Leistungsbeschreibung

Beratungsleistung ISMS

Inhalt

Ausgangssituation

Die FernUniversität in Hagen benötigt zur Erreichung von Zielen in der Informationssicherheit beratende und aktive Unterstützung**.**

Hierzu wird ein Dienstleister gesucht, der im universitären Umfeld die Herausforderungen bezogen auf die Prozesse in Forschung und Lehre kennt und die Hochschule aktiv bei den Themenfeldern Informationssicherheitsmanagement nach BSI IT-Grundschutz gemäß 200-1 bis 200-3 unterstützt.

Zu den Leistungen gehören **Beratung und aktive Unterstützung** in den Themenbereichen:

- Steuerungsorganisation & Governance,
- Basis- Absicherung der kritischen Geschäftsprozesse,
- Erweiterung zur Standard- Absicherung der kritischen Geschäftsprozesse.
- Reifegraderhöhung des ISMS und Reporting

Es werden hohe Erwartungen an die Kompetenz des Bieters, bezogen auf die geforderten Themenbereiche, gestellt:

- Beratungskompetenz hinsichtlich des BSI IT-Grundschutzes,
- Kenntnisse und Lösungskompetenz im universitären Umfeld sowie der Öffentlichen Verwaltung.

Angeboten werden sollen im Gesamtkontext des Informationssicherheitsmanagement, insbesondere das Risikomanagement, das Sicherheitsvorfall Management, die Awareness, KVP Zyklen, sowie das Reporting.

Leistungsbeschreibung

Zu den hier nachfolgenden Punkten ist eine Beratung und Unterstützung durch den externen Dienstleister notwendig.

1) Weiterentwicklung der ISMS Governance

Um Sicherheit ganzheitlich betrachten zu können, muss eine Organisation aufgebaut werden, die die Informationssicherheit für die gesamte Verwaltung sowie die Lehre steuert. Der Bereich Forschung muss sich dem anschließen können, wird aber nicht a priori dazu verpflichtet.

Dazu ist die Weiterentwicklung einer Sicherheitsorganisation zu entwickeln, die die Informations-Sicherheitsbelange der Zentralen Hochschulverwaltung (ZHV) sowie Lehre und Forschung gleichermaßen berücksichtigt und sicherstellt. Diese Sicherheitsorganisation handelt gemäß der vom BSI vorgegeben Richtlinien.

In diesem Rahmen wird der Dienstleister die Sicherheitsorganisation unterstützen die Top-Down Struktur für die Steuerung & Kontrolle der Informationssicherheit im Kontext der FernUniversität in Hagen weiter zu entwickeln. Es wird somit die Voraussetzung für die geforderte Einführung des Basis-Absicherung der Kern-Prozesse geschaffen.

Darüber hinaus unterstützt der Dienstleister die Sicherheitsorganisation das ISMS kontinuierlich in seinen Richtlinien und der Handlungsanweisungen zu erweitern und zu schärfen. Dazu werden unter anderem das Risikomanagement, die Awareness sowie das Sicherheitsvorfallmanagement ausgebaut.

Daraus leiten sich dann die folgenden Anforderungen ab:

- Weiterentwicklung einer Top-Down-Struktur für die Steuerung & Kontrolle der ISM
- ISMS-Regelwerk (z.B. Leitlinien, Richtlinien) wird für die ZHV und Lehre erstellt und verabschiedet.
- Eine Anschlussfähigkeit des Bereichs Forschung an das ISMS wird konzipiert.
- Die Verpflichtung der Leitung zur Informationssicherheit wird formalisiert (Management Commitment).
- Ein Prozess zum Umgang mit Risiken und Chancen wird etabliert.
- Eine Anleitung zur Operationalisierung der IS-Vorgaben auf lokaler Ebene wird erstellt.
- Ein Prozess zur Effektivitätsmessung der IS-Maßnahmen wird eingeführt.
- Ein Reporting-Prozess für die Informationssicherheit an die Leitungsebene wird etabliert.
- Der kontinuierliche Verbesserungsprozess (KVP) für das ISMS wird eingeführt.

