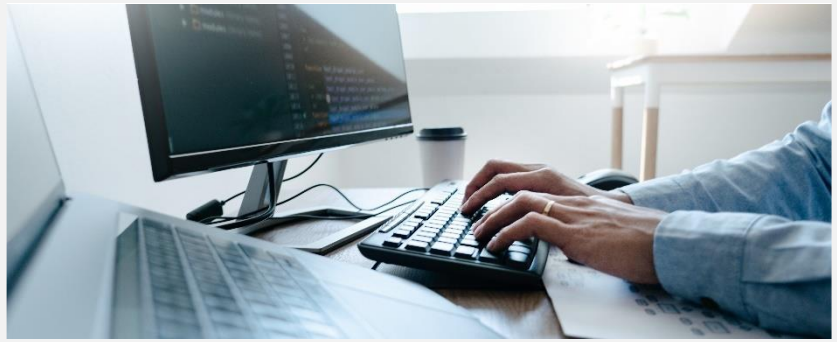
# Welche Lessons learned gibt es aus Umsetzungen vom IT-Sicherheitsgesetz 2.0?



All for One Group – Mittelstandsforum 2022

Kent Andersson, ausecus GmbH

# Agenda

- ausecus
- IT-Sicherheitsgesetz 2.0
- Lessons learned Umsetzungen
- Zusammenfassung

ausecus.

- Langjährige praktische Erfahrung in der Leit- und Fernwirktechnik
  - Gründung 2012
  - > 100 ISMS Einführungen
- Klarer Fokus auf Informations-, IT- und Netzwerksicherheit bei KRITIS-Betreibern
- Systeme zur Angriffserkennung als Dienstleistung

# Mit wem arbeiten wir zusammen?

# ausecus.Leistungen

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

## Beratung

**ISMS**
(Sektorspezifisch)

**ISB**
(Informationssicherheits-beauftragter)

**Interne Audits**

**Begleitung Zertifizierungsaudits**

**IT-Sicherheitscheck**
(Organisatorische GAP Analyse)

**ISMS Praxis Workshop / ISMS Awareness Training**

**Business Continuity Management**
(BCM)

**ISMS Software**
(Einführung und Betrieb)

**BCM Software**
(Einführung und Betrieb)

## Netzwerksicherheit

**KRITIS Defender**
System zur Angriffserkennung

**Penetrationstests**

**Analyse Netzwerksicherheit**
(Technische GAP Analyse)

# Zeitachse gesetzliche Anforderungen an Kritische Infrastrukturen

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

**IT-Sicherheitsgesetz 1.0**

Juli 2015

**BSI-KritisV Korb 1**

Mai 2016

**BSI-KritisV Korb 2**

Juni 2017

**Freigabe B3S Wasser/ Abwasser**

Sept. 2017

**IT-Sicherheitsgesetz 2.0**

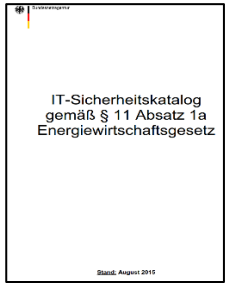
Mai 2021

**3. BSI-KritisV**

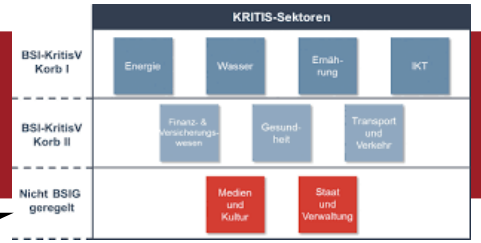
Q3 2022


Veröffent-lichung

August 2015

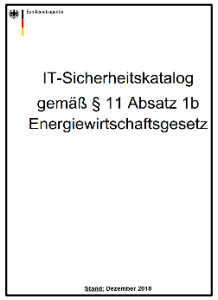



**Strom und Gas**




Veröffent-lichung

Dezember 2018




**Erzeugungsanlagen**

**Konkretisierungen:**
**- Schwellenwert MHKWs**
**- Unternehmen im besonderen öffentlichen Interesse**

# Schwerpunkte ITSiG 2.0

- Verpflichtung für KRITIS-Betreiber gemäß BSIG § 8a sowie EnWG § 11 Abs 1d/1e zum Einsatz von Systemen zur Angriffserkennung und organisatorische Einbindung der unterstützenden Prozesse hierzu.

