Beyond IT

Wie resilient können wir sein?

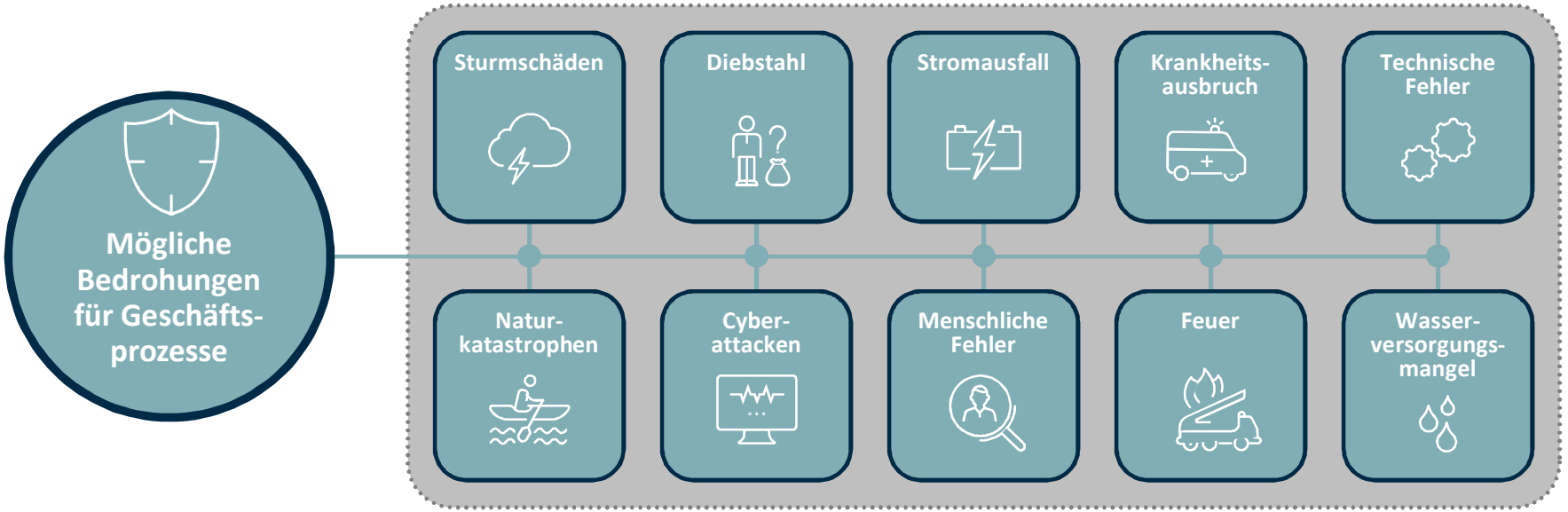
8. Kommunaler IT-Sicherheitskongress 2022

Berlin, 03.05.2022

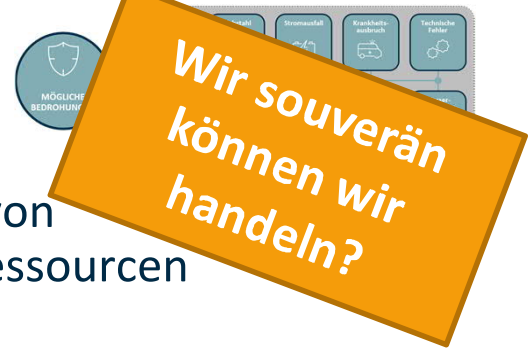
STADT ESSEN

FB 03-01 Digitalisierungsstrategie / Chief Digital Officer (CDO)

Mögliche Bedrohungen für die Aufrechterhaltung der Geschäftsprozesse



Weitere Einflussfaktoren



- Abhängigkeit von Hard- und Softwarewareanbietern
  - Cloud-Systeme
  - Service / Support
  - Funktionale Weiterentwicklung
  - Versorgung mit technischen Komponenten (z.B. Chips, Server, …)
  - Patentnutzungen
  - Basistechnologie (z.B. Betriebssysteme)
  - Innovationskraft
  - Vertragliche Regelungen
  - Geschäftsbetrieb
- Abhängigkeit von personellen Ressourcen
  - Fachkräfte
  - Forschung und Entwicklung
- Politische Abhängigkeiten
  - Rahmen für KI und Big Data
  - Gesetze und Verordnungen
  - EfA- oder Jeder-für-sich-Modell
  - Export-/Import-Beschränkungen
- Weitere Abhängigkeiten
  - Rohstoffe
  - Akzeptanz der Lösungen

