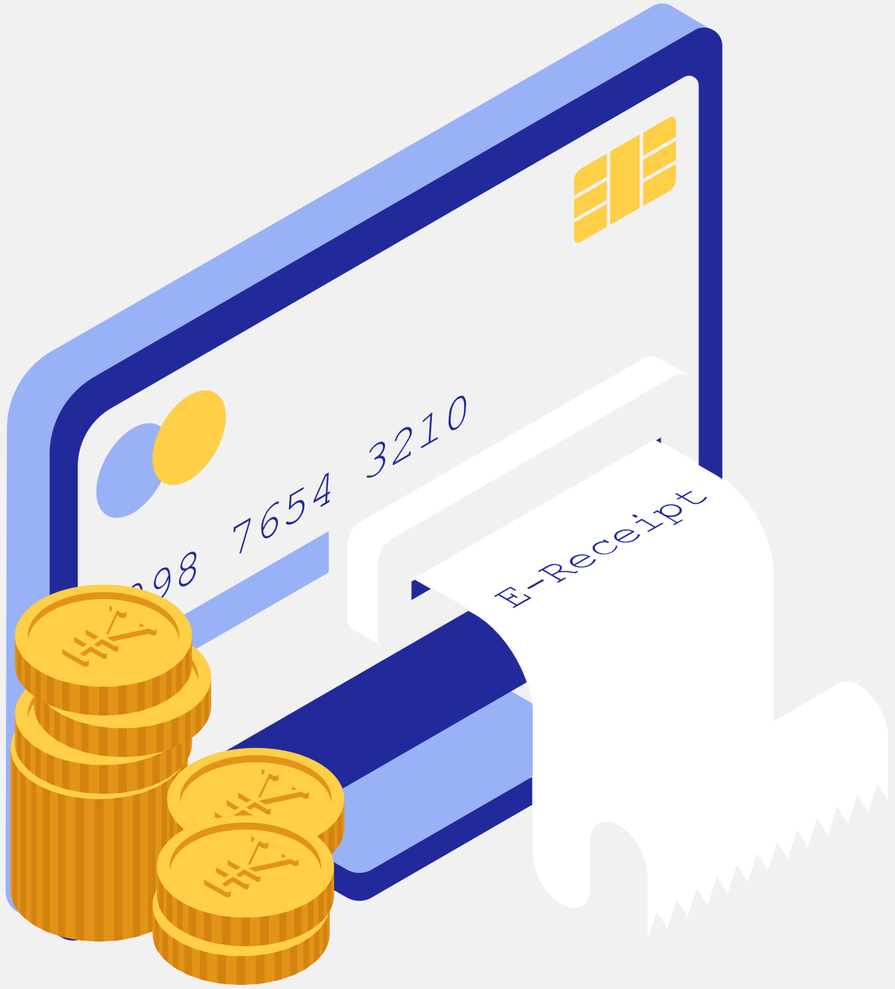


Understanding its power and influence

BCM und ITSCM 360 – Digitalisierung erfordert integrierte Sichtweise

How it changes the way we communicate and interact

Digitalisierung ITSCM

Permanent neue und höhere Anforderungen an die IT-Bereiche

- Tripple AAA ?
- Welche Auswirkungen hat die rasch steigende Digitalisierung in vielen Geschäftsbereichen ?
- Gibt es eine integrierte Sichtweise auf GRC, BCM und ITSCM ?
- Wie lange überleben Sie den Ausfall kritischer IT-Services ?
- Welche Ergebnisse aus anderen Projekten / Aufgabenstellungen sind verfügbar ?

