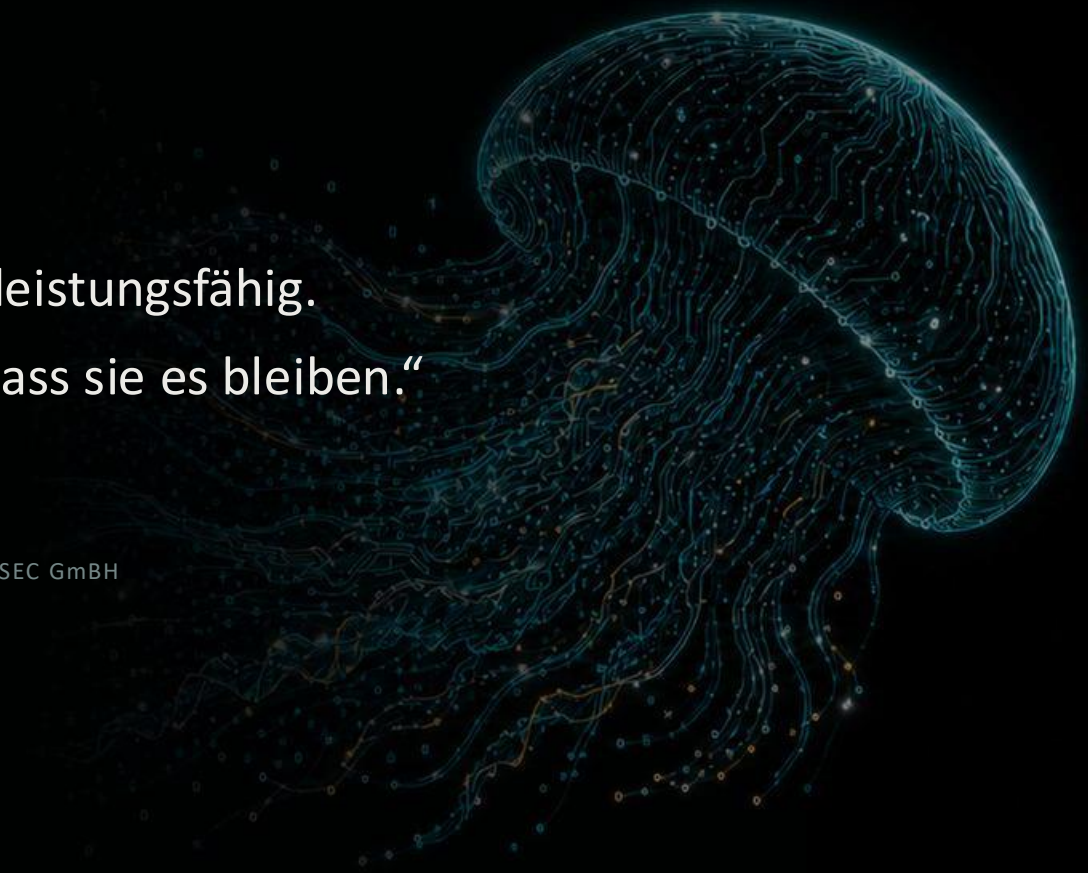
ZDT JAHRESTAGUNG 2026

Informationssicherheit an Hochschulen



Vom Projekt zum wirksamen Managementsystem. Erfahrungen aus dem hochschulübergreifenden ISMS-Aufbau in Brandenburg.

„Digitalisierung macht Hochschulen leistungsfähig.
Informationssicherheit sorgt dafür, dass sie es bleiben.“



SASCHA FRÖHLICH · Director Information Security & Governance · BASEC GmbH

01 · AUSGANGSLAGE

Digitale Dienste sind Voraussetzung für den Hochschulbetrieb.

Hochschulen sind besonders komplex zu schützen, weil Offenheit und Vernetzung Teil ihres Auftrags sind.

OFFEN

Austausch, Kooperation und Zugänglichkeit sind Teil von Forschung und Lehre.

DEZENTRAL

Zentrale und dezentrale Einheiten teilen Systeme, Aufgaben und Verantwortung.

HETEROGEN

Technologien, Fachanwendungen, Geräte und Nutzergruppen unterscheiden sich stark.

VERNETZT

Studierende, Beschäftigte, Forschende, Partner und Dienstleister greifen gemeinsam zu.