2) Basis Absicherung der kritischen Geschäftsprozesse

Erstes Ziel ist, den Schutz des Basis Betriebs zur Sicherstellung der Funktion von Verwaltung und Lehre zu erreichen. Hierzu ist es notwendig den Betrieb in den Stand der Technik der IT und Informationssicherheit zu transformieren. Dazu muss eine Analyse des Basis Betriebs durchgeführt werden. Im Rahmen einer Risikobetrachtung müssen entsprechende Schwachstellen innerhalb der Technik und auch innerhalb der Betriebsorganisation identifiziert und entsprechend der Sicherheitsziele behandelt werden.

Dies gliedert sich in die folgenden Bereiche:

Die Anforderungen des BSI IT-Grundschutzes müssen innerhalb des IT-Betriebes operationalisiert werden. Dazu müssen die Anforderungen in technische Maßnahmen übersetzt werden und in den IT-Systemen und der Organisation implementiert werden.

Dazu wird die Leitungsebene der Organisation in die Lage versetzt die Anforderungen in Arbeitsanweisungen innerhalb Ihrer Dezernate / Abteilungen zu definieren. Der Dienstleister unterstützt die Transformation zwischen dem Richtlinie Management und dem der Arbeitsanweisungen.

Ebenfalls ist die Zusammenarbeit mit Dienstleister, die die Sicherheitsanforderungen der Fernuniversität Hagen innerhalb ihrer Dienstleistungserbringung umsetzen müssen, zu berücksichtigen. Hierzu ist eine aktive Dienstleistersteuerung als Teil der Organisation oder als Dienstleistung aufzubauen. Hier berät und unterstützt der Dienstleister die Fernuniversität in Hagen und deren Organisation, die das Dienstleistungsmanagement übernimmt.

Auf Basis dieser nach BSI IT-Grundschutz erstellten Richtlinien werden die technischen Grundlagen für einen sicheren Systembetrieb gelegt.

Dies betrifft im Besonderen:

Erstellung von Sicherheitskonzepten für kritische Geschäftsprozesse nach BSI IT-Grundschutz:

- Feststellung des Schutzbedarfes der Informationen innerhalb des Geschäftsprozess
- Strukturanalyse des Geschäftsprozesses
- Herstellung des BSI IT-Grundschutzes
- Risikobewertung des Umsetzungsstandes
- Erweitere Anforderungen
- Umsetzung der Anforderungen

Durch dieses Vorgehen werden die folgenden Ziele erreicht:

- Umfassende Sicherheitsbewertung der Geschäftsprozesse
- Sicherheitsbewertung der Infrastruktur der Fernuniversität in Hagen
- Sicherheitsbewertung der betriebenen Systeme
- Sicherheitsbewertung der von Dienstleistern betriebenen Systeme
- Sicherheitsanalyse der Netzwerkarchitektur und der aktiven Komponenten

Aus diesen Sicherheitsbewertungen die nach BSI IT-Grundschutz erstellt wurden, leiten sich die folgenden Maßnahmen ab:

- Reifegraderhöhung der ISMS Grundschutzmethodik nach BSI 200-1 bis 200-3
- Beschreibung und Umsetzung von Sicherheitsmaßnahmen gemäß des BSI Grundschutz-Kompendiums 2023
- Monitoring und Reporting der Sicherheits- Maßnahmen für die kritischen Geschäftsprozesse.
- Aufbau eines Schwachstellen- und Sicherheitsvorfallmanagements.
- Beschreibung und Umsetzung eines zielgruppenorientiertes Awareness Programms innerhalb der Hochschulen.

3) Umsetzungszeitraum und Ziele

Der Dienstleister wird den Reifegrad des ISMS betreuen und mit gezielten Maßnahmen die Sicherheitsorganisation unterstützen die Standardabsicherung der kritischen Geschäftsprozesse bis Ende 2027 zu erreichen.

Die folgenden Maßnahmen sind umzusetzen:

- Basis Absicherung der kritischen Geschäftsprozesse bis Mitte 2026
- Begleitung des internen Audits in 2026
- Erweiterung des IT-Grundschutz auf Standard-Absicherung für kritische Geschäftsprozesse
- Begleitung des BSI Testat in 2027

Der Reifegrad wird durch eine definierte KPIs nachverfolgt. Dazu sind diese KPIs mit dem Dienstleister und der Sicherheitsorganisation zu definieren. Die Zielerreichung des Reifegrades wird durch regelmäßige KPI Messungen erbracht und dem Reporting zugeführt.