- Einführung eines neuen KRITIS-Sektors „Siedlungsabfallentsorgung“ als KRITIS-Betreiber.

- Verpflichtung von Mindeststandards für die IT-Sicherheit bei „Unternehmen im besonderen öffentlichen Interesse“.

- Überarbeitung des Bußgeldregimes.

# Schwerpunkte ITSiG 2.0

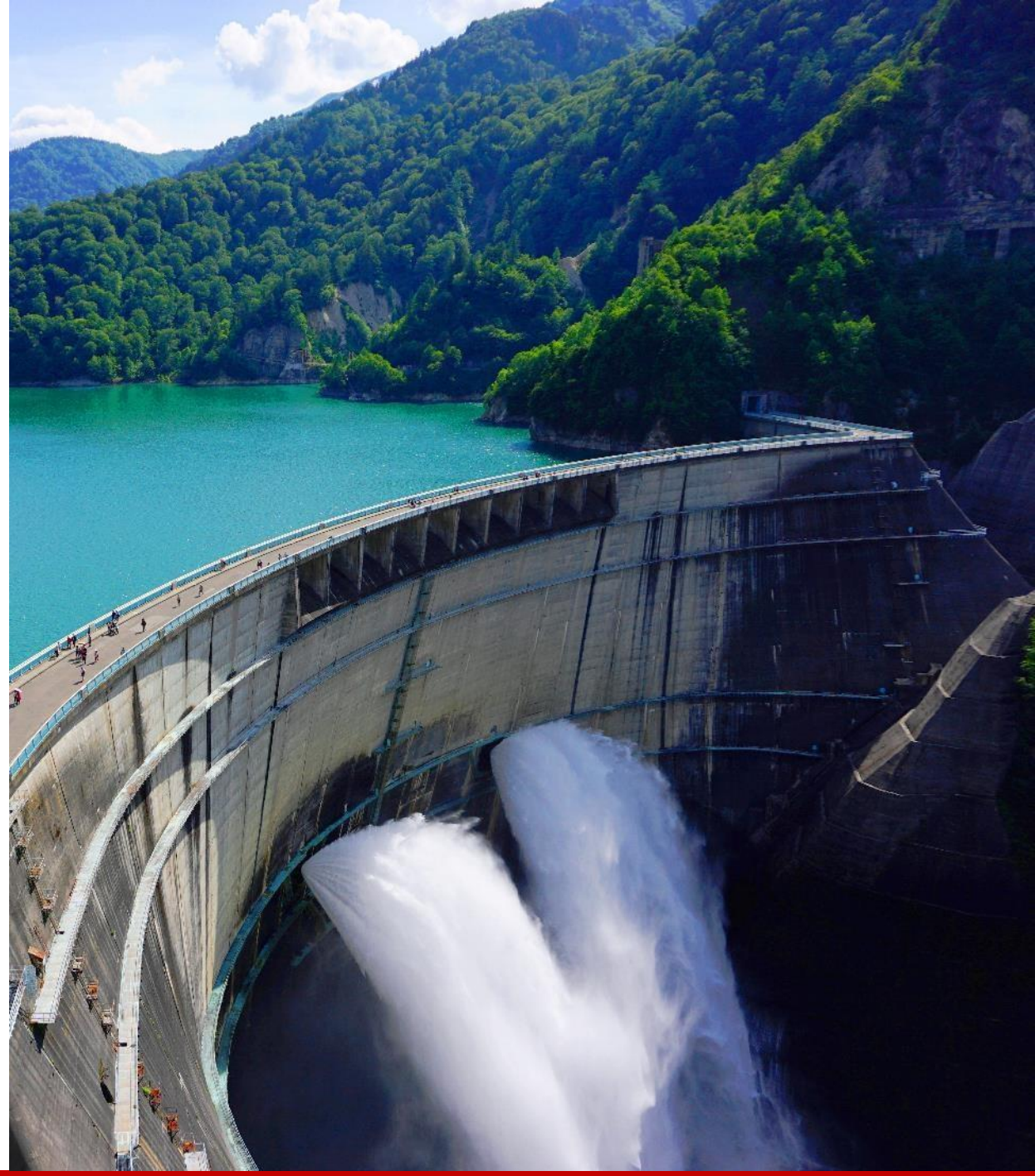
- Erweiterung Kompetenzen und Aufgaben von BSI.
- BSI wird Nationale Behörde für Cybersicherheits-Zertifizierung (EU-Verordnung 2019/881).
- BSI wird Allgemeine und Zentrale Meldestelle für die Sicherheit in der Informationstechnik.
- Detektion von Sicherheitsrisiken und von Angriffsmethoden durch BSI:
  - Durchführung von Portscans
  - IP-Adressraum – „Weiße Liste“
  - Einsatz „aktiver Honeypots“
- Erteilung von Befugnis und Auditierungen bei Konformitätsbewertungsstellen.