BETROFFENE LEISTUNGEN

- Lehre und Studium
- Forschung
- Verwaltung
- Kommunikation und IT-Infrastruktur

02 · AUSWIRKUNGEN

Cybervorfälle können den Hochschulbetrieb über Monate prägen.

24.11.2025

Hochschule Mainz

Nach einem Cyberangriff wurden sämtliche IT-Systeme heruntergefahren. E-Mail und zentrale Verwaltungsdienste waren beeinträchtigt. Noch im Februar 2026 lief der Aufbau einer neuen IT-Infrastruktur; dienstliche Endgeräte wurden schrittweise neu aufgesetzt und verteilt. Der Präsenzlehrbetrieb wurde weitestgehend aufrechterhalten.

28.10.2026

Universität Leipzig

Nach einem Angriff wurden die digitalen Dienste vorsorglich offline genommen. Lehre, Forschung und Verwaltung arbeiten mit erheblichen Einschränkungen. Die Rektorin erklärte am 2. November 2026, dass die vollständige Wiederherstellung voraussichtlich Wochen dauern werde.

Prävention allein reicht nicht. Hochschulen müssen Angriffe beherrschen und ihren Betrieb wiederherstellen können.

Quellen: Universität Leipzig – Statement der Rektorin, Hochschule Mainz – Wiederaufbau vom 17.02.2026

03 · BEDROHUNGSLAGE

Hochschulen stehen unterschiedlichen Angreifern und Angriffszielen gegenüber.

ANGRIFF	TYPISCHES ZIEL	MÖGLICHE WIRKUNG
Ransomware und Cybercrime	Geld · Daten · Betriebsfähigkeit	Verschlüsselung, Datendiebstahl und Erpressung
Phishing und Identitätsdiebstahl	Konten · E-Mail · Cloud	Kompromittierte Identitäten und Zugänge
Spionage und gezielte Angriffe	Forschung · Wissen · Kooperationen	Abfluss sensibler oder strategischer Informationen
Sabotage und Verfügbarkeit	Digitale Dienste · Infrastruktur	Störung oder Ausfall des Hochschulbetriebs

Das Angriffsziel kann Geld, Daten, Wissen, Zugänge oder die Betriebsfähigkeit der Hochschule sein.

04 · PROJEKT

Acht Hochschulen auf dem Weg zum zertifizierbaren ISMS.

VERBUND

8 Hochschulen im Beratungsverbund

PROJEKTZIEL

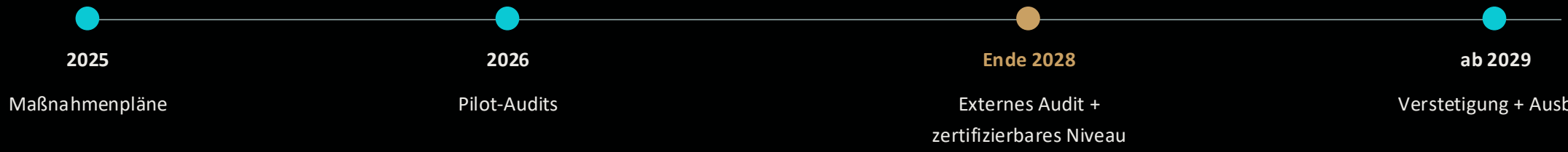
Ende 2028

zertifizierbares ISMS-Niveau

MEINE ROLLE

Externe fachliche und methodische Beratung. Gemeinsame Fragestellungen werden möglichst einmal gelöst und im Verbund wiederverwendbar gemacht.

PROJEKTPFAD



Das Projekt baut Strukturen auf. Das ISMS muss danach dauerhaft weiterleben.

Quelle: MWFK Brandenburg, Schreiben vom 10.04.2025, S. 2 bis 4.

05 · UMSETZUNG

Drei Formate unterstützen den Aufbau des ISMS.

Drei Formate, drei unterschiedliche Funktionen im Aufbau.

01	ISB-Coaching	Wöchentliche, aufeinander aufbauende ISMS-Themen.	**Kompetenz und gemeinsamer fachlicher Stand**
02	Interne Audits	Standortbestimmung, Auditpraxis und sichtbarer Entwicklungsbedarf.	**Transparenz und Lernkurve**
03	BCM-Leuchtturm	Zwei Hochschulen entwickeln Methodik und Blueprints vertieft.	**Resilienz und Wiederverwendbarkeit**

Coaching schafft Kompetenz. Audits schaffen Transparenz. BCM schafft Resilienz.