CSP – Cyber Security Plattform

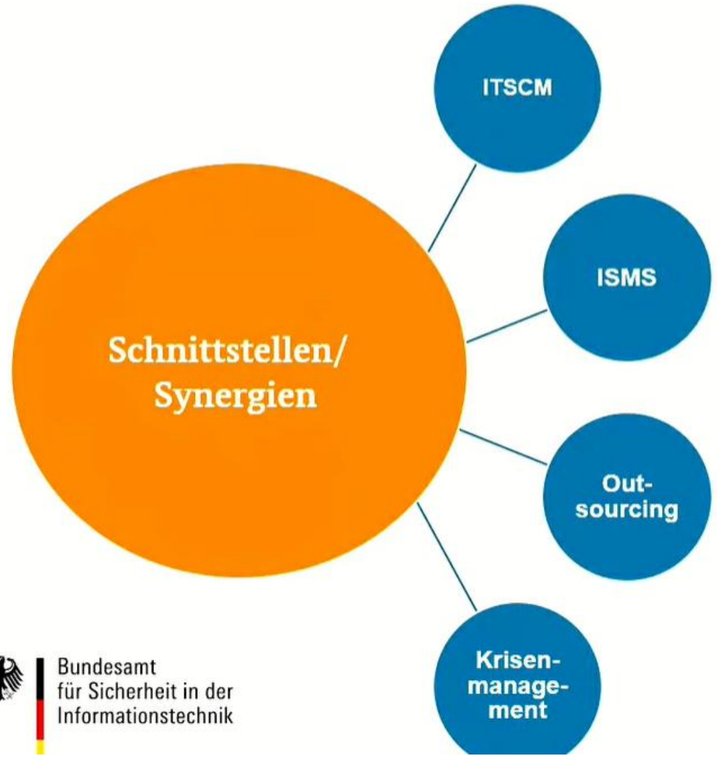
Hintergrund

- Digitalisierung kritischer Dienste
- Ausbau des IoT: weltweit 25 Mrd. verbundene Objekte bis 2025
- Anstieg von Cyberangriffe um 241 % (DDoS)
- Cyberkriminalität in der EU verursachte Kosten iHv 5,5 Billionen Euro im laufenden Jahr
- Die Pandemie beschleunigt die Abhängigkeit und vergrößert die Angriffsfläche (Krankenhäuser, Impfstoffverteilung)
- Geopolitischer Wettbewerb um den Cyberspace: autoritäre Regime untergraben das offene globale Internet und versuchen internationale Gremien/Normsetzung zu dominieren

Standards- und Normen – z.B. BSI 200-4

Neu im BSI-Standard 200-4

Abgrenzung zu weiteren Managementsystemen und Synergien in der Initiierung und darüber hinaus



Bundesamt
für Sicherheit in der
Informationstechnik

Mögliche Synergien

- **Viele** Möglichkeiten zum Austausch/Abgleich und zur Wiederverwendung von Ergebnissen
- Möglichkeiten zur **gemeinsamen** Erhebung
- Klare Aufteilung der **Verantwortlichkeiten/Zuständigkeiten** – auch im Notfall & in der Krise
- Darstellung in **Synergieboxen**

sichtigen. Unter anderem erfüllen die Risikomanagement-Standards BSI-Standard 200-3 *Risiko-management* sowie die Norm DIN ISO 31000:2018 *Risikomanagement –Leitlinien* diese Voraussetzung.

Synergiepotenzial:

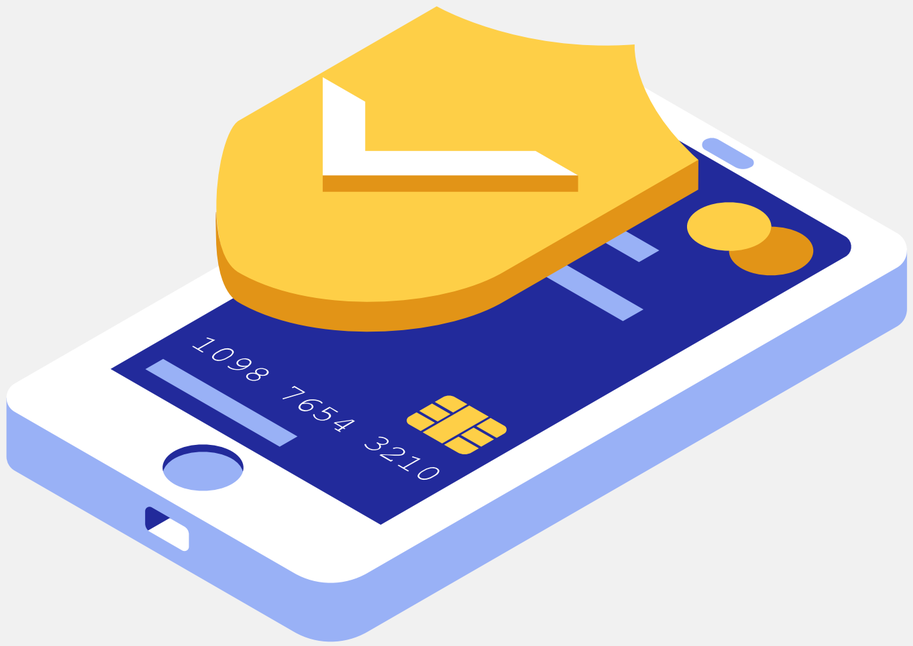
Auf Grund der methodischen Kompatibilität zu anderen Arten von Risikoanalysen ist es nicht zwingend erforderlich, eine eigenständige Methodik für die BCM-Risikoanalyse festzulegen. Es ist empfehlenswert, in einem ersten Schritt zu prüfen, inwieweit vorhandene Risikoanalyse-Methoden der Institution angewendet werden können. Hierzu können die Anforderungen an eine BCM-Risikoanalyse mit den jeweiligen Zuständigen der bestehenden Risikoanalyse-Methoden abgestimmt werden, z. B. dem Risikomanager oder Informationssicherheitsbeauftragten.