# Schwerpunkte ITSiG 2.0

- Bei der Zusammenarbeit mit Dritten aus der Wirtschaft wird auf etablierte Melde- und Austauschmöglichkeiten wie MISP (Malware Information Sharing Plattform) zurückgegriffen.

- Befugnis für das BSI, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen TK-Netzen zu detektieren sowie Einsatz von Systemen und Verfahren zur  Analyse von Schadprogrammen und Angriffsmethoden.

- Schaffung einer Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemedien-anbieter zur Abwehr spezifischer Gefahren für die Informationssicherheit.

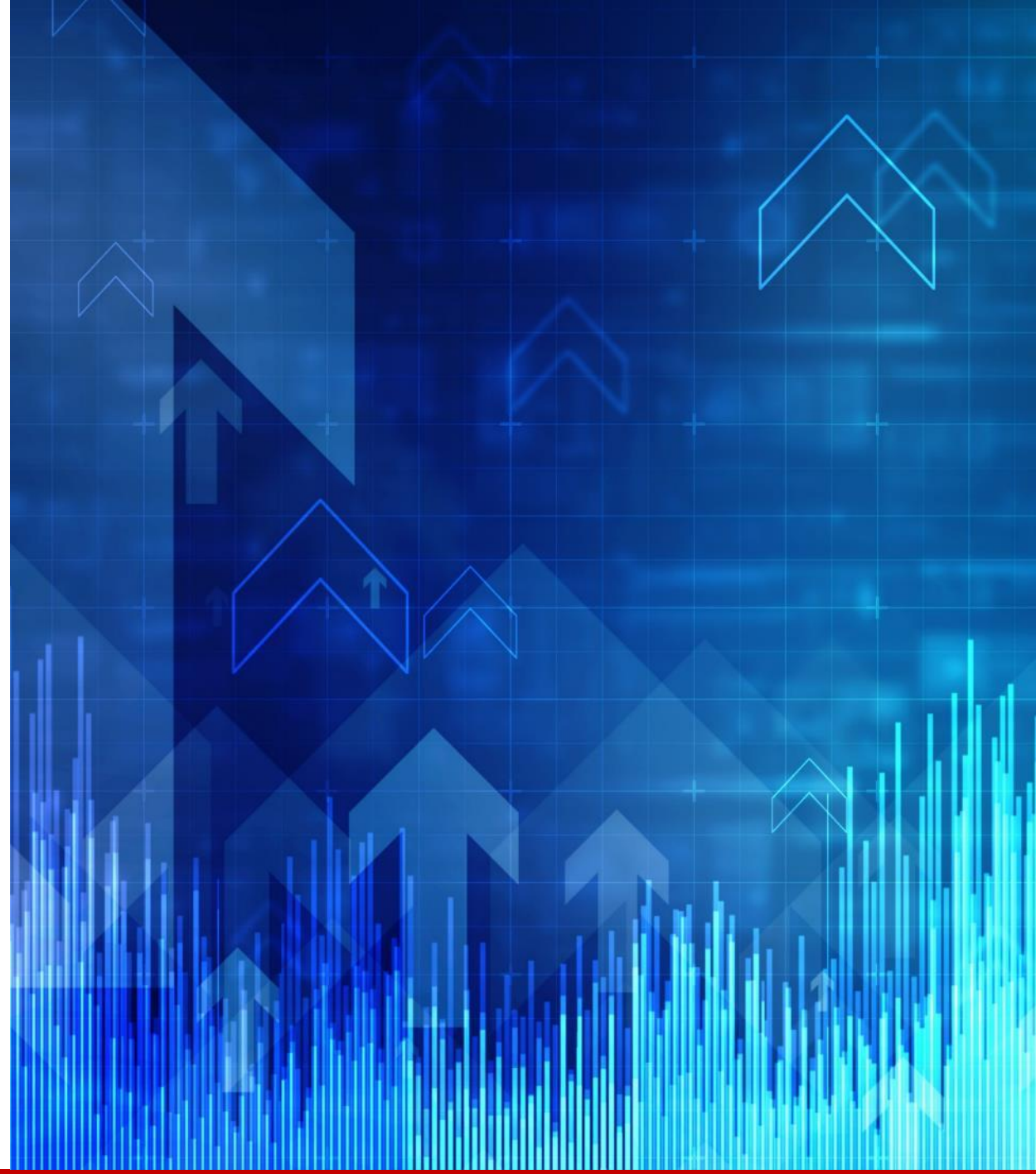


# Erfüllungsaufwand Verwaltung

- Erfüllungsaufwand von **insgesamt** 1.585 Planstellen/Stellen mit einem jährlichen Erfüllungsaufwand in Höhe von 202 Mio. € (Personalkosten und Sachkosten).

- Erfüllungsaufwand **BSI** in Höhe von 799 Planstellen/Stellen mit Personalkosten in Höhe von jährlich 74 Mio. €.

- Zusätzliche Sachkosten **BSI** in Höhe von einmalig 28 Mio. € und jährliche Sachkosten in Höhe von 49 Mio. € zur Umsetzung des Gesetzes.

