Aufbau strategisches Projektportfoliomanagement

Organisation

Führungscoaching

Ad interim Mandate CISO as a Service

Organisationsentwicklung

Prozessanalyse

Beschaffungsunterstützung

Programm-/Projektleitung

Qualitäts- und Risiko-management in Projekten

IT-Notfallorganisation

Technologie

Anforderungsmanagement

IT-Infrastruktur (Beratung/PL)

Microsoft 365 (Beratung/PL)

Informationssicherheit- und Datenschutz-Konzepte

Ransomware-Notfallplan

Erfolgreiche Transformation

UNABHÄNGIG

Ein kompetenter Ansprechpartner
Unabhängige Beratung
Auf Sie massgeschneiderte Lösung

KOMMUNIKATIONSSTARK

Starke Ziele, vereinte Kräfte
Überwinden von internen Grenzen
Aufzeigen innovativer Lösungsansätze

KOMPETENZ AUF ZEIT

Spezialwissen – dann wenn Sie es brauchen
Keine Überkapazitäten nach Projektabschluss
Wissenstransfer zu Ihren Mitarbeitenden

BRANCHENKENNER

Verständliche Sprache
Beste Marktübersicht und -beziehungen
Sofort produktive Leistungen

PROFESSIONELL

Termintreue
Budgeteinhaltung
Klare und übersichtliche Resultate

VERTRAUENSVOLL

Stimmige «Chemie» im Team
Entlastung von herausfordernden Arbeiten
Keine schlaflosen Nächte

Agenda

1. Vorstellungsrunde
2. Kurzvorstellung CSP
3. Dienstleistungen Cyber- und Informationssicherheit
4. Wieso Cybersecurity mit CSP?
5. Einige konkrete Themen, Leistungen und Services (ja nach Interesse)

Beratung Cyber- & Informationssicherheit



CISO / DPO ad interim



Leitung von Security-Projekten



Expertise in Security-Fokusthemen



BERATUNG CYBER- & INFORMATIONSSICHERHEIT

- Standortbestimmungen und Roadmaps (z.B. basierend auf ISO 27001 oder IKT-Minimalstandard)
- Informationssicherheits-Strategie
- Aufbau eines Informationssicherheits-Managementsystems (ISMS)
- Planung und Durchführung von Awareness-Kampagnen
- Erstellung von ISDS-Konzepten und Risikoanalysen
- Datenschutz-Vorabkonsultationen
- Erstellung von Weisungen, Policies und Richtlinien
- Vorbereitung ISO 27001 Zertifizierung



CISO / DPO ad interim

- Unterstützung oder Durchführung von sämtlichen CISO- / DPO-Arbeiten
- CISO / DPO auf Zeit / ad interim
- Etablierung der CISO- / DPO-Rolle
- Coaching



LEITUNG VON SECURITY-PROJEKTEN

Fachliche Unterstützung bei Sicherheitsvorhaben.
Referenzen:

- Einführung einer Lösung für digitale Signaturen
- Begleitung Einführung M365 in Bezug auf Compliance und Security
- Projektleitung bei IT-Infrastrukturprojekten mit Bezug zur Informationssicherheit
- Sichere Konfiguration Windows-Arbeitsplatz
- IT-Beschaffungen im Bereich Security
- Begleitung Aufbau eines Security Operation Center



EXPERTISE IN SECURITY-FOKUSTHEMEN

- Business Continuity Management (BCM),
  z.B. basierend auf BSI 200-4
- IT-Notfallplanung,
  z.B. basierend auf ISO 27031
- Datenschutz bei der Einführung von Cloud-Lösungen
- Laufende Erweiterung aktueller Themen



Agenda

1. Vorstellungsrunde
2. Kurzvorstellung CSP
3. Dienstleistungen Cyber- und Informationssicherheit
4. Wieso Cybersecurity mit CSP?
5. Einige konkrete Themen, Leistungen und Services (ja nach Interesse)

Wieso Cyber Security mit CSP?



- Consultants mit langjähriger Praxiserfahrung in Kundenorganisationen, u.a. als CISO, DPO
- Hervorragende Branchenkenntnisse
- Kombination mit der CSP-Expertise aus den Bereichen Strategie, Organisation, Kultur, Prozesse und Technologie
- Garantiert unabhängig von Produkten oder Herstellern
- Umsetzungsstark

Innovation, Transparenz, Kompetenz



Wir haben uns vom externen Dienstleister Compass Security im Rahmen einer «Attack Simulation» hacken lassen und das Ergebnis veröffentlicht.

