

Staatliches Handeln in Zeiten permanenter Unsicherheit

Ein Leitfaden für souveräne und resiliente Verwaltungen



Management Summary

Die öffentliche Verwaltung ist ein zentrales Rückgrat kritischer Infrastrukturen – und muss auch in Krisen handlungsfähig bleiben. Resilienz bedeutet mehr als IT-Sicherheit: Sie umfasst digitale Souveränität, vorausschauende Planung und die Fähigkeit, Störungen flexibel abzufedern. Das Whitepaper zeigt zentrale Schwachstellen in Technologie, Organisation und Kultur auf und beschreibt fünf strategische Bausteine: souveräne Infrastruktur, Frühwarn- und Krisenmanagement, Cybersicherheit, Einsatz von KI und Innovation sowie eine resiliente Führungs- und Fehlerkultur. Entscheidend ist ein ganzheitlicher Ansatz: Resilienz muss politisch gewollt, organisatorisch verankert und kulturell gelebt werden. So wird Verwaltung krisenfest, souverän und gewinnt dauerhaft Vertrauen.



Inhaltsverzeichnis

Zusammenfassung	4
Fünf strategische Bausteine für mehr Resilienz und Souveränität	6
1. Die Welt im Umbruch	8
2. Deutschlands strukturelle Verwundbarkeiten	9
3. Ein souveränes, widerstandsfähiges Deutschland	10
4. Fünf strategische Bausteine staatlicher Souveränität und Resilienz	11
Baustein 1: Technologische Souveränität und resiliente Infrastrukturen	12
Baustein 2: Frühwarnsysteme und Krisenmanagement	13
Baustein 3: Cybersicherheit und Datenschutz	14
Baustein 4: KI-Einsatz und datengetriebene Innovationen	15
Baustein 5: Resiliente Führungs-, Organisations- und Fehlerkultur	16
Fazit: Resilienz beginnt heute – und in Ihrer Organisation	17
Unsere Unterstützung für Sie	18
Quellen und Verweise	19
Anhang: Praktische Handlungsempfehlungen mit Checkliste	20
Abkürzungsverzeichnis	21
Glossar	21
Ihre Ansprechpersonen	22

Zusammenfassung

Behörden sind Teil kritischer Infrastrukturen. Ihre Funktionsfähigkeit ist entscheidend für die Aufrechterhaltung der öffentlichen Sicherheit und staatlichen Ordnung. Daher müssen Behörden in Deutschland widerstandsfähig (resilient) gegenüber Krisen, Cyberangriffen und disruptiven Veränderungen sein. Resilienz bedeutet dabei weit mehr als reine IT-Sicherheit – sie umfasst die Fähigkeit, digitale Souveränität aufzubauen, Störungen frühzeitig zu erkennen, angemessen und schnell darauf zu reagieren und den Dienstbetrieb kontinuierlich aufrechtzuerhalten.

Insbesondere Ereignisse wie die COVID-19-Pandemie, Naturkatastrophen, Cyberangriffe und geopolitische Krisen haben deutlich gemacht, wie essenziell es für Verwaltungen ist, ihre Dienstleistungen auch unter extremen Bedingungen zuverlässig bereitzustellen. Entwicklungen in den USA und weiteren Ländern verdeutlichen zudem die wachsende Bedeutung digitaler Souveränität, besonders bei der Nutzung von Cloud- und KI-Technologien. Rechtliche Vorgaben wie das KRITIS-Dachgesetz und die NIS-2-Richtlinie spannen den Handlungsrahmen auf.

Notwendigkeit staatlicher Souveränität in einer turbulenten Welt

Souveränität ist kein Selbstzweck, sondern Voraussetzung für die Aufrechterhaltung staatlicher Funktionen, gesellschaftlicher Gestaltungsfreiheit und Werte.



Wie kann sich der öffentliche Sektor diesen äußeren Zwängen widersetzen, um den eigenen Resilienz- und Souveränitätsgrad zu erhöhen?

Vor dem Hintergrund der veränderten europäischen und internationalen Sicherheitsordnung, der Werte und Normen bis hin zu Datenschutzaspekten nehmen Bedrohungen und Risiken durch staatliche und nichtstaatliche Akteure zu. Gleichzeitig führen klimatische Veränderungen zu immer häufigeren und schwerwiegenden Schadenslagen. Zudem steht die Welt am Beginn des Datenzeitalters: Digitale Infrastrukturen und das darin gespeicherte Wissen werden zunehmend zur Lebensader moderner Gesellschaften. Der Schutz dieser Systeme ist daher essenziell.

Die Bundesregierung hat 2022 eine Resilienz-Strategie beschlossen, die alle Phasen des Krisenmanagements – von Prävention über Vorsorge und Bewältigung bis hin zum Wiederaufbau – abdeckt. In der Nationalen Sicherheitsstrategie 2023 wird Resilienz als zentrales Prinzip hervorgehoben. Internationale Standards wie ISO 22301 (Business Continuity Management) und das Sendai Framework der UN bieten praxisnahe Leitlinien. Auch die OECD empfiehlt einen ressortübergreifenden und ganzheitlichen Ansatz zur Stärkung der staatlichen Widerstandsfähigkeit.

Best Practices aus Ländern wie Estland, Finnland und Singapur zeigen, wie digitale Souveränität und Innovation Resilienz konkret fördern können – etwa durch gesicherte Dateninfrastrukturen im Ausland (Estlands digitale Kontinuität) oder umfassende Gesamtverteidigungskonzepte wie Finnlands comprehensive security.

In diesem Whitepaper steht staatliche, organisationale, digitale Resilienz im Mittelpunkt – also die Frage, wie Verwaltungen in Deutschland krisenfester und anpassungsfähiger werden. Dabei richten wir uns gezielt an Praktiker:innen in Behörden: Führungskräfte, CIOs, Organisationsentwickler:innen, IT-Referatsleitungen, Datenschutz- und Informationssicherheitsbeauftragte und Projektleitende, die Resilienz vor Ort umsetzen wollen. Ihnen bietet dieses Papier konkrete Strategien, Beispiele und Handlungsempfehlungen, um Resilienz im eigenen Haus zu stärken.

Dieses Whitepaper verfolgt drei Ziele:

1



Analyse

Es beschreibt strukturelle Schwächen und Systemgrenzen in der aktuellen Resilienzarchitektur Deutschlands.

2



Vision

Es skizziert eine realisierbare Vision für ein souveränes, widerstandsfähiges Deutschland.

3



Umsetzung

Es identifiziert konkrete Handlungsfelder und Bausteine, die zu einer systematischen Resilienz-Strategie beitragen können – über Politikbereiche und Sektoren hinweg auch mit Blick auf die digitale Souveränität.

Fünf strategische Bausteine für mehr Resilienz und Souveränität

Resilienz in der öffentlichen Verwaltung entsteht nicht zufällig – sie muss bewusst gestaltet, politisch gewollt und organisatorisch verankert werden. Der erste Schritt ist die Entwicklung einer klaren Resilienz-Strategie, die durch einen politischen Beschluss legitimiert und mit konkreten Zeitvorgaben unterlegt wird. Nur so lässt sich sicherstellen, dass Resilienz nicht als Nebenprojekt im Alltagsbetrieb untergeht, sondern als prioritäres Handlungsfeld ernst genommen wird.