IT-Sicherheit

und / oder

Informationssicherheit

und / oder

Resilienzmanagement

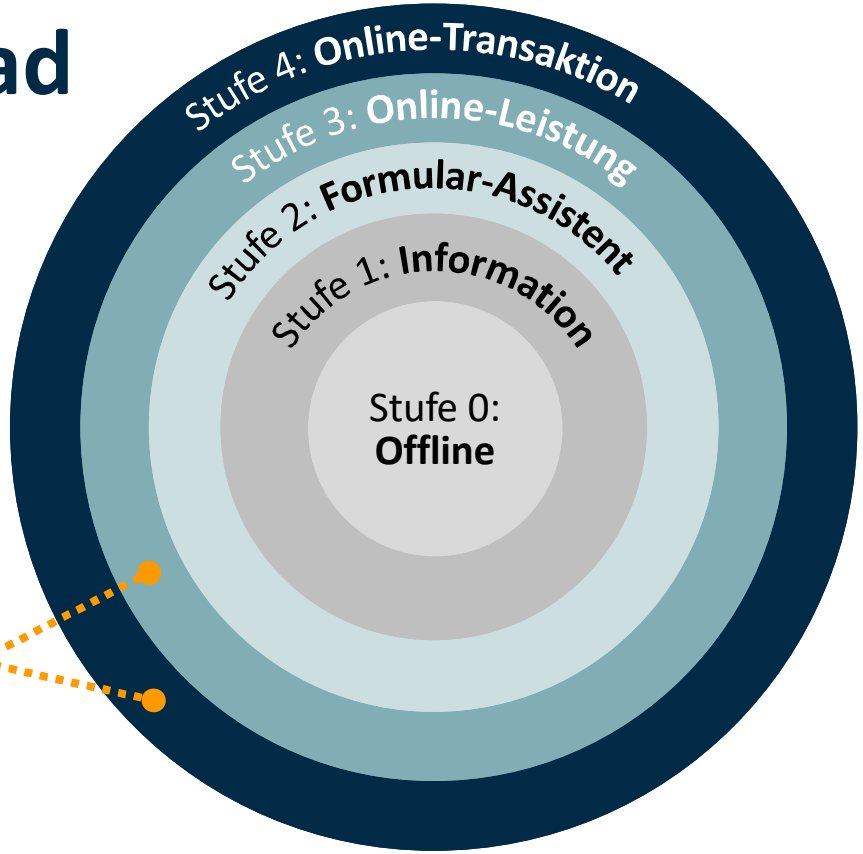
STADT
ESSEN

OZG: Digitaler Reifegrad

- Stufe 0: Keine Information online verfügbar.
- Stufe 1: Die Leistungsbeschreibung ist online verfügbar und ein Formular steht als Download zum Ausdruck zur Verfügung.
- Stufe 2: Eine Online-Beantragung ist grundsätzlich möglich. Nachweise können regelmäßig noch nicht online übermittelt werden.

OZG erfüllt

- **Stufe 3: Die Online-Leistung kann einschließlich aller Nachweise vollständig digital abgewickelt werden. Der Bescheid wird digital zugestellt.**
- **Stufe 4: Die Beantragung ist online möglich, bei der Daten und Nachweise aus Registern der Verwaltung abgerufen werden können („Once Only“) statt sie durch Nutzer*innen einzureichen.**