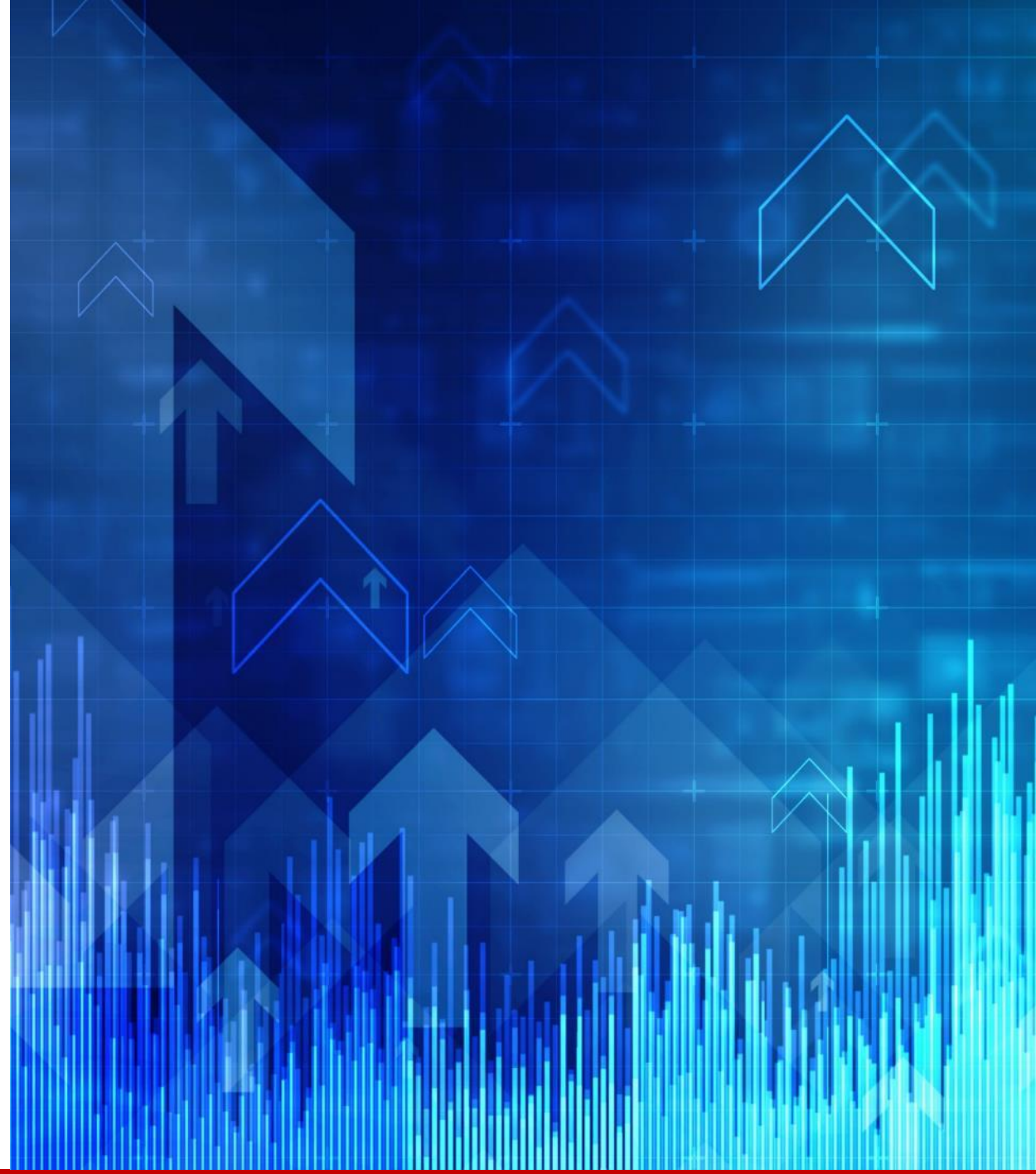


# Erfüllungsaufwand Verwaltung

ITSiG 2.0

Tabelle 1: Überblick zum gemeldeten Stellenmehrbedarf

| Ressort einschließlich Geschäftsbereich | Stellen | Davon: | | |
|---|---|---|---|---|
| | | Höherer Dienst | Gehobener Dienst | Mittlerer Dienst |
| Bundesministerium des Innern, für Bau und Heimat (BMI) | 873 | 561 | 309 | 3 |
| Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) | 15 | 9 | 6 | - |
| Auswärtiges Amt (AA) | 51 | 14 | 29 | 8 |
| Bundesministerium für Arbeit und Soziales (BMAS) | 15 | 4 | 11 | - |
| Bundesministerium der Finanzen (BMF) | 278 | 20 | 247 | 11 |
| Bundesministerium für Gesundheit (BMG) | 5 | 3 | 2 | - |
| Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) | 9,3 | 0,5 | 8 | 1 |
| Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) | 32 | 4 | 28 | - |
| Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) | 254,5 | 85,5 | 109 | 60 |
| Bundesministeriums für Wirtschaft und Energie (BMWi) | 34 | 3,5 | 18,5 | 12 |
| Bundeskanzleramt (BKAmt) | 17 | 9 | 7 | 1 |



# Erfüllungsaufwand Wirtschaft

ITSiG 2.0

- In Summe entsteht dadurch der Wirtschaft ein jährlicher Erfüllungsaufwand in Höhe von **12,8 Mio. €**.