- ...und vieles mehr.

ITSCM im Bereich kritische Infrastruktur

Massiver Wandel in den letzten Jahren / Jahrzehnten

- Unbundling
- Immer höhere GRC–Anforderungen (Gesetze, Regulatoren…..)
- Digitalisierung
- IT / OT Herausforderungen
- IoT – Smart Meter….
- Viele Spezialanwendungen
- Keine “simple” Flucht in die Cloud



Schlüsselthemen

Notwendige Investitionen

und Ressourcen ?

Thema 1 — Klare Verantwortlichkeiten – kein Silodenken

Rolle der Stakeholder – Vereinbarkeit der Zielsetzungen ?

Thema 2 — “Pragmatische” Definition von IT-Business services

Ausreichender Detaillierungsgrad mit Fokus auf kritische Bereiche

Thema 3 — Hoher Abhängigkeitsgrad zwischen den Themen

Ohne entsprechende Tools Zusammenhänge nicht mehr erkennbar

Thema 4 — Priorisierung der Handlungsfelder

Unterschiedliche Sichtweisen der Stakeholder / Geschäftsbereiche

Thema 5 — Szenarien – Planung, Übung, KVP…

Blue Team / Red Team Übungen, Backup & Recoveryübungen…

Themen und Herausforderungen 1

Neue IT-Angriffsvektoren

Seit vielen Jahren findet eine ständige Vergrößerung der IT-Angriffsvektoren statt (Mobiler Arbietsplatz, IT/OT, Lieferketten, Ökosysteme usw.). Dies bedeuetet eine laufende Evaluierung neuer Risken und Gefahren sowie eine stetige Anpassung der Maßnahmen in allen Bereichen (Unternehmensrisikomanagement, BCM, ITSCM, Tools…)

Mergers & Acquisitions

Besonders in Konzernen findet ein laufender Wandel der Unternehmensorganisation und der Zugehörigkeit von Unternehmen statt. Es bedarf einer vorbereiteten Vorgehensweise um potentielle Auswirkungen rasch zu bewerten und entsprechende Anpassungen durchzuführen. Einbindung der IT in den Due Dilligence Prozess ?

Gesetze und Regulatorik

In den letzten Jahren gibt es immer höhere Anforderungen aus diesen Bereichen. Beispiele dafür sind NIS-Gesetz, GDPR, Nachweispflichten. Für viele Risikobereiche fehlt die Awareness über die potentiellen Auswirkungen (z.B. nicht rechtmäßige Verwendung von Open Source, Bewertung der Lieferantenrisken usw…). Ein spannender Bereich ist auch der Abdeckungsbereich durch Versicherungen !

Fernwartung

Viele Unternehmen haben Tätigkeiten vermehrt ausgelagert. Es fehlt das interne Knowhow oder die Ressourcen (auch ein Grund für die Cloud..). Unternehmen haben in ihren Verträgen Fernwartungen geregelt, oftmals ohne die potentiellen Risken zu adressieren. Gerade in diesem Bereich fehlt es inbesondere an Standards und Normen sowie umsetzbaren “Best Practices” oder dem “Stand der Technik”

Themen und Herausforderungen 2

Neue Technologien

Die Technologielandschaft entwickelt sich rasant weiter. Frühere Lösungsansätze (z.B. vollständige Trennung von Steuerungssystemen) sind heute aus Businesssicht nicht mehr möglich).
Beispiele sind Entwicklungen wie Cloud, Smart Meter, Echtzeitsteuerungen für neue Bereiche usw.)