06 · PROJEKTRISIKEN

Vier Risiken gefährden das Projektziel bis Ende 2028.

Drei Risiken entstehen vor allem in der Umsetzung.

01	Zu geringe Ressourcen	Kapazität fehlt nicht nur beim ISB, sondern auch in IT, Personal, physischer Sicherheit und weiteren Bereichen.
02	Zu wenig fachliche Kompetenz	Anforderungen müssen verstanden, eingeordnet und in passende Maßnahmen übersetzt werden.
03	Fehlende Umsetzung	Risiken, Auditfeststellungen und Vorgaben wirken erst, wenn daraus konkrete Veränderungen entstehen.

SCHLÜSSELRISIKO

Zu geringe Aufmerksamkeit und Unterstützung durch die Hochschulleitung

Ohne Priorisierung, Entscheidungen und Rückhalt durch die Hochschulleitung fehlt die notwendige Umsetzungskraft.

Das größte Risiko ist nicht fehlende Dokumentation, sondern fehlende Umsetzungskraft.

07 · VERANTWORTUNG

Informationssicherheit ist Führungsverantwortung.

HOCHSCHULLEITUNG	INFORMATIONSSICHERHEITSBEAUFTRAGTER
setzt Richtung und Priorität	berät fachlich und methodisch
stellt Ressourcen bereit	koordiniert das ISMS
entscheidet über Risiken und Zielkonflikte	schafft Transparenz über Risiken
fordert Umsetzung ein	begleitet Maßnahmen und Umsetzung
trägt die Gesamtverantwortung	**bereitet Entscheidungen vor und hält das ISMS steuerbar**

Der ISB kann ein ISMS nicht alleine aufbauen.

Quelle: MWFK Brandenburg, Schreiben vom 10.04.2025, Zielsetzung zur Verantwortung der Hochschulleitungen.

08 · ISMS

Ein ISMS schafft Klarheit vom Risiko bis zur Umsetzung.

Ein ISMS verbindet Risikoanalyse, Verantwortung und konkrete Umsetzung.

04	Mindestniveau sichern	MFA, angemessene Verschlüsselung, Berechtigungen, Risikoanalysen und Schwachstellenmanagement verbindlich etablieren.
03	Umsetzung steuern	Aus Risiken und Anforderungen werden konkrete Maßnahmen, Prioritäten und Verantwortlichkeiten.
02	Verantwortung klären	Festlegen, wer entscheidet, wer Maßnahmen umsetzt und wer die Wirksamkeit überprüft.
01	Risiken verstehen	Prozesse, Informationen und Systeme bewerten und relevante Risiken transparent machen.

Das ISMS schafft einen nachvollziehbaren Weg vom Risiko zur Umsetzung.

09 · BCM

Nicht jeder Ausfall lässt sich verhindern.

Business Continuity schafft Klarheit darüber, was die Hochschule auch in einer Störung leisten können muss.



- Kritische Leistungen kennen und priorisieren.
- Abhängigkeiten von IT, Personen, Räumen und Dienstleistern verstehen.
- Wiederanlauf und Kommunikation vorbereiten.
- Übungen nutzen, bevor der Ernstfall die Abläufe testet.

10 · ZIELBILD ENDE 2028

Ein gemeinsames Sicherheitsniveau entsteht durch gelebte Strukturen.

Das Zielbild ist kein Organigramm, sondern ein funktionierendes Zusammenspiel.



HOCHSCHULLEITUNG

trägt das Thema

priorisiert, entscheidet und unterstützt sichtbar

ISB

ist früh eingebunden

berät, koordiniert und schafft Transparenz

IT UND ZENTRALE BEREICHE

setzen wirksam um

übersetzen Anforderungen in belastbare Maßnahmen

FACHBEREICHE UND DEZENTRALE EINHEITEN

leben Sicherheit

berücksichtigen Sicherheit in Entscheidungen und Alltag

Das Ziel ist erreicht, wenn Informationssicherheit Teil der normalen Hochschulsteuerung geworden ist.

11 · FAZIT

Drei Dinge bleiben.

Zum Schluss

01	Führungsverantwortung	Informationssicherheit braucht Priorität, Ressourcen und Entscheidungen der Hochschulleitung.
02	Klarheit und Verbindlichkeit	Ein ISMS macht Risiken, Verantwortung und Umsetzung nachvollziehbar und steuerbar.
03	Gemeinsame Resilienz	Wirksam wird Sicherheit erst, wenn ISB, IT, Fachbereiche und Leitung zusammenarbeiten.