- Der Erfüllungsaufwand für die Wirtschaft ist nur unter hoher Unsicherheit quantifizierbar.
- Da die Entwicklung der IT-Strukturen sowie möglicher Bedrohungen kaum abzuschätzen sind und teilweise noch konkretisierende Rechtsnormen ausstehen, können nur grobe Anhaltspunkte für den Erfüllungs-aufwand benannt werden.
- Schätzwerte, die im Wesentlichen auf Annahmen basieren, bilden den unteren Rand der Spannbreite möglicher Belastungen ab und sind somit als Mindestwerte zu verstehen.

# Anpassungen BSI Kritis-Verordnung

BSI-KritisV

- Zweite Verordnung zur Änderung der BSI Kritis-Verordnung ist am 14.09.2021 veröffentlich und am 01.01.2022 in Kraft getreten.

- Änderung der Schwellenwerte für Erzeugungsanlagen.
  Anstatt 420 MW als Schwellenwert gelten:
  - 104 MW installierte elektrische Nettonennleistung
  - 36 MW bei Vermarktung als Primärregelenergie
  - 0 MW bei Schwarzstartfähigkeit

# Anpassungen BSI Kritis-Verordnung

- Die dritte Verordnung zur Änderung der BSI Kritis-Verordnung und die UBI-Verordnung werden im Q3 2022 erwartet.

- Hierin werden die Schwellenwerte für den Sektor Entsorgung bzw. die Konkretisierung zum Unternehmen im besonderen öffentlichen Interesse (UBI) erwartet.