Abstimmung der Notfallspläne

Besonders in Konzernen findet ein laufender Wandel der Unternehmensorganisation und der Zugehörigkeit von Unternehmen statt. Es bedarf einer gründlichen Vorbereitung um potentielle Auswirkungen rasch zu bewerten und entsprechende Anpassungen durchzuführen. Einbindung der IT in den Due Dilligence Prozess ?

Kommunikation

Der oftmals zitierte Stromausfall, DDoS-Attacken, Fehlverhalten von Protokollen, Kommunikation zu Stakeholdern und der Öffentlichkeit im Krisenfall – dies sind nur einige Beispiele die entsprechende Vorsorgen im Kommunikationsbereich erfordern (Planung, Übung, Test…)
Beipsiele:

- Redundate Kommunikationsmöglichkeiten (Satelittentelefon…)
- Eigene Infrastrutkur für Notfallskommunikation)

Gesamtüberblick im Management

Governanceaspekte gewinnen an Bedeutung, Klare und eindeutige Verantwortung auf Vorstands- und Bereichsleitungsebene, Einrichtung eines entsprechenden IKS (Internen Kontrollsystems), Abbildung der “Controls” im Kontext Prozesse und Verantwortung

Themen und Herausforderungen 3

Übung macht den Meister

Die einzelnen Krisen- und Notfallspläne müssen aufeinander abgestimmt sein und Abläufe entsprechend geübt warden:

- Backup- und Recovery
- Patchmanagement
- Ausfall kritischer IT-Business Services (z.B. Handelssysteme, Steuerungssysteme….)

Schulungsmaßnahmen

Laufende Unternehmens- und rollenspezifische Schulungen sind vermehrt notwendig. Das richtige Ausmaß zu finden gestaltet sich als schwierig. Unternehmensinterne Übungen und das Durchspielen von Szenarien sowie die Umsetzung von Verbesserungsmaßnahmen erreicht schell eine 3-stellige Anzahl von Personentagen je Themenbereich

Bewertung der Risken

In den letzten Jahren gibt es immer höhere Anforderungen aus diesen Bereichen (NIS,….). Für viele Risikobereiche fehlt die Awareness über die potentiellen Auswirkungen (z.B. nicht rechtmäßige Verwendung von Open Source, Bewertung der Lieferantenrisken usw…).
Die Sichtweise der Wirtschaftsprüfer, Prüfung durch “QuaSte” (Qualifizierte Stellen lt. NIS-Gesetz….) führen zu weiteren (berechtigten ?) Anforderungen !

Gesamtüberblick im Management

Informationen sind heute oftmals in Silosystemen verfügbar, ein managementorientierter Gesamtüberblick fehlt. Für die Weiterentwicklung der entsprechenden Prozesse, Systeme und Fähigkeiten ist eine Priorisierung notwendig. Dies kann nur auf dem Gesamtverständnis der Zusammenhänge beruhen.

Systeme für das Management

von BCM und ITSCM

- Gesamtüberblick zu Interdependenzen und Abhängigkeiten (Visualisierung, “Zoom-in”) notwendig
  - Behörden - Gesetze – Auflagen – Umsetzungskontrollen
  - Viele Ergebnisse aus anderen Projekten
    - Prozessmodell (8. EU Richtlinie)
    - Klassifikation Data Assets (GDPR)
    - ….
  - Individuallösung vs. Standardsoftware
    - Häufig relevante Informationen in “Spezialsystemen”

Beispiele für positive Entwicklungen

- Eine Reihe von europäischen und österreichischen Initiativen und Verfügbarkeit von Hilfestellungen / “öffentliches” Knowhow
- Zusammenarbeit in Communities (CMG, VOICE, EU) – “Digitale Souveränität”
- Technologie bietet zunehmend Automatisierungs-möglichkeiten
- Zusammenarbeit in der Energiewirtschaft (e-cert, ENCS,….)
- Cyber Risk Rating - KSÖ