Dabei ist zu berücksichtigen: Eine Resilienz-Strategie ist kein einmaliges Dokument, sondern ein dynamischer, lernorientierter Prozess. Er beginnt mit einer fundierten Risikoanalyse, einem initialen Reifegradcheck und ersten operativen Maßnahmen – von IT-Sicherheitsaudits über die Aktualisierung von Notfallplänen bis hin zur Krisenstabsbenennung und Mitarbeitersensibilisierung. Im weiteren Verlauf gilt es, erkannte Lücken systematisch zu schließen, den Reifegrad kontinuierlich weiterzuentwickeln und Resilienz fest in der strategischen Steuerung der Verwaltung zu verankern – unterstützt durch Governance-Strukturen, technologische Weiter-

entwicklung, institutionalisierte Kooperationen sowie eine transparente Kommunikation, die sicherstellt, dass die Strategie in den Köpfen und im Handeln der Mitarbeitenden ankommt. Nur durch begleitende Maßnahmen wie interne Kampagnen, Dialogformate und Führungskräftekommunikation wird Resilienz als gemeinsame Aufgabe verstanden und im Alltag gelebt – statt als abstraktes Konzept auf dem Papier zu bleiben.

Innovationsansätze wie Reallabore bieten zudem eine wichtige Chance: Sie ermöglichen das risikobewusste Erproben neuer Lösungen unter realen Bedingungen. Der jüngste gesetzliche Vorstoß zu Reallaboren schafft hierfür einen geeigneten Rahmen und sollte von Verwaltungen aktiv genutzt werden, um regulatorisches Lernen und technologische Anpassung zu fördern.


Erst auf dieser Grundlage entfalten die folgenden fünf strategischen Bausteine ihre Wirkung. Sie konkretisieren, wie Resilienz und Souveränität in zentralen Handlungsfeldern gestärkt werden können – technologisch, organisatorisch und kulturell.



 Die fünf zentralen Handlungsfelder im Überblick


1. Technologische Souveränität und resiliente Infrastruktur

Ziel ist es, die Unabhängigkeit von einzelnen Anbietern zu stärken und technologische Abhängigkeiten zu reduzieren. Dazu gehört der konsequente Einsatz offener Standards für eine interoperable und zukunftssichere IT-Landschaft in der Verwaltung. Besonders wichtig ist der Aufbau und die Nutzung souveräner Cloud-Infrastrukturen sowie vertrauenswürdiger Datenräume, um sensible Informationen sicher, transparent und regelbasiert zu verarbeiten. Kritische Infrastrukturen sollten redundant, skalierbar und sicher gestaltet werden, um im Krisenfall funktionsfähig und updatefähig zu bleiben.


2. Frühwarnung und Krisenmanagement

Der Ausbau von Frühwarnsystemen wie Cell Broadcast und Warn-Apps sowie der Einsatz moderner Risikomanagement-Tools sind essenziell, um Gefahren frühzeitig zu erkennen und gezielt zu handeln. Eine zentrale Herausforderung bleibt die fehlende automatisierte und standardisierte Datenaufbereitung und Bereitstellung, die die Erstellung übergreifender Lagebilder erschwert. Deshalb braucht es verbindliche Regelungen zur Datenverfügbarkeit sowie eine enge, koordinierte Zusammenarbeit zwischen Bund, Ländern und weiteren Akteuren. Regelmäßige Krisenübungen wie LÜKEX sind wichtig, um Abläufe zu testen und die Reaktionsfähigkeit kontinuierlich zu verbessern.


3. Cybersicherheit und Datenschutz

IT-Grundschutz und neue Vorgaben wie die NIS2-Richtlinie müssen konsequent umgesetzt werden – insbesondere in der öffentlichen Verwaltung. Der Aufbau von Security Operations Centern (SOC) sowie die regelmäßige Schulung der Mitarbeitenden in Cyber-Hygiene sind zentrale Maßnahmen, um Angriffe abzuwehren und kritische Daten zu schützen.

Dabei darf es keine Ausnahmen geben: Finanzielle Engpässe oder fehlendes Fachpersonal werden häufig als Begründung angeführt, um notwendige Sicherheitsvorgaben zu umgehen – insbesondere im Verwaltungsbereich, in dem sehr sensible Daten von Bürger:innen liegen und staatliche Funktionsfähigkeit direkt erlebbar wird. Diese Haltung ist angesichts der wachsenden Bedrohungslage nicht länger tragbar.


4. KI und Innovation einsetzen

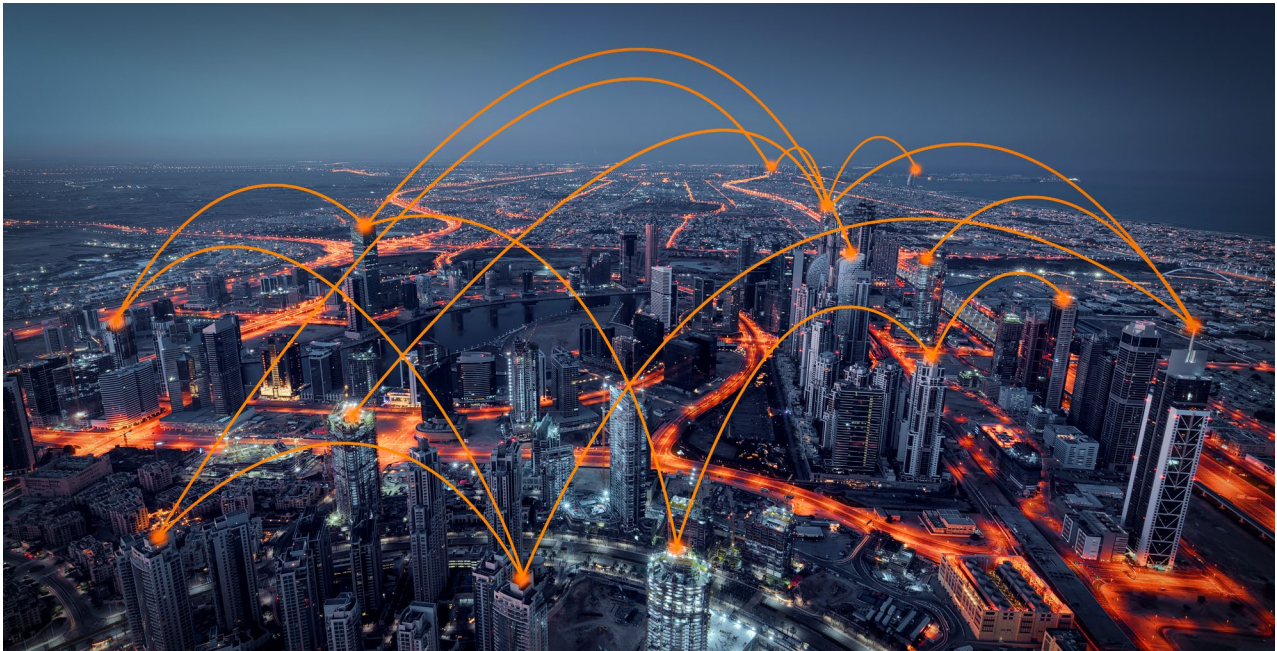
Die strategische Bedeutung von Daten muss stärker in den Fokus rücken – sowohl im Hinblick auf deren Schutz im Bereich Cybersicherheit als auch auf ihr Potenzial für eine vorausschauende Verwaltung. Künstliche Intelligenz (KI) kann dabei helfen, Anomalien frühzeitig zu erkennen (z. B. bei Cyberangriffen), Prozesse zu automatisieren und datenbasierte Entscheidungen zu verbessern sowie Personalressourcen zu schonen.