Quelle Reifegradbeschreibung: BMI
Quelle Grafik: Stadt Essen

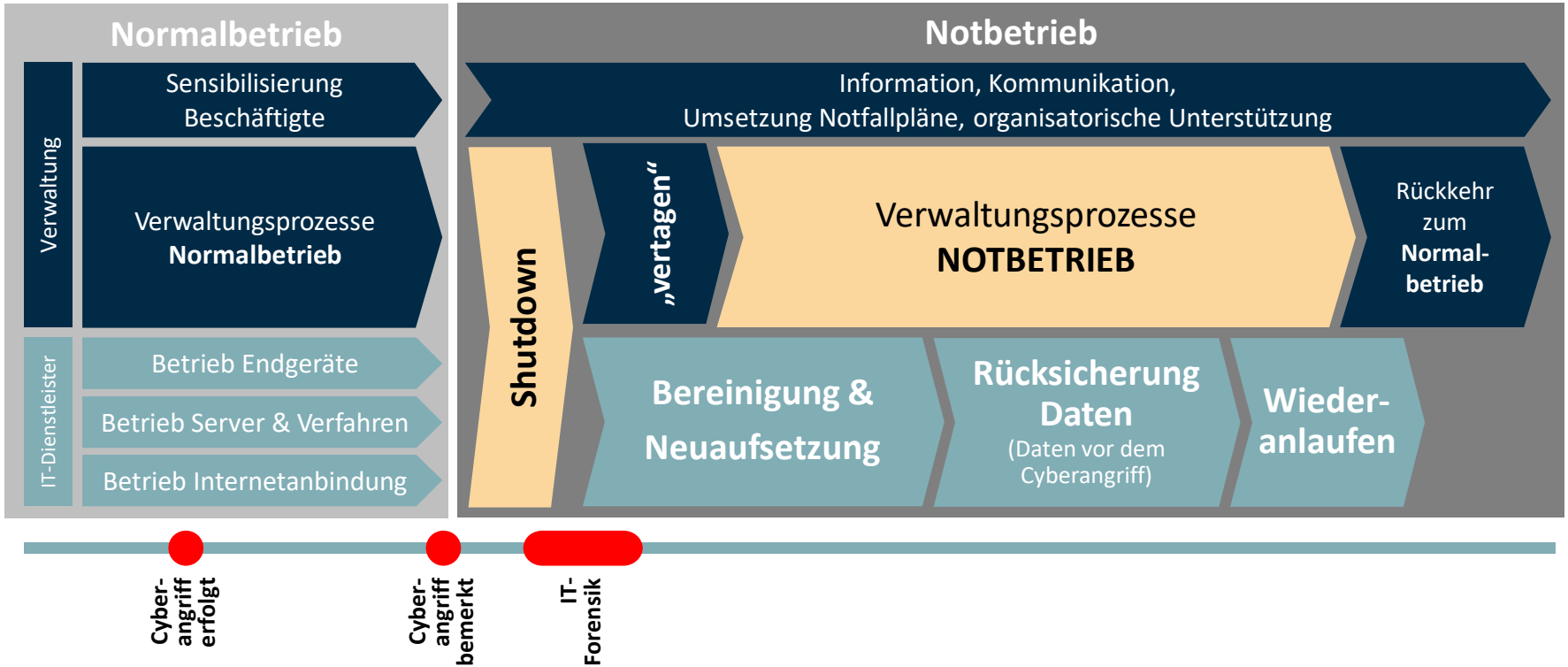
Ziel des Resilienzmanagements:

Insbesondere

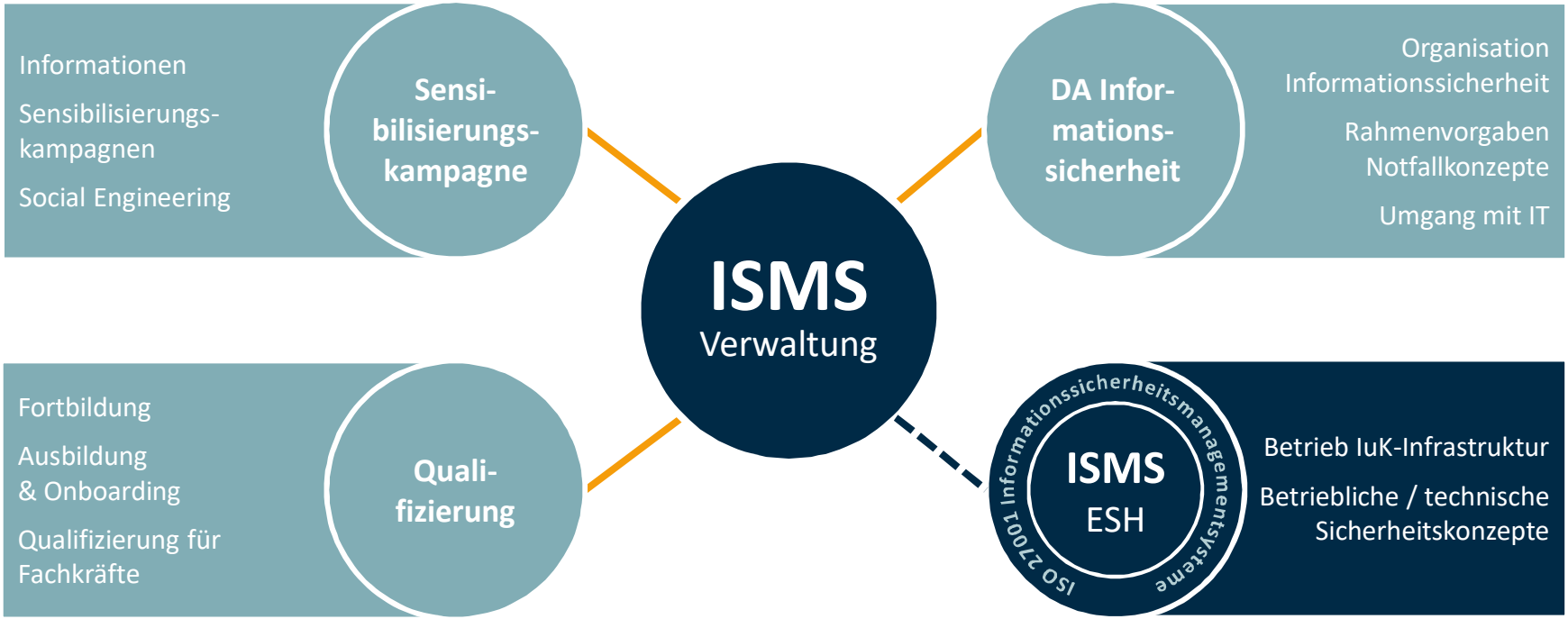
Aufrechterhaltung der kritisch(st)en Geschäftsprozesse

STADT ESSEN

Cyberangriff: IT-gestützte Verwaltungsprozesse



Informationssicherheitsmanagement



Die Absicherung durch technische Sicherheitsvorkehrungen ist vorrangig und grundlegend

STADT ESSEN

Handlungsfelder

Technik

- Firewall
- Spam-/Reputationsfilter
- DDoS-Absicherungen
- 2-Faktor-Authentisierung
- Mobile Device Management
- Sperrung kritischer Dienste
- Analyse Netzwerkverkehr
- Penetrationstests
- Softwarescans
- Zertifizierung (z.B. ISO 27001)
- Informationsaustausch CERT
- **Anforderungsgerechte IT**
  (z.B. Rücksicherungszeiten beachten)

Organisation

- Bestellung ISB
- Business Impact Analyse
- Bewertung Kritikalität
- Priorisierung von Prozessen
- **Checklisten** Notfallplanung
- **Notfallpläne** für Notbetrieb und Wiederherstellung
- Informationssicherheits-managementsystem (ISMS)
- Aufbau Prozessregister und Zuordnung Software
- **Anforderungsgerechte IT**
  (z.B. Rücksicherungszeiten vorgeben)

Beschäftigte

- Regelmäßige Informationen
- Sensibilisierungsmaßnahmen
- Phishingangriffe simulieren
- Kurze Lernvideos
- Plattform für Schulungen zur Informationssicherheit
- Übungen zur Umsetzung von Notfallplänen
- **Ebenengerechte Kommunikation**
  - Sachbearbeitungen sind keine ISB
  - Zu hohe Komplexität führt zu Sicherheitslücken

Planung und Dokumentation, um Notfälle zu vermeiden und etwaige Schäden so gering wie möglich zu halten

- Angriffe **vermeiden**
- Während einer Beeinträchtigung bestmöglich **handlungsfähig** bleiben
- Nach einem (Teil-)Ausfall das schnellstmögliche **Wiederanlaufen** ermöglichen

Planung und Dokumentation,
um im Notfall nicht noch das „Wie“ zu klären

Zielgruppe:

„Dieses IT-Grundschutz-Profil richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen.