DAS ÖSTERREICHISCHE CYBER RISK SCHEMA des KURATORIUM SICHERES ÖSTERREICH

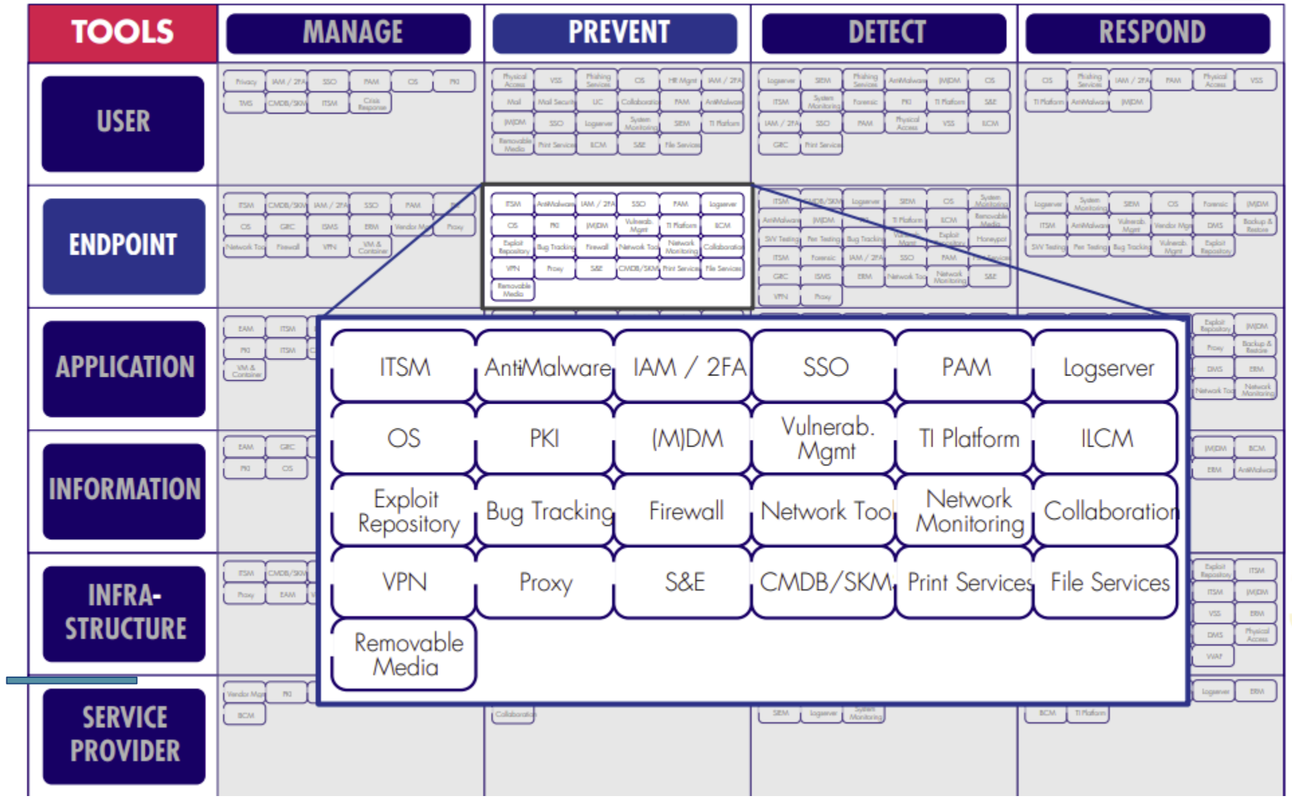
FINDING GAPS - ACCOUNTABILITY

1 BUILD ON EXISTING STANDARDS

2 DEFINE A STABLE STRUCTURE

3 ASSESS AND IMPROVE

ORGANIZATION	MANAGE	PREVENT	DETECT	RESPOND
USER	IAM Team, Security	IAM Team, Security	IAM Team, Security	IAM Team, Security
ENDPOINT	Workplace, Security	Workplace, Security	Workplace, Security	Workplace, Security
APPLICATION	Service Managers, Enterprise Architects	Service Owners, Enterprise Architects, Security	ROOM FOR IMPROVEMENT	
INFORMATION	Platform Managers, DPO	Platform Managers, DPO	Platform Managers	Platform Managers
			Platform Managers	Platform Managers
			Vendor Managers	Vendor Managers