Gleichzeitig gilt es, die Innovationsfähigkeit der öffentlichen Verwaltung zu fördern, um technologische Entwicklungen frühzeitig zu identifizieren und nutzbar zu machen. Dafür braucht es neue Formen der Zusammenarbeit zwischen Staat, Wirtschaft und Wissenschaft. Pilotprojekte wie der GovTech-Campus oder das KI-Portal KIPITZ sollten gezielt unterstützt werden, um konkrete Use Cases für resilientere Verwaltungsservices zu entwickeln und zu skalieren.


5. Resiliente Führungs-, Organisations- und Fehlerkultur

Die technologische Welt ist zunehmend komplex und dynamisch – viele Herausforderungen lassen sich nur in einem iterativen Ansatz bewältigen. Daher braucht es eine agile Organisationskultur und eine spezielle Aufbauorganisation für den Krisenfall, in der Mitarbeitende ermutigt werden, Fehler offen anzusprechen und daraus zu lernen.

Führungskräfte sollten Querschnittskompetenzen fördern, bereichsübergreifend zusammenarbeiten und im Krisenfall klar und transparent kommunizieren. Resilienz ist kein einmaliges Ziel, sondern ein kontinuierlicher Verbesserungsprozess, der sich nur durch Lernbereitschaft und kulturellen Wandel dauerhaft verankern lässt.



1. Die Welt im Umbruch

Behörden sind Teil kritischer Infrastrukturen. Ihre Funktionsfähigkeit ist entscheidend für die Aufrechterhaltung der öffentlichen Sicherheit und staatlichen Ordnung. Die vergangenen Jahre haben gezeigt, dass die öffentliche Verwaltung in Deutschland gezielter auf Krisen vorbereitet sein muss, um auch unter extremen Bedingungen handlungsfähig zu bleiben.

Die COVID-19-Pandemie war auch ein Stresstest für staatliche Strukturen. Weitere Ereignisse wie das Hochwasser 2021 im Ahrtal, Sabotageakte auf die Bahn-Infrastruktur (z. B. 2022 in Norddeutschland), Angriffe auf Ostsee-Datenkabel oder Cyberattacken auf Behördenportale im Zuge geopolitischer Spannungen haben verdeutlicht, wie verwundbar digitale und physische Infrastrukturen sind. Die Verwundbarkeit der Souveränität und des Wertekanons demokratischer Staaten äußert sich sichtbar mit subtilen gesetzlichen Regelungen wie dem US-Cloud-Act, mit der Verpflichtung zur Herausgabe von Daten auf Anforderung staatlicher Einrichtungen. Solche hybriden Bedrohungen zeigen, dass Verwaltungen robust, flexibel und lernfähig sein müssen und dass föderale Schranken Reaktionsgeschwindigkeit kosten können.

Resilienz bedeutet hierbei mehr als klassische Gefahrenabwehr. Während Sicherheit meist auf das Verhindern von Schadensereignissen, etwa von Hackerangriffen, fokussiert und Krisenmanagement die Reaktion nach Eintritt eines Ereignisses beschreibt, geht Resilienz ganzheitlicher vor.

Resiliente Behörden:

- antizipieren Risiken früh,
- absorbieren Störungen bestmöglich und
- adaptieren sich agil an neue Gegebenheiten, um ihren staatlichen Auftrag weiterhin erfüllen zu können.

Ein einzelnes Rechenzentrum mit USV-Batterien aufzubauen, mag IT-Redundanz schaffen – aber echte Resilienz erfordert auch einen Plan B, falls Mitarbeitende oder Lieferant:innen ausfallen und die Fähigkeit, aus jeder Krise zu lernen und sich neu aufzustellen.

2. Deutschlands strukturelle Verwundbarkeiten

Trotz wirtschaftlicher und institutioneller Stärke offenbaren jüngste Krisen strukturelle Schwächen im deutschen Verwaltungssystem. Diese betreffen sowohl technische als auch organisatorische und kulturelle Grundlagen der Krisenbewältigung. Das Problem ist weniger das Fehlen einzelner Maßnahmen, sondern der Mangel an systemischer Verknüpfung, strategischer Klarheit und konsequenter Umsetzung.



Technologische Abhängigkeiten

Deutschland ist in zentralen Schlüsseltechnologien stark auf außereuropäische Anbieter angewiesen – etwa im Bereich Cloud-Computing, digitaler Plattformen oder künstlicher Intelligenz. Laut Bitkom (2025) nutzen viele deutsche Unternehmen Cloud-Dienste mit Anbietern außerhalb der EU. Dies limitiert die digitale Souveränität und erschwert eine wertebasierte Technologiegestaltung.



Mangel an Redundanz und Resilienz in kritischen Infrastrukturen

Hoher Effizienzdruck, Globalisierung und Sparzwänge haben dazu geführt, dass kritische Infrastrukturen häufig ohne ausreichende Puffer betrieben werden. Es fehlen robuste Redundanzsysteme, sektorübergreifende Notfallpläne und regelmäßige Stresstests/Übungen. Personalkapazitäten und operative Einsatzkonzepte werden aus Kostengründen oft nicht aufgebaut.



Zersplitterte Steuerung

In akuten Lagen zeigen sich die Grenzen föderaler und ministerieller Zuständigkeitsverteilungen – mit Abstimmungsproblemen, ineffizienten Abläufen und uneinheitlichem Krisenhandeln. Die Diskussion um Zuständigkeiten bei Drohnenüberflügen über militärischen Sperrbezirken verdeutlicht dies ebenso wie der Koordinierungsbedarf bei Naturkatastrophen (s. u. a. Ahrtalflut). Zwar benennt die Deutsche Resilienz-Strategie koordinierte Führungsstrukturen und gemeinsame Lagezentren als Ziel, doch klare Umsetzungsmechanismen fehlen häufig bzw. haben sie einen längeren Vorlauf, bis sie aktiviert werden.



Mangelnde Vernetzung und Kooperation

Eine wesentliche Schwachstelle ist die fehlende institutionalisierte Zusammenarbeit zwischen Behörden und Verwaltungsebenen. Daten und Informationen sind zwar häufig vorhanden, können aber nicht effektiv geteilt oder genutzt werden – sei es aus technischen, organisatorischen oder rechtlichen Gründen bzw. einer Kombination, die dafür sorgt, dass Informationen bestenfalls in Krisenlagen geteilt werden, jedoch nicht regulär und automatisiert. Doppelstrukturen entstehen, wenn vergleichbare Kapazitäten unabhängig voneinander aufgebaut werden. Stattdessen wäre ein vernetzter, kooperativer Ansatz effizienter: Durch abgestimmte Rollenverteilungen, gemeinsame Nutzung vorhandener Ressourcen und Daten sowie föderationsübergreifende Standards könnten Synergien geschaffen und die Resilienz insgesamt gestärkt werden.



Unzureichende Integration von Frühwarnung und Planung

Frühwarnsysteme existieren, sind jedoch selten systematisch in strategische Entscheidungsprozesse eingebunden. Der Mangel an vorausschauender Planung verhindert eine proaktive, risikoorientierte Steuerung – wie sie etwa im Sendai-Rahmenwerk der UN oder in Ländern wie Finnland vorgesehen ist. Eine übergreifende Datennutzung, etwa durch Open Data oder föderationsübergreifende Standards, ist bislang nur punktuell realisiert, somit bleiben Potenziale der Nutzung von Künstlicher Intelligenz zur Krisenfrüherkennung ungenutzt.



Kulturelle Faktoren

Resilienz ist auch eine Frage von Führung und Organisationskultur. Fehlende Fehlerkultur, mangelnde Verantwortungsübernahme, unklare Rollen und Verantwortlichkeiten sowie unzureichend ausgeprägte Lernprozesse behindern die Anpassungsfähigkeit.