Ein wirksames ISMS kann nur die Hochschule als Ganzes aufbauen und leben.

KONTAKT

Fragen? Gern im Anschluss oder im Nachgang.



Sascha Fröhlich

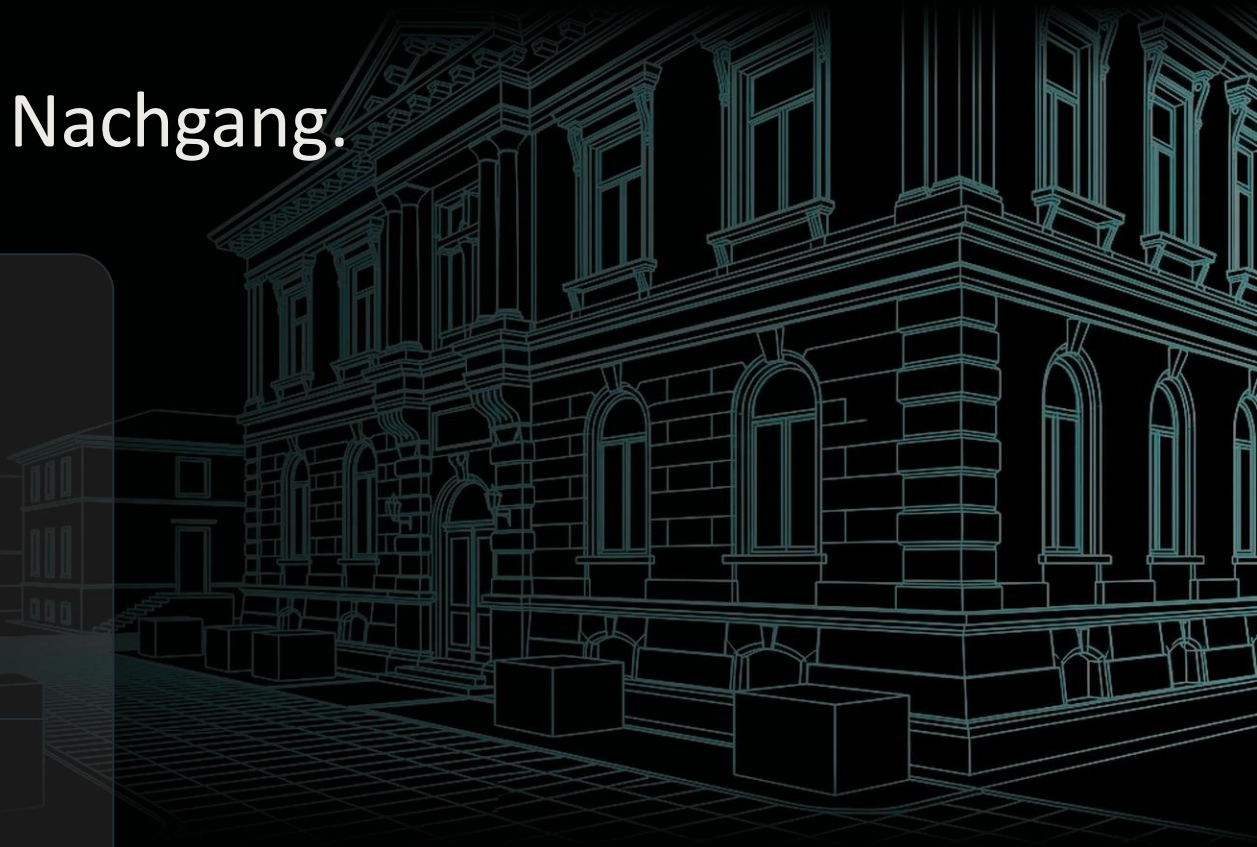
Director Information Security & Governance · BASEC GMBH

sascha.froehlich@basec.de

+49 155 659 18979

→ TERMIN VEREINBAREN

Basec GmbH · Weinstraße 5b · 67146 Deidesheim · basec.de



Hinweis zur Erstellung. Für Grafik, Gliederung und Textbearbeitung dieser Präsentation wurden generative KI-Systeme eingesetzt. Sämtliche Inhalte wurden von Basec fachlich geprüft, überarbeitet und freigegeben. Die inhaltliche Verantwortung liegt bei der Basec GmbH.