1 BUILD ON EXISTING STANDARDS

2 DEFINE A STABLE STRUCTURE

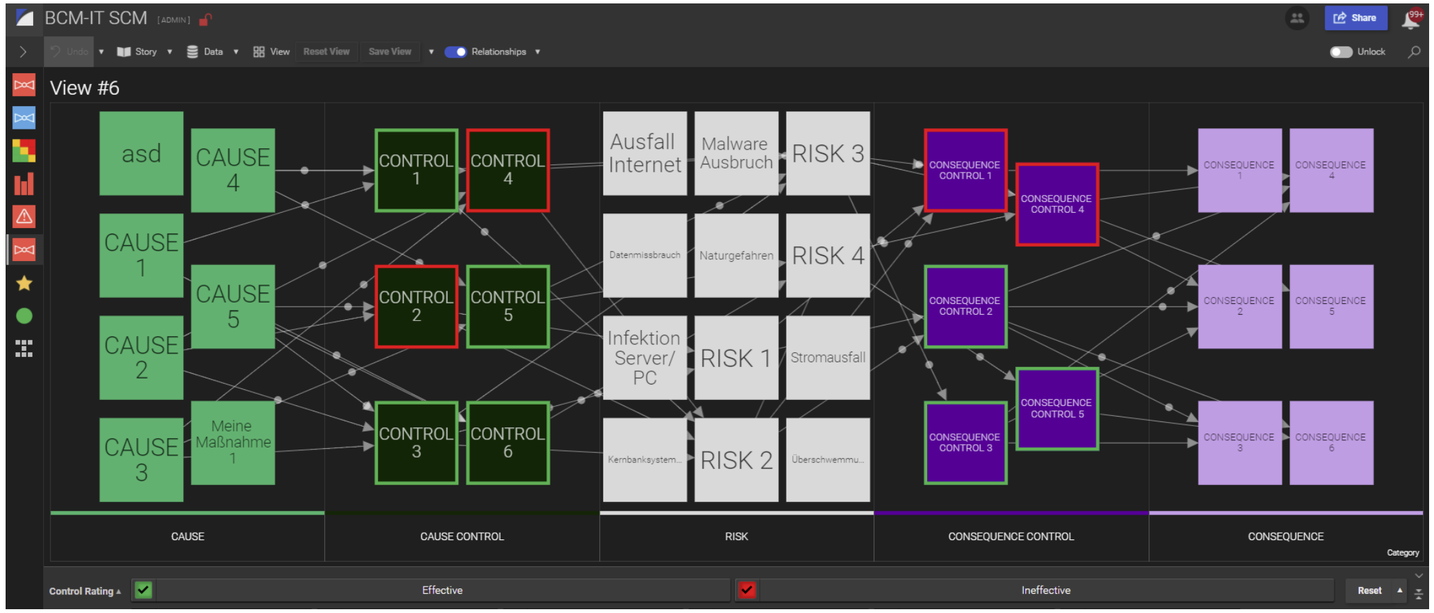
3 ASSESS AND IMPROVE

Securityarchitecture

- Erweiterung des Ansatzes für BCM und ITSCM
- Integrierter Gesamtüberblick
- Toolunterstützung Sharpcloud
- Ein Bild sagt mehr als tausend Worte

Ihre Beiträge:

- Erfassung und Darstellung von BCM und ITSCM – “Bausteinen”
  - Areas of interest - Handlungsfelder
  - **Risken und Herausforderungen**
  - Produkte und Lösungen
  - Maßnahmen
  - Allgemein
  - Wissensbeiträge (z.B. CMG-Leitfaden)



BCM und ITSCM

Digitalisierung und neue Geschäftsmodelle erfordern die enge Verzahnung aller Pläne und Maßnahmen

Regelmässiger Austausch im Unternehmen und…..

Unternehmensrisikomanagement, Notfall- und Krisenmanagement, Rechtsbereich und IT, neue Anforderungen durch gesetzliche Entwicklungen