Es … adressiert … **Hauptverwaltungs-beamtinnen und –beamte** … und **Informationssicherheitsbeauftragte**“

STADT ESSEN

Anlage zur DA Informationssicherheit:
Business Impact Analyse – Ersteinschätzung

Für eine Ersteinschätzung über die Kritikalität eines Prozesses ist das nachfolgende Schema zu nutzen.

Betrachteter Geschäftsprozess*	
Kurzbezeichnung Prozess	
Fachbereich	
Geschäftsbereich	
Ansprechperson, Rufnummer	
Von welchen Systemen ist der Geschäftsprozess abhängig (z.B. welche Fachverfahren)	
Wo liegen die Daten und wer betreibt das IT-Verfahren? (z.B. Laufwerk i:, ESH oder Cloudsystem xy von xz)	
Datum dieses Dokumentes	

*) Die Business Impact Analyse (BIA) dient der Ermittlung der Kritikalität von einem Geschäftsprozess. Sie beschreibt die Auswirkungen eines Vorfalls auf einen Geschäftsprozess. Ein Geschäftsprozess ist eine sich wiederholende Abfolge von Tätigkeiten mit dem Ziel, eine konkrete Verwaltungsleistung zu erbringen, die nach innen oder außen gerichtet ist. Geschäftsprozesse dienen damit z.B. der Ausstellung einer Personenstandsurkunde, dem Betrieb der Lichtsignalanlagen, der Beantragung und Auszahlung von Wohngeld (hier liegen evtl. sogar zwei Geschäftsprozesse vor), u.ä. Pro Fach- oder Geschäftsbereich wird es mehrere Geschäftsprozesse geben, die jeweils eine unterschiedliche Kritikalität aufweisen. Die Erfassung über die BIA dient der Herstellung eines Überblicks über die kritischen Geschäftsprozesse mit den gravierendsten Auswirkungen. Dies kann der Priorisierung von Gegenmaßnahmen oder zur Festlegung einer Wiederherstellungsreihenfolge z.B. bei der Behebung von Cyberangriffen dienen. Die BIA im Rahmen eines IT-Notfallkonzeptes betrachtet das Szenario „Cyberangriff" und der Annahme, dass die IT-Systeme und damit Daten und Fachverfahren für den jeweiligen Geschäftsprozess für drei Tage, drei Wochen oder drei Monate nicht zur Verfügung stehen. Die Erstellung von Notfallkonzepten obliegt im Rahmen der dezentralen Ressourcenverantwortung den produktverantwortlichen Fachbereichen. Querschnittsbereiche unterstützen durch Checklisten, Beratung und teilw. gesamtstädtische Maßnahmen. Die BIA ist keine vollständige Geschäftsprozessdarstellung.

Schadensbewertung

Auswirkungen bitte von 1-4 bewerten (siehe Bewertungsmatrix unten).
Bei „Begründung..." können konkrete Auswirkungen kurz und prägnant beschrieben werden.

Auswirkungen \ Ausfallzeit	IT-Ausfall 3 Stunden	IT-Ausfall 3 Tage	IT-Ausfall 3 Wochen	IT-Ausfall 3 Monate
Beeinträchtigung der Aufgabenerfüllung				
Begründung der Bewertung				
Beeinträchtigung der persönlichen Unversehrtheit				
Begründung der Bewertung				
Finanzielle Auswirkungen für die Verwaltung				
Begründung der Bewertung				
Verstoß gegen Gesetze, Vorschriften und Verträge				
Begründung der Bewertung				
Negative Innen- und Außenwirkung (Imageschaden)				
Begründung der Bewertung				

Es handelt sich um einen Geschäftsprozess, der zur kritischen Infrastruktur nach der KRITIS-Verordnung (https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html) gehört
☐ Ja ☐ Nein

Zu dem v.g. Prozess wurde ein Notfallkonzept (Dokumentation von Maßnahmen zur Vermeidung von Ausfällen, zur Aufrechterhaltung eines Notbetriebes im Fall einer Beeinträchtigung und für ein schnelles Wiederanlaufen nach einem Vorfall) ...
☐ bereits erstellt ☐ noch nicht erstellt

Für die Erstellung oder Überarbeitung eines Notfallkonzeptes wird Unterstützung benötigt
☐ Ja ☐ Nein