3. Ein souveränes, widerstandsfähiges Deutschland

Resilienz heißt nicht nur, Krisen zu überstehen, sondern sich aktiv und vorausschauend auf Unsicherheiten einzustellen. Eine resiliente Gesellschaft erkennt Risiken früh, schützt kritische Strukturen proaktiv, bleibt im Ernstfall handlungsfähig und lernt aus Herausforderungen. Souveränität bedeutet dabei, unabhängig, selbstbestimmt und wertegeleitet zu handeln.



Ein widerstandsfähiges Deutschland ist in der Lage,

- strategische Risiken frühzeitig zu erkennen und zu bewerten,
- technologische Kernkompetenzen eigenständig zu sichern und weiterzuentwickeln,
- kritische Infrastrukturen physisch wie digital zu schützen,
- Institutionen agil und anpassungsfähig zu steuern,
- sowie Vertrauen durch transparente Kommunikation und Beteiligung zu stärken.

Diese Vision beruht auf vier zentralen Resilienz-Dimensionen:



Politisch-
institutionell



Techno-
logisch



Gesell-
schaftlich



Organisa-
torisch

4. Fünf strategische Bausteine staatlicher Souveränität und Resilienz

Ein souveräner und widerstandsfähiger Staat braucht belastbare Strukturen, klare Zuständigkeiten und praxistaugliche Instrumente. Für Behörden bedeutet das nicht, alles selbst entwickeln zu müssen – aber Verantwortung in der Umsetzung zu übernehmen, aktiv an der strategischen Steuerung mitzuwirken und Resilienz als Daueraufgabe zu integrieren.

Aufbauend auf den strategischen Vorgaben lassen sich fünf zentrale Handlungsfelder bzw. Bausteine definieren, aus denen sich eine resiliente Verwaltung zusammensetzt.

Diese Bausteine sind eng miteinander verzahnt und sollten ganzheitlich entwickelt werden:

Strategischer Rahmen: Integrierte Resilienz-Strategie



Technologische Souveränität und resiliente Infrastruktur:

Aufbau eigener digitaler Kompetenzen, souveräner Cloud- sowie KI-Infrastrukturen und Investitionen in den Schutz kritischer Systeme und Versorgungslinien.



Frühwarnung und Krisenmanagement:

Etablierung resilienter BCM-Strukturen, aktuelle Krisenpläne und integrierte Kommunikation.



Cybersicherheit und Datenschutz:

Umsetzung und Verankerung präventiver Schutzmaßnahmen und Standards.



KI und Innovation einsetzen:

Kritische Technologien werden mit eigenem Know-how entwickelt, um Abhängigkeiten zu vermeiden.



Resiliente Führungs- und Fehlerkultur:

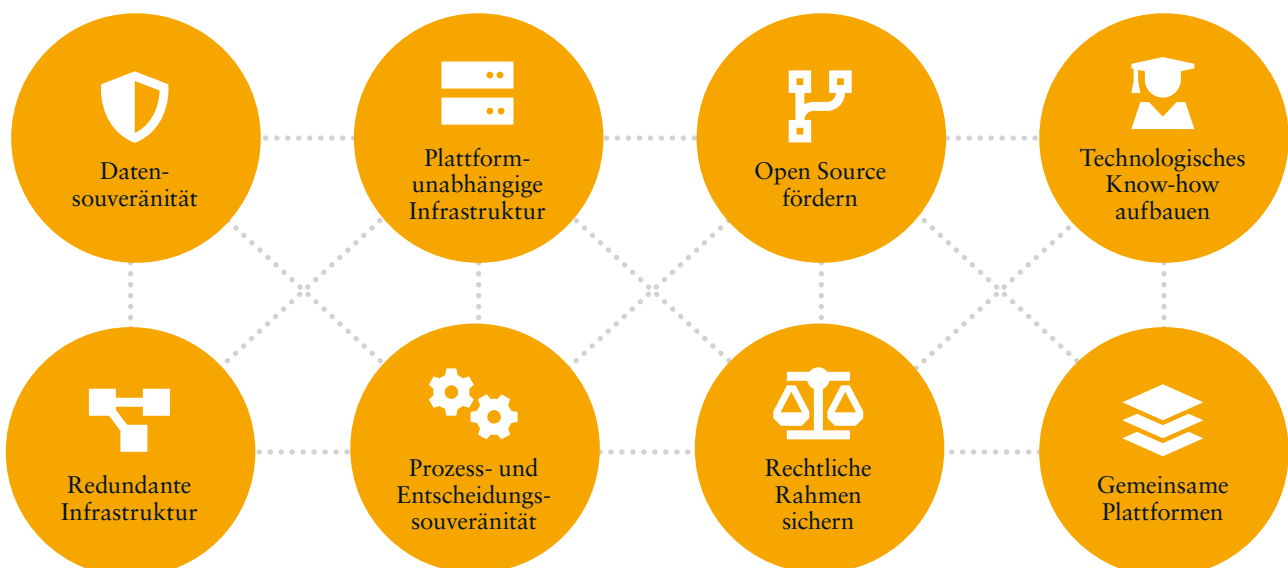
Qualifizierung von Entscheider:innen, klare Zuständigkeiten, integrierte Steuerung.

Baustein 1: Technologische Souveränität und resiliente Infrastrukturen

Technologische Souveränität bedeutet, dass der Staat unabhängig und selbstbestimmt in der digitalen Welt agieren kann. Ziel ist es, Abhängigkeiten systematisch zu reduzieren und kritische Technologien eigenständig oder im europäischen Verbund zu kontrollieren.

Kernansätze für Behörden:

- Datensouveränität stärken:**
 DSGVO-konforme Kontrolle über Speicherung, Verarbeitung und Nutzung sensibler Daten sicherstellen, um Abhängigkeiten von externen Dienstleistern zu reduzieren.
- Plattform- und Infrastruktursouveränität:**
 Digitale Dienste und IT-Infrastrukturen so betreiben, dass ein Lock-in zu Hyperscalern vermieden wird und eigene updatefähige souveräne Cloud-Lösungen genutzt werden.
- Softwaresouveränität durch Open Source:**
 Nutzung und gezielte Förderung offener Software sowie offener Standards zur Sicherstellung von Interoperabilität und Anpassungsfähigkeit (z.B. Umstieg auf LibreOffice in Schleswig-Holstein).
- Eigenständige Technologiekompetenz:**
 Aufbau und Entwicklung von eigenem Know-how im Umgang mit kritischen Technologien, um Abhängigkeiten langfristig zu vermeiden.
- Resiliente und redundante Infrastruktur:**
 Aufbau geografisch verteilter, redundanter Systeme wie Rechenzentren, sichere Backups und alternative Kommunikationswege (Satellit, Funk), um im Krisenfall handlungsfähig zu bleiben.
- Prozess- und Entscheidungssouveränität sichern:**
 Digitale Abläufe stets intern steuerbar gestalten und menschliche Aufsicht gewährleisten, um die Kontrolle über Prozesse und Entscheidungen zu behalten.
- Rechtliche Souveränität gewährleisten:**
 Digitale Lösungen konsequent deutschem bzw. EU-Recht unterwerfen und diese gegen ausländische Zugriffe absichern.
- Gemeinsame Plattformen etablieren:**
 Einheitliche IT-Architekturen und gemeinsame Basisdienste schaffen (z.B. Deutschland-Stack, ID-Management, Formulare Systeme), um Behörden interoperable und effiziente Lösungen zu bieten und gegenseitige Unterstützung zu erleichtern.