Die Hacker waren erfolgreich und wir konnten uns verbessern.

https://www.cspcybersecurity.ch

Kunden und Testimonials

- Gemeinde Uznach
- Kanton Basel-Landschaft, Bildungs- Kultur- und Sportdirektion
- Kanton Basel-Landschaft, Finanz- und Kirchendirektion
- Kanton Basel-Landschaft, Sicherheitsdirektion
- Kanton Basel-Landschaft, Zentrale Informatik
- Kanton Graubünden, Amt für Informatik
- Kanton Graubünden, Personalamt
- Kanton St. Gallen, Gesundheitsdepartement
- Kanton St. Gallen, Migrationsamt
- Kanton St. Gallen, Staatsanwaltschaft
- Kanton Thurgau, Steuerverwaltung
- Kantonspolizei St. Gallen
- MEDISYN SA, Luzern
- MIBA Genossenschaft, Aesch
- Schweizerisches Epilepsie-Zentrum
- Schweizer Zucker AG
- SFS Services AG
- Somedia AG
- TISG – Trägerverein Integrationsprojekte St. Gallen

„Die fachliche, methodische und effiziente Unterstützung zur Erstellung von zahlreichen ISDS-Konzepten hat uns begeistert."



Roman Rüegg
Chief Information Security Officer / CISO, Kanton Graubünden

„Die unkomplizierte und pragmatische Unterstützung der CSP zu unterschiedlichen Themen im Bereich Cyber-Sicherheit hat uns überzeugt."



Damiano Tuena
Leiter IT Engineering und SIBE Cybersecurity, Somedia Services

„Die kompetente Beratung und Unterstützung im Bereich Cyber-Sicherheit ist für uns wertvoll. Wir schätzen die pragmatische und lösungsorientierte Zusammenarbeit sehr.»"



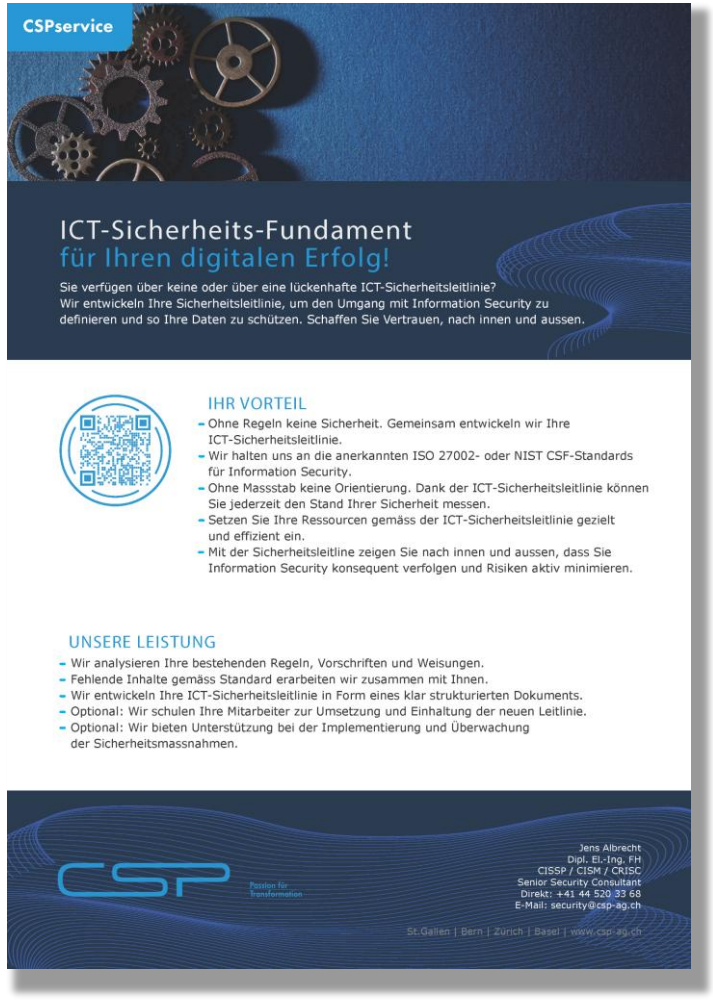
Claudia Nef
Geschäftsführerin TISG
Trägerverein Integrationsprojekte St.Gallen TISG