Bewertungsmatrix und Legende

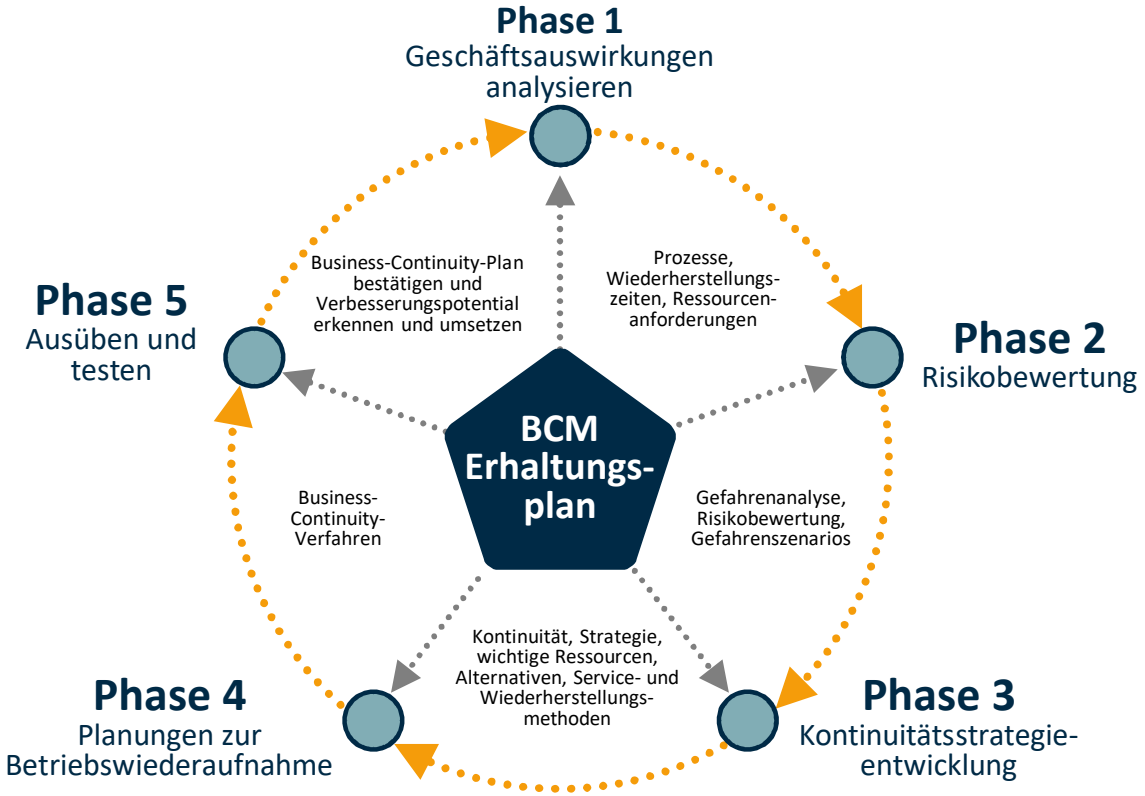
Auswirkung	Maßstab
	Schadensszenario „Beeinträchtigung der Aufgabenerfüllung" Kommt es durch den Ausfall zu Beeinträchtigungen der Aufgabenstellung der Organisationseinheit?
1 – niedrig	Keine nennenswerten Auswirkungen.
2 – mittel	Beeinträchtigung wird von Beschäftigten und Kunden toleriert / andere Tätigkeiten können vorgezogen werden / Nacharbeit behindert die Aufgabenerfüllung nicht merklich / andere Organisationseinheiten, Institutionen oder Externe werden in ihrer Arbeit nicht wesentlich gestört.
3 – hoch	Nicht tolerierbare Unterbrechungen bzw. Einschränkungen / Minderung der Arbeitsqualität / Fristversäumnisse nach außen wirksam / das Aufholen von Arbeitsrückständen ist nicht innerhalb der normalen Arbeitszeit möglich / andere Organisationseinheiten, Institutionen oder Externe werden in ihrer Arbeit erheblich gestört, auch dort müssen Rückstände aufgeholt werden.
4 – sehr hoch	Gravierende Beeinträchtigung der Aufgabenerfüllung / Rückstände können nur mit externer Hilfe oder gar nicht aufgeholt werden / Verzögerte und fehlerhafte Ergebnisse werden extern deutlich bemerkt / schwerwiegende Minderung der Servicequalität.
	Schadensszenario „Beeinträchtigung der persönlichen Unversehrtheit" Wie beeinträchtigt der Ausfall der Geschäftsprozesse die persönliche Unversehrtheit?
1 – niedrig	Eine Beeinträchtigung erscheint nicht möglich.
2 – mittel	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
3 – hoch	Eine Beeinträchtigung der persönlichen Unversehrtheit ist möglich. Gefahr für Leib und Leben kann nicht absolut ausgeschlossen werden.
4 – sehr hoch	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Es besteht Gefahr für Leib und Leben.
	Schadensszenario „Finanzielle Auswirkungen" Wie wirkt sich der Ausfall des Geschäftsprozesses auf die Institution aus?
1 – niedrig	Keine nennenswerten Auswirkungen (z. B. Schaden geringer als 1.000€).
2 – mittel	Der finanzielle Schaden bleibt für die Institution tolerabel (z. B. Schaden ist 1.000 bis 100.000€).
3 – hoch	Der Schaden bewirkt beachtliche finanzielle Verluste (z. B. Schaden ist 100.000 bis 500.000€).
4 – sehr hoch	Der finanzielle Schaden ist für die Institution untragbar (z. B. Schaden ist höher als 500.000€).
	Schadensszenario „Verstoß gegen Gesetze, Vorschriften und Verträge" Können durch den Ausfall des Geschäftsprozesses gesetzliche, vertragliche oder regulatorische Vorgaben beeinträchtigt oder nicht eingehalten werden?
1 – niedrig	Keine nennenswerten Auswirkungen.
2 – mittel	Verstöße gegen Gesetze und Bestimmungen mit geringen Konsequenzen / Verstöße werden nur intern bemerkt.
3 – hoch	Verstoß gegen Gesetze und Bestimmungen mit hohen Konsequenzen / Verstöße werden auch außerhalb der Institution bemerkt.