Baustein 2: Frühwarnsysteme und Krisenmanagement

Vorbereitung ist zentral: Je früher eine Behörde Gefahren erkennt und je besser sie vorbereitet ist, desto geringer der Schaden und schneller die Wiederherstellung. Dieser Baustein umfasst technische und organisatorische Frühwarnsysteme sowie professionelles Krisenmanagement.

Kernaspekte:

- Frühwarnung durch Monitoring:** Krisen kündigen sich oft an – etwa durch Wetterwarnungen, IT-Anomalien oder Personalausfälle. Monitoring-Systeme wie SIEM-Lösungen analysieren Logdaten automatisiert und melden Auffälligkeiten. Für physische Risiken stehen Systeme wie Cell Broadcast oder Warn-Apps (z. B. NINA) bereit. Wichtig ist die interne Weiterleitung von Warnungen über verlässliche und bestenfalls automatisierte Kommunikationskanäle.
- Lagebilder und Informationsaustausch:** Übergreifende, integrierte Lagebilder fehlen oft – obwohl viele Datenquellen existieren. Bund und Länder bauen Systeme wie das Digitale Lagebild Bevölkerungsschutz auf. Behörden sollten vorhandene (offene) Informationen systematisch auswerten und auch die Einbindung ziviler KRITIS-Lagebilder prüfen, z. B. Drohnenlagebilder an Flughäfen. Eine feste Funktion oder Rolle zur Beobachtung und Bewertung von Lageinformationen kann dies leisten – ohne neue Strukturen schaffen zu müssen.
- Krisenpläne und -stäbe:** Trotz Prävention treten Krisen ein. Jede Behörde benötigt aktuelle Krisenpläne: Wer übernimmt welche Rolle? Wo trifft man sich? Was sind erste Maßnahmen? Diese Pläne müssen durch regelmäßige Übungen – mindestens einmal jährlich – erprobt werden. Szenarien wie IT-Ausfall oder Stromunterbrechung eignen sich zur Prüfung der Abläufe. Auch externe Partner wie Polizei oder IT-Dienstleister sollten einbezogen werden.
- Kommunikation als integraler Bestandteil des Krisenmanagements:** Wirksames Krisenmanagement braucht eine durchdachte Kommunikationsstrategie – vor, während und nach der Krise. Kommunikation steuert Wahrnehmung, schafft Vertrauen und hält handlungsfähig. Dabei ist klare Kommunikation entscheidend. Intern: schnell und transparent über sichere Kanäle informieren. Extern: abgestimmte Botschaften an Öffentlichkeit und Medien senden. Eine Krisen-Stakeholderanalyse, vorbereitete Kommunikationspläne und Media-Trainings helfen, in Ausnahmesituationen souverän zu agieren.
- Nachbereitung und Lernen:** Jede Krise bietet Lernpotenzial. Systematische Auswertung, Dokumentation und Umsetzung der Erkenntnisse (Lessons Learned) stärken langfristig die Resilienz. Beispiel: Die Einführung von Cell Broadcast nach dem Warntag 2020 oder der Ausbau der Sireneninfrastruktur nach der Flut 2021 zeigen, wie konsequente Nachbereitung Schwächen beheben kann. Krisenmanagement ist kein linearer Prozess, sondern zyklisch: Was aus einer Krise gelernt wird, fließt unmittelbar in die Vorbereitung auf zukünftige Ereignisse ein – organisatorisch, technisch und kommunikativ. So entsteht mit jeder durchlebten Krise ein robusteres System.



Kreislauf für Resilienz

Baustein 3: Cybersicherheit und Datenschutz

Cybersicherheit ist eine Grundvoraussetzung für resiliente Verwaltung. Fällt zentrale IT aus oder werden Daten kompromittiert, steht die Handlungsfähigkeit der Behörde auf dem Spiel. Die Zunahme schwerer Cyberangriffe – von Verschlüsselungstrojanern in Kommunen bis zu Angriffen auf Regierungsnetze – zeigt: Keine Resilienz ohne Security.

Kernfelder für Behörden:

- **IT-Grundschutz und Basissicherheit:** Der BSI-Grundschutz bietet konkrete Maßnahmen, um IT-Systeme zu sichern – etwa Segmentierung, Zugriffssteuerung, Verschlüsselung, Patch-Management, Backups und Multi-Faktor-Authentifizierung. Interne Audits und Penetrationstests decken Schwachstellen auf. Die Umsetzung der NIS-2-Richtlinie, deren deutsche Fassung (NIS2UmsuCG) sich aktuell in Verzug befindet, wird künftig deutlich höhere Anforderungen an IT-Sicherheit und Meldepflichten (z. B. binnen 24 Stunden) stellen. Behörden sollten sich frühzeitig auf diese Standards vorbereiten.
- **Security Operations Center (SOC):** Größere Verwaltungen oder IT-Dienstleister sollten ein SOC betreiben – eine Einheit, die Systeme überwacht, Vorfälle erkennt und schnell reagiert. Für kleinere Behörden bieten sich gemeinsame SOC-Strukturen auf Landes- oder Kreisebene an. Entscheidend sind klare Zuständigkeiten und Notfallpläne (Incident Response). Kooperationen mit dem BSI oder externen Sicherheitsfirmen ermöglichen schnelle Hilfe im Ernstfall.
- **Sensibilisierung und Schulung:** Viele Angriffe gelingen über Mitarbeitende. Daher sind kontinuierliche Schulungen zentral – z. B. E-Learnings, Phishing-Tests oder Sicherheitskampagnen. Ziel ist eine Sicherheitskultur, in der Mitarbeitende wachsam agieren und Risiken melden.
- **Datenschutz und Notfallzugriff:** Datenschutz muss auch in Krisen gelten. Vorab sollten Regelungen definiert werden, etwa welche Daten im Krisenfall genutzt werden dürfen. Auch die Verarbeitung von Cloud-Backups im Ausland erfordert datenschutzkonforme Vereinbarungen (Stichwort DSGVO, Schrems II).
- **Integration physischer und digitaler Sicherheit:** Bedrohungen sind zunehmend hybrid. Sicherheitskonzepte müssen physische (z. B. Zutrittskontrolle) und digitale Aspekte (z. B. Admin-Zugriffe) gemeinsam adressieren. Alarmierungen sollten beide Bereiche berücksichtigen, und gemeinsame Übungen zwischen IT- und Objektschutzteams stärken das Zusammenwirken.



„Keine Resilienz ohne Security – Cybersicherheit ist die Grundvoraussetzung für eine handlungsfähige Verwaltung.“

Baustein 4: KI-Einsatz und datengetriebene Innovationen

Künstliche Intelligenz (KI) und datenbasierte Technologien bieten große Chancen für die Resilienz öffentlicher Verwaltung – etwa durch Frühwarnung, Automatisierung und Entscheidungsunterstützung. Gleichzeitig erfordern sie eine verantwortungsvolle Nutzung, um Risiken wie Intransparenz oder Abhängigkeit zu vermeiden.