Agenda

1. Vorstellungsrunde
2. Kurzvorstellung CSP
3. Dienstleistungen Cyber- und Informationssicherheit
4. Wieso Cybersecurity mit CSP?
5. Einige konkrete Themen, Leistungen und Services (ja nach Interesse)

Einige konkrete Themen und Leistungen 1

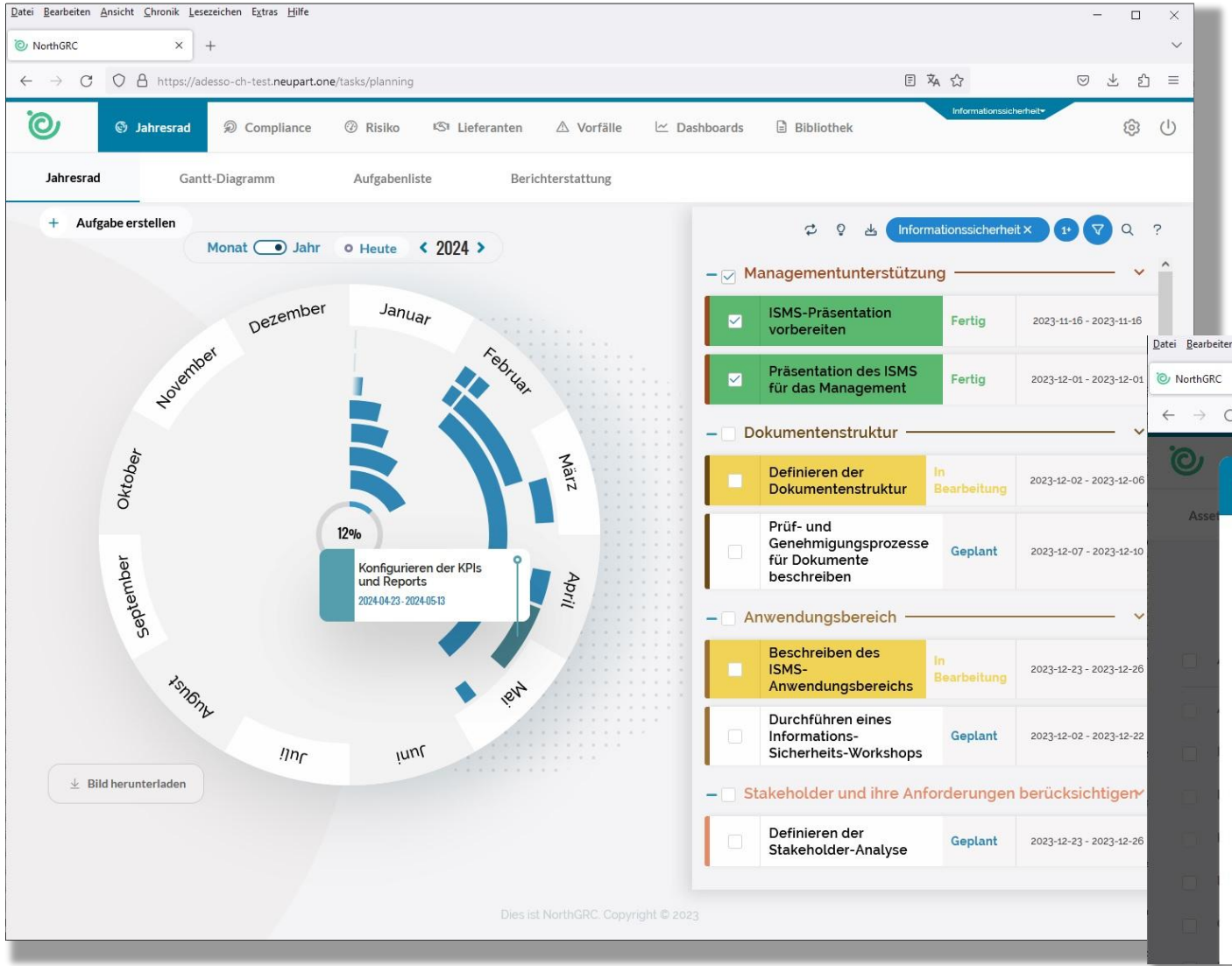


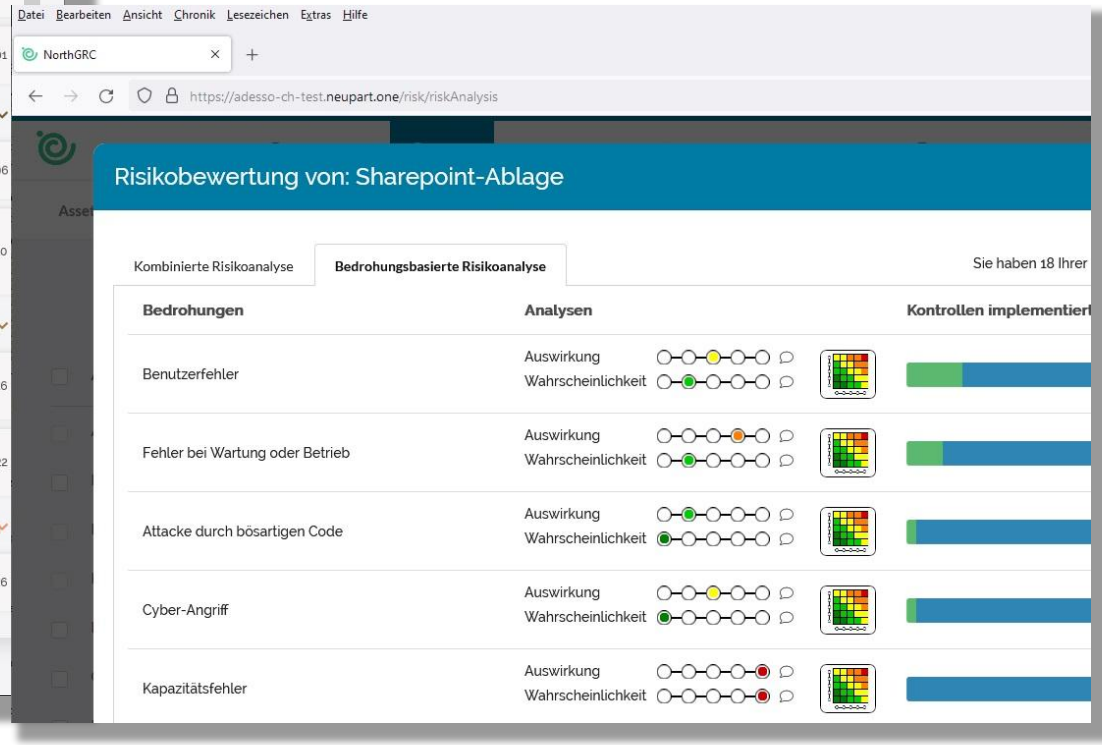


Einige konkrete Themen und Leistungen 2

Beratung rund um ISMS:

- Evaluation
- Implementation
- Konfiguration
- Betrieb
- Schulung





360 Grad Standortbestimmung Cyber-Sicherheit

Zur Gewährleistung der Cyber-Sicherheit in einem Unternehmen sind zahlreiche Aspekte (Technik, Organisation, Weisungen, Prozesse, Mitarbeitende, Lieferanten) mit zahlreichen Anspruchsgruppen (CISO, GL, Mitarbeitende, Fachabteilungen, Lieferanten, Behörden) abzustimmen. Wie steht es um ihre Cyber-Sicherheit? Wie hoch ist der Maturitätslevel ihres Unternehmens in den einzelnen Bereichen?