Berater/in

Der Auftragnehmer benötigt Beratung hinsichtlich der ISMS Management Methodik und der praktischen Umsetzung des BSI IT-Grundschutzes für die kritischen Geschäftsprozesse.

Der Dienstleister stellt dazu einen BSI Berater, sowie zeitweise ein Auditor nach BSI IT-Grundschutz Methodik, dem Auftragnehmer nach Aufwand (gem. Kontingent) zur Verfügung.

Qualifikation & Referenzen des Anbieters

Referenzen des Anbieters:

Der Anbieter hat mindestsens folgende Erfahrungen und Referenzprojekte vorzuweisen:

- Mind. Drei Referenzprojekte zum BSI-Grundschutz allgemein
- Mind. Zwei Projekte im Hochschulumfeld
- Mind. Eine Durchgeführte Zertifizierungen im Hochschulumfeld: Beratung und Zertifizierung zusammen

Qualifikation des Anbieters:

Der Anbieter kann folgende zertifizierte Mitarbeiter nach BSI vorweisen:

- ISO 27001 Lead Auditor oder vergleichbar
- BSI IT-Grundschutzpraktiker(Berater)
- Security Officer ISO 27001 oder vergleichbar

Anforderungen an das eingesetzte Personal

Der Dienstleister setzt während der Auftragsdurchführung das Personal ein, welches in der Anlage „Personalprofile“ angegeben ist.
Im Übrigen müssen die folgenden Mindestanforderungen stets eingehalten sein:

- Der Berater des Auftragnehmers muss über mindestens drei Jahre Berufserfahrung im Bereich BSI IT-Grundschutz verfügen
- Der Auftragnehmer darf sein Projektpersonal grundsätzlich nicht auswechseln.
- Ausnahmen gelten, soweit ein wichtiger Grund vorliegt. Wichtige Gründe in diesem Sinne sind insbesondere:
    - dauerhafte Krankheit,
    - Tod,
    - Kündigung des Mitarbeiters,
    - Schwangerschaft und Elternzeit.

Der neu hinzutretende Mitarbeiter muss über das gleiche Niveau an fachlicher Qualifikation und Berufserfahrung verfügen wie der ausscheidende Mitarbeiter.

Bewertungskriterien und -gewichtung

Die Wertung der Angebote erfolgt anhand folgender Kriterien:

Kriterium	**Gewichtung (%)**
Kosten	30
Qualifikation & Referenzen des Anbieters	30
Umsetzung / Zeitplanung	20
Absicherung der kritischen Geschäftsprozesse	10
Reifegraderhöhung der ISMS Governance	10

Das vollständige Bewertungsschema mit Erläuterungen zu jedem Kriterium entnehmen Sie bitte dem Anhang Bewertung_ISMS Support_Dienstleister, welche von Ihnen in den Spalten C und D auszufüllen ist.

Einsatzort

Der Einsatz des Dienstleisters kann Remote oder vor Ort in den Räumlichkeiten der FernUniversität in Hagen erfolgen.

Sonstige Informationen

Es gelten die vertraglich ausdrücklich vereinbarten Kosten. Anderweitige Kosten können gegenüber der Auftraggeberin nicht geltend gemacht werden. Nachforderungen sind ausgeschlossen.

Bieterfragen

Bieter können Fragen ausschließlich über die in der Bekanntmachung angegebene Vergabeplattform stellen. Der Auftraggeber wird die Fragen über die Vergabeplattform beantworten. Telefonische Auskünfte werden nicht erteilt.

Datenschutz

Die vom Wettbewerbsteilnehmer bereitgestellten Daten werden ausschließlich zum Zwecke des Vergabeverfahrens und – im Zuschlagsfall – der Vertragsdurchführung verarbeitet und gespeichert. Im Übrigen sichert der Auftraggeber den potenziellen Auftragnehmern zu, dass die übermittelten personen-bezogenen Daten gemäß der Datenschutzgesetze stets vertraulich behandelt und verarbeitet werden.