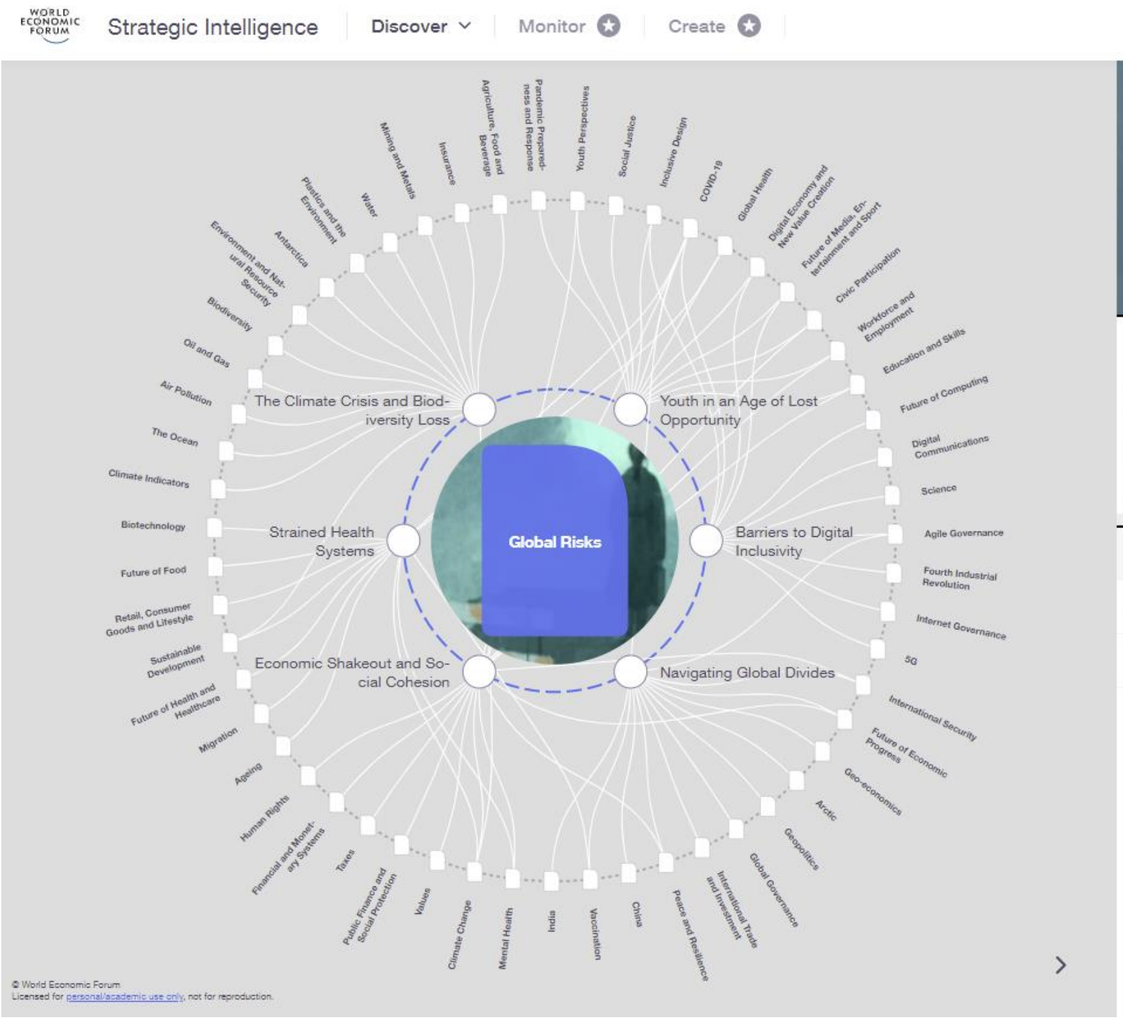
Business Kritikalität der IT-Businessservices