Kundennutzen

- Neutrale Standortbestimmung
- Berücksichtigung sämtlicher Aspekte und unterschiedlicher Sichten der wichtigsten Anspruchsgruppen (360 Grad)
- Vergleich mit anderen Unternehmen/Behörden soweit möglich
- Konkrete Vorschläge und Massnahmen zum weiteren Vorgehen

Unsere Leistung

- Umfassende Standortbestimmung nach z.B. ISO 27001/27002 oder einem branchenspezifischen Standard des BWL
- Berücksichtigung der Perspektive aller Anspruchsgruppen
- Reporting der Maturität sämtlicher Bereiche
- Ausarbeitung von konkreten Massnahmen und einer Roadmap

Maturität der Cyber-Sicherheit in allen Aspekten bestimmt, Roadmap für Verbesserungen bekannt

Aufbau oder Weiterentwicklung ISMS

Ein Informationssicherheits-Managementsystem (ISMS) bildet die Grundlage für die Gewährleistung der Informationssicherheit in einem Unternehmen. Ein ISMS muss nicht nach dem ISO-Standard 27001 aufgebaut sein sondern kann auch mit wenigen Elementen und Prozessen einen hohen Nutzen bieten. Was gehört dazu? Welche Elemente sind wichtig? Braucht es ein Tool dazu? Wie setzt man die Prozesse in der Praxis um?

Kundennutzen

- Das Thema Informationssicherheit ist systematisch und nachhaltig im Unternehmen verankert
- Sämtliche Anspruchsgruppen (GL, Mitarbeitende, IT-Abteilung, Fachabteilungen) sind nach Bedarf einbezogen
- Jahrelange Erfahrung unserer ehemaligen CISOs: Effiziente Prozesse und Vorgehensweise

Unsere Leistung

- Aufbau eines ISMS gemäss den Anforderungen des Kunden (nach/angelehnt an ISO 27001 oder auch einfache/pragmatische Variante)
- Einbezug sämtlicher Stakeholder
- Erstellung von Dokumenten, Policies und Prozessen nach Bedarf
- Umsetzung in die Praxis, Integration in bestehende (IT-)Landschaft

Angemessenes ISMS in Ihrem Unternehmen

CISO / DPO as a Service

Das Know-How und die Ressourcen für ein CISO (Chief Information Security Officer, IT-Sicherheitsbeauftragter) sind nicht in jedem Unternehmen intern vorhanden. Gute Mitarbeitende in diesem Bereich sind schwierig zu finden. Benötigen Sie CISO- / DPO-Ressourcen nach Bedarf?

Kundennutzen

- Ressourcen für IT-Sicherheitsbeauftragter / CISO / DPO flexibel nach Bedarf (Überbrückung, Teilzeit-Mandat, punktuelle Unterstützung)
- Langjährige Praxiserfahrung und Expertise von unseren Consultants (ehemalige CISO)
- Neutrale, externe Sicht
- Kommunikation auf allen Stufen (Management, Technik, externe Stellen)

Unsere Leistung

- Pensum je nach Kundenbedarf
- Unterstützung in sämtlichen Aufgabenbereichen eines CISO / DPO
- Übernahme von operativen Aufgaben im Tagesgeschäft
- Erarbeitung von Grundlagen-Policies, Durchführung einer Standortbestimmung und Erstellung einer Roadmap falls gewünscht

CISO- / DPO-Ressourcen nach Bedarf: Überbrückung, Teilzeit, Unterstützung

Strategie und Massnahmen Security-Awareness

Die Security-Awareness der Mitarbeitenden und des Managements ist ein wichtiges Thema, in der Praxis jedoch nicht ganz einfach umzusetzen. Massnahmen wie Weisungen zum sicheren Umgang oder ein E-Learning für neue Mitarbeitende sind relativ schnell umgesetzt, regelmässige Phishing-Checks ebenfalls. Was kommt danach? Wer ist die Zielgruppe? Was sind die Botschaften? Wie oft werden welche Massnahmen umgesetzt?

Kundennutzen

- Reduzierte Anzahl von IT-Sicherheitsvorfällen aufgrund besserer Awareness der Mitarbeitenden
- Besseres Verständnis für das Thema Cybersicherheit, beispielsweise für die Zielgruppe «Management»
- Gezielte Awareness für ausgesuchte Zielgruppen wie zum Beispiel IT-Mitarbeitende

Unsere Leistung

- IST-Analyse der Awareness soweit möglich und notwendig
- Definition der Zielgruppen, Botschaften, Ziele und Massnahmen (Awareness-Strategie)
- Evaluation Tool-Unterstützung
- Operative Umsetzung von Awareness-Massnahmen
- Evaluation der Zielerreichung

Angemessene Security-Awareness sämtlicher Zielgruppen

Sicher in die Cloud (ISDS-Konzepte)

Bei der Migration von Daten oder Fachanwendungen in die Cloud (z.B. M365, SaaS) ist die Gewährleistung des Datenschutzes und der Datensicherheit oft eine Herausforderung. Compliance-Anforderungen sind schwierig zu verstehen/umzusetzen. Je nachdem muss eine Vorabkonsultation bei Datenschutz-Aufsichtsbehörden durchgeführt werden. Bringen Sie das notwendige Know-How dazu selbst mit?