Wichtige Potenziale im Überblick:

- Frühzeitige Umsetzung eigener Projekte:**
 Behörden sollten frühzeitig eigene Daten- und KI-Projekte starten, um praktische Erfahrungen mit der Technologie und datengetriebenen Analysen zu sammeln. Förderprogramme von Bund und Ländern bieten gute Einstiegsmöglichkeiten.
- Frühwarnung mit Predictive Analytics:**
 KI kann Muster in großen Datenmengen erkennen, die Menschen entgehen. Sie analysiert z. B. soziale Medien, Nachrichten oder Netzwerkverkehr, um Krisenindikatoren frühzeitig zu erkennen – von Cyberangriffen bis zu Lieferengpässen. Anomalie-Erkennung unterstützt dabei insbesondere die IT-Sicherheit.
- Automatisierung für Entlastung:**
 KI-gestützte Systeme wie Chatbots oder RPA-Lösungen übernehmen Routineaufgaben (z. B. E-Mail-Zu-/Verteilung zu den Stäben, Formularbearbeitung, Zusammenfassung komplexer Lagedokumente), entlasten das Personal und sichern Grundfunktionen – vor allem bei hohen Ausfallraten. Voraussetzung sind stabile, regelmäßig aktualisierte Systeme.
- KI-gestütztes Wissensmanagement:** Digitale Assistenten können im Krisenfall schnell relevante Informationen liefern – wie Einsatzberichte, Rechtsgrundlagen, Checklisten. Erste Projekte wie das KI-Portal KIPITZ bieten Raum, eigene Anwendungen zu erproben und auszubauen.
- Risikobewusste Nutzung und Governance:** KI darf nicht blind übernommen werden. Verwaltungen brauchen erklärbare, nachvollziehbare und rechts-sichere Systeme, Notfallpläne für technische Ausfälle, ein sauberes Datenmanagement sowie geschultes Personal („human-in-the-loop“). Nur so bleibt die Entscheidungshoheit gewahrt.
- Vernetzung und Kollaboration:** Viele relevante Daten sind vorhanden – oft scheitert die Nutzung an fehlendem Austausch zwischen Behörden und auch an mangelnden Ressourcen zur Aufbereitung von Daten für einen Austausch. Doppelte Strukturen, isolierte Datenräume und parallele Projektentwicklungen bremsen das Potenzial datengetriebener Innovationen. Resiliente KI-Strategien erfordern ein kooperatives Vorgehen: gemeinsame Datenräume, standardisierte Schnittstellen und koordinierte Entwicklungsinitiativen. Behörden sollten Silos aufbrechen und in ressort- und ebenenübergreifende Zusammenarbeit investieren.

— KI-Basierte Mailverteilung im Krisenfall —



Baustein 5: Resiliente Führungs-, Organisations- und Fehlerkultur

Technik und Prozesse allein genügen nicht – Resilienz steht und fällt mit der Organisationskultur. Starre Hierarchien, Silodenken oder Verantwortungsdiffusion behindern Anpassungsfähigkeit. Eine resiliente Verwaltung braucht ein Umfeld, das Lernen, Zusammenarbeit und Eigenverantwortung fördert.

Wichtige Elemente:

- **Agilität und Lernbereitschaft:** Führungskräfte sollten flexibel agieren, Mitarbeitende ermutigen, neue Ideen einzubringen, und Veränderungen als Chance begreifen. Eine Kultur kontinuierlicher Verbesserung stärkt die Krisenfestigkeit.
- **Changemanagement:** Veränderung ist kein Ausnahmezustand mehr – sie ist Normalität geworden. Ob Digitalisierungsvorhaben, Organisationsreformen, neue Fachverfahren oder gesetzliche Vorgaben: Resiliente Verwaltungen brauchen die Fähigkeit, Veränderungsprozesse vorausschauend, systematisch und partizipativ zu gestalten, zu kommunizieren und zu monitoren. Changemanagement wird zur Kernkompetenz krisenfester Organisationen.
- **Positive Fehlerkultur:** Fehler müssen offen benannt und analysiert werden dürfen – ohne Angst vor Sanktionen. Statt Schuldzuweisung geht es um Lernen. Formate wie regelmäßige Retrospektiven helfen, Erfahrungen systematisch auszuwerten.
- **Interdisziplinarität und Teamwork:** Resilienz entsteht durch Zusammenarbeit über Abteilungsgrenzen hinweg. Gemischte Teams aus IT, Fachbereichen und Stabsstellen fördern Perspektivenvielfalt und brechen Silos auf. Jobrotation oder Hospitation unterstützen diesen Wandel.
- **Führung und Empowerment:** Gute Führungskräfte schaffen Klarheit, ermöglichen Beteiligung und achten auf Belastung. Sie handeln in Krisen entschlossen, beziehen aber Wissen aller Ebenen ein und befähigen. Schulungen in Krisenführung und Stressmanagement sind hilfreich.
- **Wissensmanagement:** Wissen muss dokumentiert, zugänglich und übertragbar sein. Vertretungsregelungen und ein gepflegtes Intranet mit Notfallressourcen sichern den Betrieb bei Personalausfall. Investitionen in Dokumentation zahlen sich im Ernstfall aus.



Fazit: Resilienz beginnt heute – und in Ihrer Organisation

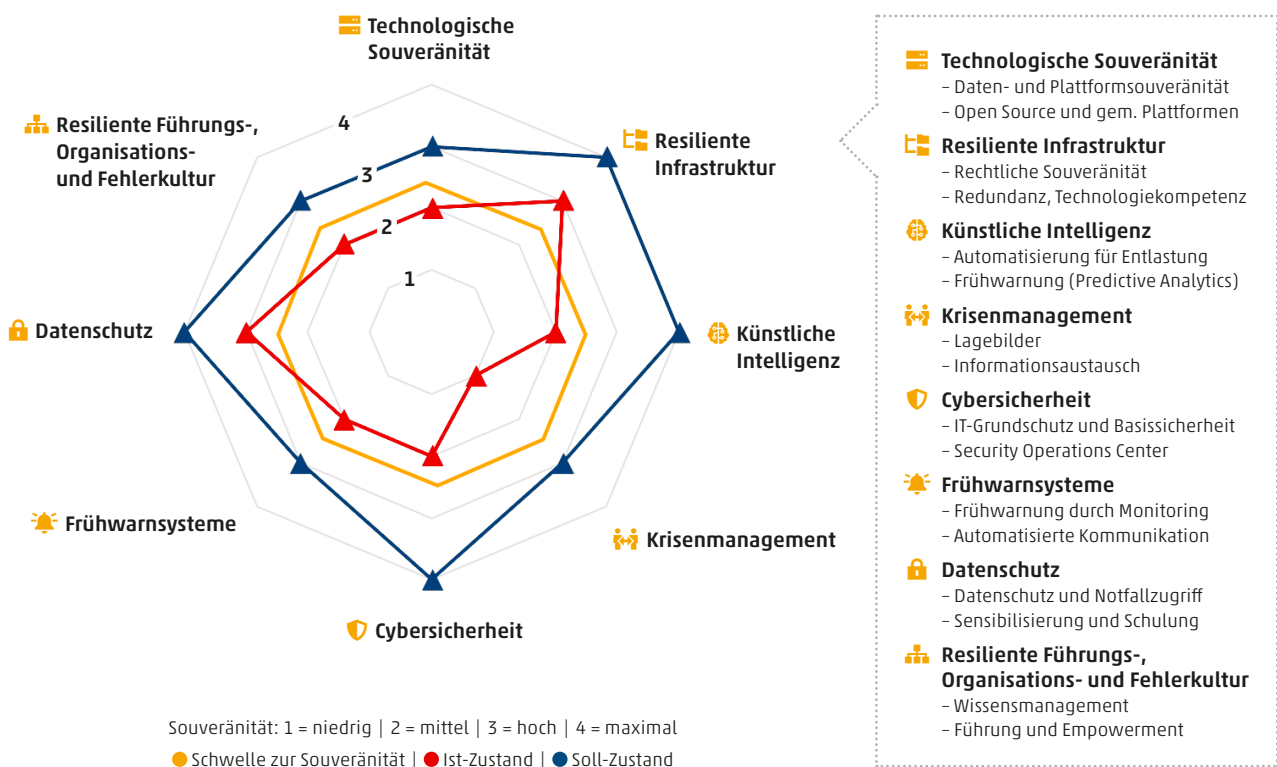
Resilienz in der öffentlichen Verwaltung ist kein Schlagwort, sondern eine notwendige Antwort auf eine Welt im permanenten Wandel. Pandemien, Cyberangriffe, Naturkatastrophen und technologische Umbrüche machen auch vor Ämtern nicht halt. Verwaltungen in Deutschland bringen vieles mit, worauf sich aufbauen lässt – qualifiziertes Personal, funktionierende Strukturen und bewährte Sicherheitsstandards.