# Lessons learned aus Umsetzungen - Schlankes ISMS

- Geltungsbereich festlegen
  - so klein wie möglich; so groß wie nötig
  - interne und externe Schnittstellen festlegen
  - Ausschlüsse beschreiben – was ist nicht enthalten.

- Begriffe und Vorgehensweise aus dem eigenem Unternehmen nutzen – nicht die aus der Norm.

- Das ISMS passt sich an das Unternehmen an - nicht das Unternehmen an das ISMS!

# Lessons learned aus Umsetzungen
# Schutzbedarf und Risikoanalyse

- Strukturierte Gruppierung der Assets vorher durchführen.
- Schutzbedarf und Risikoanalyse miteinander in einem Dokument bearbeiten.
- Gleichen Schutzbedarf zusammenfassen
  - **Nicht >=** 1000 Zeilen und **nicht >=** 60 Spalten.
- Keine ewig langen Formeln einsetzen:
  - =WENN(L1049="";"";WENN(L1049="nein";"-";WENN(UND(AR1049="x";L1049="ja");WENN(AQ1049<5;2;WENN(AQ1049<9;3;3));WENN(UND(AR1049=0;L1049="ja");WENN(AQ1049<5;1;WENN(AQ1049<9;2;3))))))

# Lessons learned aus Umsetzungen - ISMS Dokumentation

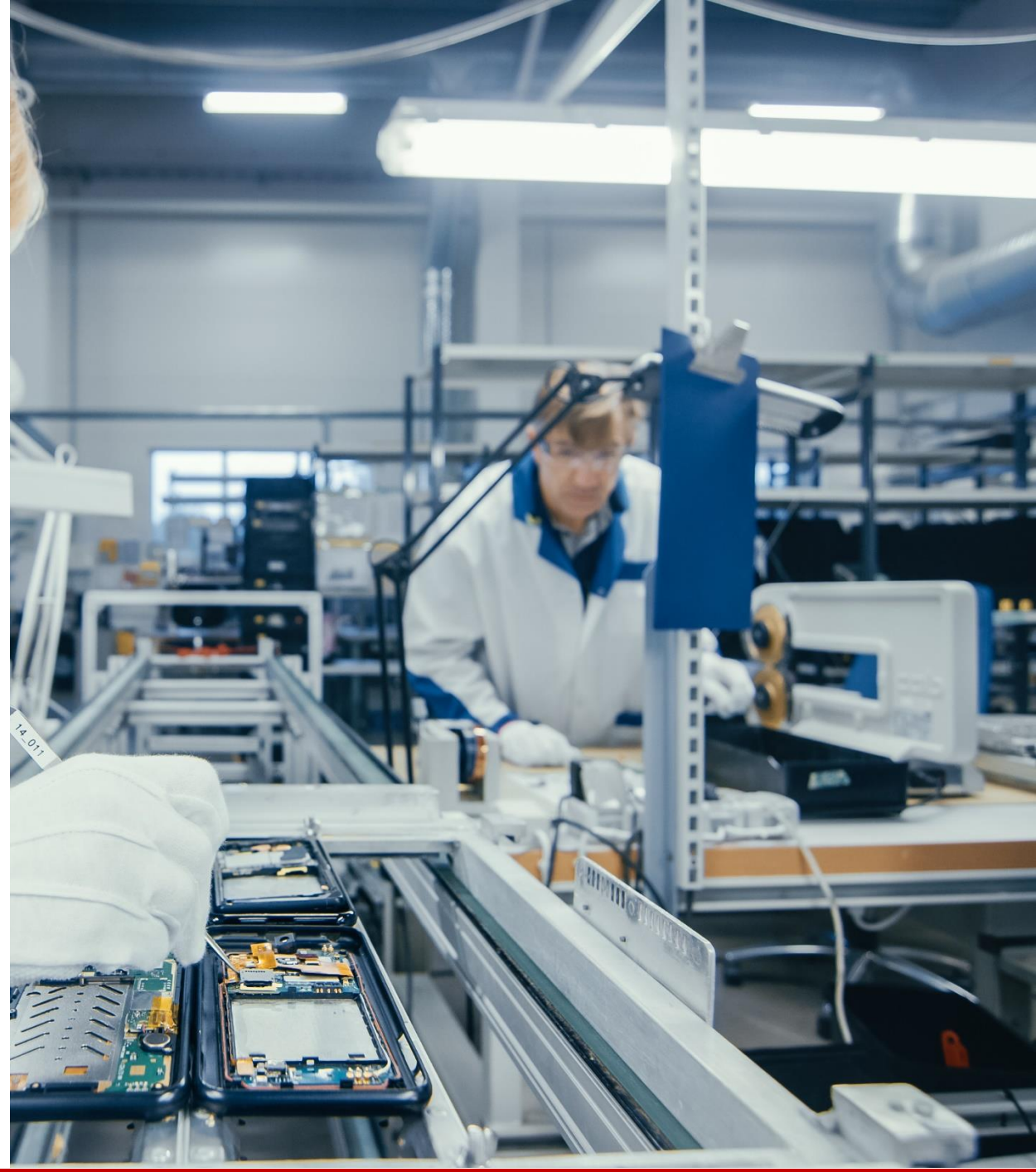
- ISMS-Dokumentation – Umfang, Aufteilung und passende Detailtiefe.
- Nicht zu detailliert beschreiben soll „lebbar“ sein.
- Keine Informationen doppelt halten
  → besser Verweise und Verlinkungen machen.
- Alles was geschrieben ist, soll die praktische Umsetzung im Unternehmen beschreiben.
- Bezeichnungen von Bereiche/Abteilungen/Gruppen in ISMS-Dokumenten nutzen; keine Namen.