Kundennutzen

- Risiken, Massnahmen und Restrisiken bei der Migration in die Cloud sind bekannt
- Compliance-Anforderungen sind geprüft
- Transparenter Umgang mit Risiken gegenüber allen Stakeholdern
- Konkrete Schutzmassnahmen können umgesetzt werden
- Aufsichtsbehörden sind nach Bedarf miteinbezogen

Unsere Leistung

- Erstellung Schutzbedarfsanalyse, ISDS-Konzept, Risikoanalyse, DSFA und Berechtigungskonzept
- Einbringen von Fach-Expertise zu Datenschutz und Datensicherheit
- Einbezug sämtlicher Stakeholder (IT-Abteilung, Management, DSB, CISO, Fachabteilung)
- Vorabkonsultation bei Datenschutz-Aufsichtsbehörden nach Bedarf

Sicherer Cloud-Einsatz, erfüllte Compliance-Anforderungen

BCM, IT-Notfallplanung, Ransomware-Readyness

Externe Bedrohungen (z.B. Pandemie, Strommangellage, Ransomware, gehackte Lieferanten) haben in den letzten Jahren zugenommen. Kann Ihr Unternehmen/Ihre Behörde angemessen auf einen Notfall oder eine Krise reagieren? Ist die Geschäftsfortführung beim Ausfall der IT oder der Stromversorgung weiterhin möglich?
Sind Geschäftsfortführungspläne oder IT-Notfallpläne vorhanden?

Kundennutzen

- Resilienz der wichtigsten Geschäftsprozesse oder der IT gegenüber externen Bedrohungen
- Schneller Wiederanlauf bei einem Notfall oder einer Krise
- Ausgearbeitete Pläne für eine schnelle und effiziente Reaktion auf ausgesuchte Bedrohungen
- Geübte und verifizierte Notfallprozesse, z.B. im Rahmen einer Tabletop Exercise

Unsere Leistung

- Erstellung BCM basierend auf Standards wie BSI 200-4 oder ISO 22301 mit einer Business-Impact-Analyse (BIA) und Geschäftsfortführungsplänen
- Erarbeitung Strategie, Organisation, Prozesse in den Bereichen BCM oder IT-Notfallplanung
- Erstellung von IT-Notfallplänen, z.B. basierend auf ISO 27031
- Erstellung von spezifischen Plänen (z.B. Ransomware-Readyness)

Erhöhte Resilienz in Notfällen und Krisen

Vorbereitung ISO 27001 Zertifizierung

Je nach Dienstleistungsangebot verlangen Kunden vermehrt eine ISO 27001 Zertifizierung als Nachweis für ein funktionierendes ISMS. Wollen oder müssen Sie Ihr Unternehmen ISO 27001 zertifizieren? Steht eine Rezertifizierung an? Benötigen sie einen neutralen Auditor für ein internes Audit?

Kundennutzen

- Effizient zur ISO 27001 Zertifizierung
- Aufbau eines ISMS nach ISO 27001 mit hohem Praxisbezug durch ehemalige CISO
- Neutrale Auditoren für interne Audits

Unsere Leistung

- Zertifizierte ISO 27001 Lead Auditoren für die Vorbereitung einer formellen Zertifizierung und den Aufbau eines ISMS nach ISO 27001
- Anpassungen und Unterstützung bei einer Rezertifizierung, z.B. beim Wechsel von ISO 27001:2013 auf ISO 27001:2022
- Auditoren für interne Audits gemäss ISO 27001
- Standortbestimmungen basierend auf ISO 27001

Zertifizierungsunterstützung ISO 27001 nach Bedarf

WIR SIND

DANKBAR

SG | ZH | BE | BS

csp-ag.ch

Diese Arbeit © 2024 der CSP AG ist lizenziert unter CC BY-NC-ND 4.0