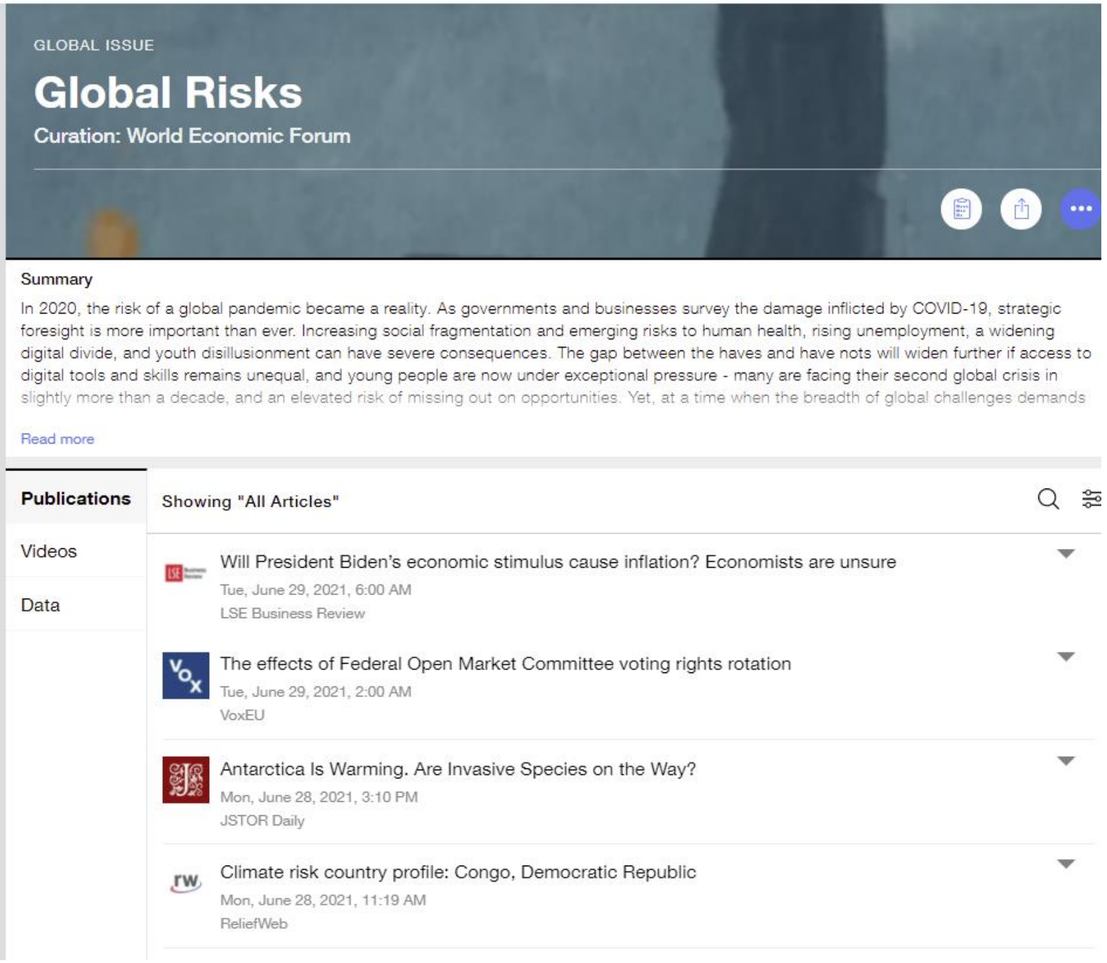
Ein vollständiger und abgestimmter Katalog als Grundlage für alle Maßnahmen. Die zunehmende Verlagerung von Services in die Cloud sowie IoT-Herausforderungen erhöhen die Komplexität.

ITSC - Plan

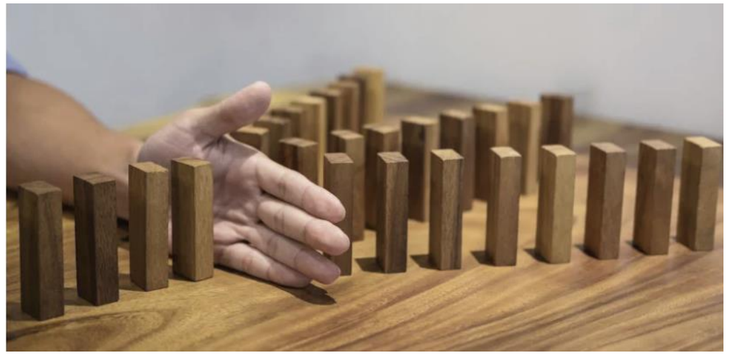
Viele Bausteine und Maßnahmen wurden über die Zeit entwickelt (Prozessmodell, Data Assets, redundante Komponenten usw.). Die Wirksamkeit ist regelmäßig zu prüfen.

Global Risks – World Economic Forum





Weiterführende Informationen



Communities,

Whitepapers,….

Webinare….

T1 Deutscher IT-Grundschutztag – BSI-200/4

https://www.youtube.com/playlist?list=PLEnTDCi_wQ6LeliJGpULuAdCvy3eFdKQK

T2 Datensicherungsstrategien bei neuer Schadsoftware

https://bcom.stickiebox.org/share/s/gLc-qMZZSpKOybw_jQjr6g

T3 Security Insider – Mit ITSCM für den Notfall gewappnet

https://www.security-insider.de/mit-itscm-fuer-den-notfall-gewappnet-a-897816/

T4 Club CISO – Security Maturity Report 2020

https://bcom.stickiebox.org/share/s/2qNl4ysXSOumgGwX3O9mgw

T5 NIST Publikationen

https://csrc.nist.gov/publications/sp

T6 Die Schnittstellen zwischen BCM und ITSCM - KPMG

https://bcom.stickiebox.org/share/s/5fP1dmACQK2mned3H1fNRw