Mit den in diesem Whitepaper skizzierten Bausteinen liegt ein praxisnaher Fahrplan vor, um diese Grundlagen gezielt weiterzuentwickeln. Entscheidend ist der Perspektivwechsel: nicht nur reagieren, sondern vorausdenken und aktiv vorsorgen. Resilienz bedeutet, in der Lage zu bleiben, zu steuern – selbst unter Druck.

Wir hoffen, Ihnen mit diesem Leitfaden konkrete Impulse gegeben zu haben. Jede Organisation kann sofort beginnen – nicht perfekt, aber entschlossen. Wichtig ist, das Thema zur Chef:innensache zu machen und Schritt für Schritt Fortschritte zu erzielen.

Am Ende stärkt Resilienz nicht nur die Verwaltung selbst, sondern auch das Vertrauen der Bürger:innen: Sie können sich darauf verlassen, dass der Staat auch in schwierigen Zeiten handlungsfähig bleibt. Mit klarem Ziel, gemeinsamer Verantwortung und dem Mut zur Veränderung kann die öffentliche Verwaltung in Deutschland zum Maßstab für Widerstandsfähigkeit werden – bereit für das, was kommt.

Integrierte Reifegrad-Analyse für Ihre Verwaltung



Unsere Unterstützung für Sie

Die Umsetzung der beschriebenen Maßnahmen erfordert Erfahrung in Organisationsentwicklung, Technologie und Changemanagement. Hier steht Ihnen Infora als zuverlässiger Partner zur Seite.

Wir verfügen über langjährige Expertise in der öffentlichen Verwaltung und bieten aus einer Hand:

■ **Strategieworkshops und Reifegradanalysen:**

Wir analysieren den Resilienz-Reifegrad Ihrer Behörde und entwickeln gemeinsam einen maßgeschneiderten Fahrplan. In moderierten Workshops identifizieren wir Handlungsbedarfe und priorisieren nächste Schritte.

- #### ■ **Technologie und Projektkompetenz:** Ob Einführung von Sicherheitslösungen, Aufbau von Cloud-Infrastrukturen und Datenräumen, die Einführung von (VS-NfD) Sicherheitslösungen- und Kommunikationssysteme oder Integration von KI – unsere Fachleute unterstützen von der Konzeption bis zur Umsetzung. Wir kennen die besonderen Anforderungen des öffentlichen Sektors (z. B. BSI-Grundschutz, EU-Normen) und sorgen für konforme, zukunftssichere Lösungen. Weitere Leistungen sind der Aufbau, die Integration und Vernetzung von Lagebildern.

- #### ■ **Schulungen und Kulturentwicklung:** Unsere Berater:innen helfen Ihnen, Resilienz in der Organisation zu verankern. Wir bieten Mitarbeiterschulungen zu Krisenmanagement und IT-Sicherheit sowie Begleitung von Change-Prozessen, um eine offene Fehler- und Lernkultur zu fördern.

■ **KI-Entwicklung und Innovation:**

Gemeinsam identifizieren wir Anwendungsfälle für neue Technologien (etwa Chatbots oder Data Analytics), die Ihre Verwaltungsleistung resilienter machen. In Innovationsworkshops und Pilotprojekten bringen wir moderne Tools praxisnah zum Einsatz und setzen KI-Assistenzsysteme für Sie um.

■ **Warum mit uns?**

Uns verbindet strategische Beratung mit technischer Umsetzungskompetenz – ein Ansprechpartner für alle Dimensionen der Resilienz. Wir sind vertraut mit den Strukturen von Bund, Ländern und Kommunen und arbeiten agil und zielorientiert. Unser Angebot passen wir flexibel an Ihre Bedürfnisse an: von kurzen Impulsen (z. B. einem Resilienz-Check in 2 Tagen) bis zur umfassenden Begleitung großer Vorhaben.

■ **Nehmen Sie Kontakt auf, um mehr zu erfahren.**

Gemeinsam machen wir Ihre Behörde fit und krisenfest für die Zukunft – damit Sie auch im Sturm sicher navigieren können.



Quellen und Verweise

- **Bitkom (2025): Cloud Monitor 2025.**
🔗 Online verfügbar unter: <https://www.bitkom.org/sites/main/files/2025-06/bitkom-pressekonferenz-cloud-report-2025-praesentation.pdf>
- **Bundesministerium des Innern und für Heimat (BMI) (2021): Cyber-Sicherheitsstrategie für Deutschland.**
🔗 Online verfügbar unter: <https://www.bmi.bund.de>
- **Bundesministerium des Innern und für Heimat (BMI) (2022): Digitalstrategie der Bundesregierung.**
🔗 Online verfügbar unter: <https://www.digitalstrategie-deutschland.de>
- **Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium und BSI-Standards.**
🔗 Online verfügbar unter: <https://www.bsi.bund.de>
- **Bundesregierung (2023): Nationale Sicherheitsstrategie der Bundesrepublik Deutschland.**
🔗 Online verfügbar unter: <https://www.bundesregierung.de>
- **eGovernment Computing (diverse Jahre): Fachbeiträge zu Verwaltung, Führung und Fehlerkultur.**
🔗 Online verfügbar unter: <https://www.egovernment.de>
- **Europäische Union (2022): Richtlinie (EU) 2022/2555 (NIS-2).**
🔗 Online verfügbar unter: <https://eur-lex.europa.eu>
- **Gaia-X Hub Deutschland: Informationen zur Domäne Öffentlicher Sektor und Pilotprojekte.**
🔗 Online verfügbar unter: <https://gaia-x-hub.de>
- **International Organization for Standardization (ISO): ISO 22301 – Business Continuity Management Systems.**
🔗 Online verfügbar unter: <https://www.iso.org>
- **Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (2023): Building Resilient Public Administration Post-COVID-19.**
🔗 Online verfügbar unter: <https://www.oecd.org>
- **OpenKRITIS.de: Informationsplattform zu Kritischen Infrastrukturen und Gesetzesinitiativen.**
🔗 Online verfügbar unter: <https://openkritis.de>
- **United Nations Office for Disaster Risk Reduction (UNDRR) (2015): Sendai Framework for Disaster Risk Reduction 2015–2030.**
🔗 Online verfügbar unter: <https://www.undrr.org>
- **Trade with Estonia: Digitale Verwaltung, Cyber-Resilienz und Datenkontinuität in Estland.**
🔗 Online verfügbar unter: <https://tradewithestonia.com>
- **Zentrum für Öffentliche Sicherheit (ZOES): Grünbuch ZMZ 4.0.**
🔗 Online verfügbar unter: <https://zoes-bund.de>

Anhang: Praktische Handlungsempfehlungen mit Checkliste

Die nachfolgenden Handlungsempfehlungen bieten Behörden konkrete und praxisorientierte Schritte, um Resilienz nachhaltig und systematisch zu verankern. Dabei werden kurzfristige, mittelfristige und langfristige Maßnahmen unterschieden, um eine stufenweise Umsetzung zu ermöglichen.