Schadensbewertung

Auswirkungen bitte von 1-4 bewerten (siehe Bewertungsmatrix unten).
Bei „Begründung..." können konkrete Auswirkungen kurz und prägnant beschrieben werden.

Auswirkungen \ Ausfallzeit	IT-Ausfall 3 Stunden	IT-Ausfall 3 Tage	IT-Ausfall 3 Wochen	IT-Ausfall 3 Monate
Beeinträchtigung der Aufgabenerfüllung				
Begründung der Bewertung				
Beeinträchtigung der persönlichen Unversehrtheit				

Business-Continuity-Kreislauf in 5 Phasen



Was fehlt?

Zusammenarbeit

- Bei einem Angriff: Wer hilft mir bei der Abwehr und den zu ergreifenden Maßnahmen, auch wenn ich nicht zu kritischen Infrastruktur gehöre
- Kommunal-CERT mindestens auf regionaler oder Landesebene mit Task Force für Akut-Maßnahmen (nicht in jeder Kommune!)
- Digitale Souveränität ist für Kommunen nur in Grundzügen kommunal zu lösen

Arbeitsmaterialien

- Kondensat der Handbücher und Richtlinien für Beschäftigte, die nicht in den Bereichen ISB oder IT arbeiten
- (Online-)Checklisten für Führungskräfte zur Hinterfragung des eigenen Geschäftsprozesses (wie z.B. Einhaltung der BSI-Servicestandards durch einen OZG-Geschäftsprozess)
- Lösungshilfen zur Ersetzung von digitalen durch analoge Notfall-Prozesse

„Ein erfolgreicher Cyberangriff findet statt. Fraglich ist **wann**.“ Quelle: BSI

Wir wissen, was passieren kann. Wenn wir uns nicht vorbereiten, handeln wir **fahrlässig**.

Eine Investition in Informationssicherheit ist **günstiger** als ein wochenlanger Notbetrieb.

STADT ESSEN

Kontaktdaten

Peter Adelskamp
Chief Digital Officer (CDO)

Digitalisierungsstrategie
Rathaus Porscheplatz
45121 Essen

Tel.: +49 201 88-88109
E-Mail: peter.adelskamp@digital.essen.de

www.essen.de

STADT ESSEN

vCard