# Lessons learned aus Umsetzungen - ISMS Aktivitäten planen und steuern

- ISMS-Kalender über 2 bzw. 3 Jahre führen
  - Beinhaltet ISMS-Kernteamsitzungen, Schulungen, Managementreviews, Interne und externe Audits.
- ALLE Maßnahmen, Vorfälle, Auditabweichungen etc. - technisch wie organisatorisch - über ein (Maßnahmen)Tool steuern.
- Ticketsystem oder Excelliste hierfür fortlaufend pflegen und dokumentieren.
- Regelmäßige Kernteamsitzungen abhalten und dokumentieren.

# Lessons learned aus Umsetzungen - ISMS effizienter umsetzen

- Review von Prozessen und Dokumenten im angemessenen Zeitraum durchführen.
- Interne Audits über 2 bzw. 3 Jahre planen und Aufwand für IA somit reduzieren.
- Interne Audits nutzen um ISMS zu „schärfen“ und zu verbessern.
- ISMS-Software einsetzen, um Prozesse und Dokumente deutlich besser lenken und steuern zu können.



# Zusammenfassung

- Ganzheitlicher Ansatz – Risikoanalyse und Maßnahmensteuerung als zentrale Elemente.
- Geltungsbereich möglichst schlank halten.
- Risikoanalyse von Schutzbedarf abhängig machen und in einem Dokument zusammenführen.
- ISMS-Dokumentation – Umfang, Aufteilung und passende Detailtiefe.
- Prozesse müssen in der Organisation lebbar sein.
- Planung und Steuerung von ISMS-Aktivitäten über 2 bzw. 3 Jahre.

# Zusammenfassung

- Erst die gesetzliche Verpflichtung über die Einführung eines Informationsmanagementsystems hat bei Betreibern zur tatsächlichen Umsetzungen geführt.

- Eigene Mitarbeiter/innen und Mitarbeiter/innen von relevanten Dienstleistern spielen eine zentrale Rolle.

- Technische Netzwerksicherheit und die im IT-Sicherheitsgesetz 2.0 verankerte Verpflichtung über den Einsatz von Systemen zur Angriffserkennung sind wichtige Eckpunkte für eine wirksamen Informations- und IT-Sicherheit.

# Ihr Ansprechpartner

**Kent Andersson**
Geschäftsführer

kent.andersson@ausecus.com
+49 821 2070 97 - 21

ausecus.
info@ausecus.com
+49 821 207097-0

# VIELEN DANK!

## IHRE FRAGEN?

https://bit.ly/3seAZFQ

**HIER FINDEN SIE:**

- die Präsentationsunterlagen
- ab morgen die Aufzeichnung des Vortrags
- weiterführende Informationen

Sie erhalten den Link am Freitag auch per E-Mail.