Kurzfristige Maßnahmen (0–12 Monate)

- Bestandsaufnahme: Sofort einen Resilienz-Check durchführen, Sicherheitskonzepte erfassen, Lücken identifizieren und Verantwortlichkeiten festlegen.
- Awareness: Frühzeitig kommunizieren, dass Resilienz Chefsache ist; erste Workshops zu Cyberhygiene oder Krisenmanagement umsetzen.
- Notfallkommunikation: Kontaktlisten und Alarmierungswege (SMS, Telefonketten) einrichten und regelmäßig testen.
- BCM: Einfache Notfallanweisungen für zentrale Prozesse erstellen und auf Vorlagen von BSI oder BBK zurückgreifen.
- IT-Sofortmaßnahmen: Kritische Sicherheitslücken schließen und eine IT-Taskforce einsetzen.
- Netzwerke: Eigene Netzwerke aufbauen oder bestehenden Initiativen beitreten, um Wissen und Ressourcen zu sichern.



Mittelfristige Maßnahmen (1–3 Jahre)

- Resilienz-Strategie: Eine verbindliche Strategie entwickeln und mithilfe eines Reifegradmodells Ziele regelmäßig prüfen.
- Infrastruktur: Investitionen in redundante Rechenzentren, Cloud- und Datenraumlösungen planen und umsetzen.
- Organisation: Resilienz-Ausschüsse oder Managementrollen etablieren, Resilienz-Checks in Projekten verankern.
- Personal: Schulungen in Krisenmanagement und IT-Sicherheit durchführen, zusätzliches Fachpersonal einstellen.
- Digitale Werkzeuge: Software einführen, die Resilienzprozesse unterstützt und ortsunabhängigen Zugriff ermöglicht.
- Innovation: Pilotprojekte umsetzen und auswerten.
- Partnerschaften: Kooperationen mit Behörden und Dienstleistern formal absichern.



Langfristige Maßnahmen (über 3 Jahre)

- Strategische Verankerung: Resilienz dauerhaft in Planung und Budget aufnehmen.
- Kontinuierliche Verbesserung: Regelmäßige Audits durchführen und Strategien anpassen, um auf neue Risiken vorbereitet zu sein.
- Technologie-Scanning: Entwicklungen beobachten und frühzeitig Maßnahmen ableiten.
- Kollaborative Resilienz: Übergreifende Kooperationen wie gemeinsame Rechenzentren oder europäische Projekte langfristig aufbauen und pflegen.
- Kulturelle Verankerung: Einen nachhaltigen Kulturwandel anstreben, um Agilität und Anpassungsfähigkeit zu fördern – durch kontinuierliche Evaluation, eine positive Fehler- und Führungskultur sowie interdisziplinäre Zusammenarbeit.

Gerne begleiten und unterstützen wir Sie und Ihre Organisation in diesem Prozess.

Abkürzungsverzeichnis

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	KRITIS	Kritische Infrastrukturen
BSI	Bundesamt für Sicherheit in der Informationstechnik	NIS2	EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau
CERT	Computer Emergency Response Team	OZG	Onlinezugangsgesetz
DSGVO	Datenschutz-Grundverordnung	RPA	Robotic Process Automation
EfA	Einer für Alle (OZG-Prinzip)	SIEM	Security Information and Event Management
IT	Informationstechnologie	SOC	Security Operations Center
IT-SiG	IT-Sicherheitsgesetz	UN	Vereinte Nationen (United Nations)
KI	Künstliche Intelligenz	VPN	Virtual Private Network

Glossar

Agilität: Die Fähigkeit einer Organisation, flexibel, anpassungsfähig und schnell auf Veränderungen zu reagieren – insbesondere in unsicheren oder dynamischen Lagen.

Anomalieerkennung: Technologiebasierte Methode zur Erkennung von Abweichungen im normalen Daten- oder Systemverhalten. Dient z. B. zur Früherkennung von Cyberangriffen.

Build Back Better: Ansatz, nach einer Krise nicht nur den Ursprungszustand wiederherzustellen, sondern Systeme robuster, nachhaltiger und zukunftsfähiger auszubauen.

Cybersicherheit: Schutz von IT-Systemen, Netzwerken und Daten vor digitalen Angriffen, Ausfällen oder unbefugtem Zugriff.

Fehlerkultur: Organisationaler Umgang mit Fehlern, der Offenheit, Lernen und konstruktive Verbesserung statt Schuldzuweisung in den Mittelpunkt stellt.

Frühwarnsysteme: Mechanismen und Technologien, mit denen Risiken und Krisen frühzeitig erkannt werden können – z. B. durch Monitoring, Sensorik oder Datenanalyse.

Kritische Infrastrukturen (KRITIS): Systeme und Einrichtungen, deren Ausfall gravierende Folgen für die Gesellschaft hätte – z. B. Stromversorgung, Wasser, Gesundheitswesen oder Verwaltung.

Künstliche Intelligenz (KI): Technologien, die menschliches Denken imitieren – etwa durch Mustererkennung, Sprachverarbeitung oder automatisierte Entscheidungsunterstützung.

NIS2-Richtlinie: EU-Richtlinie zur Stärkung der Cybersicherheit in kritischen und wichtigen Einrichtungen, einschließlich vieler öffentlicher Stellen.

Predictive Analytics: Datengestützte Methode zur Vorhersage zukünftiger Ereignisse auf Basis historischer Muster – z. B. zur Erkennung von Versorgungsengpässen oder Risiken.

Resilienz: Fähigkeit von Organisationen, Systeme und Gesellschaften, Krisen nicht nur zu überstehen, sondern gestärkt daraus hervorzugehen.

Security Operations Center (SOC): Einheit innerhalb oder für eine Organisation, die Sicherheitsvorfälle erkennt, bewertet und koordiniert darauf reagiert.

Verwaltungsmodernisierung: Prozess der strukturellen, digitalen und kulturellen Weiterentwicklung öffentlicher Verwaltungen, um effizienter, nutzerorientierter und krisenfester zu arbeiten.

Vorausschau (Foresight): Strategisches Instrument zur frühzeitigen Erkennung gesellschaftlicher, technologischer oder sicherheitsrelevanter Entwicklungen.

Ihre Ansprechpersonen



Carsten Krinke
Partner
Infora GmbH
carsten.krinke@infora.de



Taner Ünalgan
Senior Consultant
Infora GmbH
taner.uenalgan@infora.de



Thomas Kühnen
Senior Sales Manager
Materna TMT GmbH
thomas.kuehnen@materna.group



Stephan Ursuleac
Lead Business Development Safety & Defense
Materna Information & Communications SE
stephan.ursuleac@materna.group

So erreichen Sie uns:

Infora GmbH
Konrad-Adenauer-Straße 13
50996 Köln
Tel.: +49 221 - 935 05 - 00
E-Mail: info@infora.de
www.infora.de

Materna Information &
Communications SE
Robert-Schuman-Straße 20
44263 Dortmund
Tel. +49 231 - 5599 - 00
E-Mail: sales@materna.de
www.materna.de

Materna TMT
Robert-Schuman-Straße 20
44263 Dortmund
Tel. +49 231 - 55 99 - 550
E-Mail: info-tmt@materna.group
www.materna-tmt.de