ATM CONSULTING
AUDIT TRAINING MANAGEMENT

Bericht zum Audit
IT-Grundschutz –Testat für Basis-Absicherung

Testat IT-Grundschutz-Nr. IGT-0014-2023
Vom 26.06.2023

vorgelegt für:

leap in time
work-life
research center

erstellt von:

Dipl.-Ing. Erik Gremeyer,
ATM Consulting

Auditart	Datum	Auditart	Datum
☐ Erstzertifizierungs-Audit		☐ 1. Überwachungs-Audit	
☐ Stufe 2 Audit		☐ 2. Überwachungs-Audit	
☐ Nachaudit		☐ Re-Zertifizierungs-Audit	
☐ Erweiterungsaudit		☐ ……	
☒ IT-Grundschutz Testat	26.06.2023	☐	

Normengrundlage:
- ☐ ISO/IEC 27001:2013 / DIN EN ISO/IEC 27001:2017
- ☐ IT-Sicherheitskatalog gem. §11 Abs. 1a EnWG von August 2015
- ☒ IT-Grundschutz Kompendium, BSI-Standard 200-1 und 200-2

Name der Firma,

leap in time GmbH
Work-Life Forschungszentrum / leap in time Lab
Donnersbergring 16
64295 Darmstadt

Auditbeauftragter
Ansprechpartner: Ruth Stock-Homburg, Michael Rinner

ISMS Dokumentation
Stand/Datum vom: Juni 2023

Audit-Leiter: Dipl-Ing. Erik Gremeyer (BSI-ZIG-0305-2020)

Auditbericht-Nr.: ATM-BSI-2023-06-26

Geltungs-/Anwendungsbereich des ISMS:
Die leap in time GmbH mit allen Geschäftsprozessen, Anwendungen und IT-Systemen zur Erbringung der Dienstleistung.
Der Informationsverbund erstreckt sich auf die gesamte leap in time GmbH.
Die leap in time GmbH berät Unternehmen im Bereich Robotik und KI und ist im Bereich B2B tätig. Das Auftragsvolumen, die Häufigkeit der Aufträge und die Kunden/Kundinnen variieren. Es gibt einige wenige Stamm- bzw. Großkunden.

Ergebnis:

Die Anforderungen des IT-Grundschutz auf Basis ISO/IEC 27001 für Basis-Absicherung sind erfüllt. Das Nutzungsrecht für das GS-Testat (Nr. IGT-0014-2025) wird für 24 Monate erteilt.

Prüfauftrag

Die ATM-CONSULTING wurde mit der Durchführung eines Audits entsprechend den Anforderungen des Bundesamt für Sicherheit in der Informationstechnik zur Erlangung eines Testats zur Basisabsicherung beauftragt. Das Audit wurde im Zeitraum vom 11.06.2021 bis 15.06.2023 an dem Standort Darmstadt und remote durchgeführt. Diese Prüfung dient auch als Grundlage für die anstehende Managementbewertung des ISMS.

Vorgehensweise/Grundlage des Audits nach IT-Grundschutz auf Basis ISO 27001

Als Grundlage des durchgeführten Audits des Informationssicherheits-Managementsystems (ISMS) der BFS wurden die Anforderungen berücksichtigt, die sich aus den Anforderungen des BSI unter Berücksichtigung des notwendigen Umsetzungsgrad „Basis-Absicherung“ gemäß Leitfaden zur Basisabsicherung nach IT-Grundschutz ergeben.

Prüfgrundlage des Verfahrens sind:

- DIN ISO/IEC 27001: „Informationstechnik – IT-Sicherheitsverfahren – InformationssicherheitsManagementsysteme – Anforderungen“
- BSI-Standard 200-1: „Managementsystem für Informationssicherheit ISMS“
- BSI-Standard 200-2: „IT-Grundschutz-Methodik“
- BSI-Standard 200-3: „Risikoanalyse auf Basis von IT-Grundschutz“
- Auditierungsschema für ISO 27001 auf der Basis von IT-Grundschutz
- IT-Grundschutz-Kompendium

Ziele des Audits

Ziel ist die Bestätigung der Konformität des Managementsystems für Informationssicherheit (ISMS) gemäß der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz. Bei der Auditierung wurden die im Auditierungsschema beschriebenen Anforderungen an die Prüfungshandlung des Auditteamleiters und der Mitglieder des Auditteams umgesetzt.

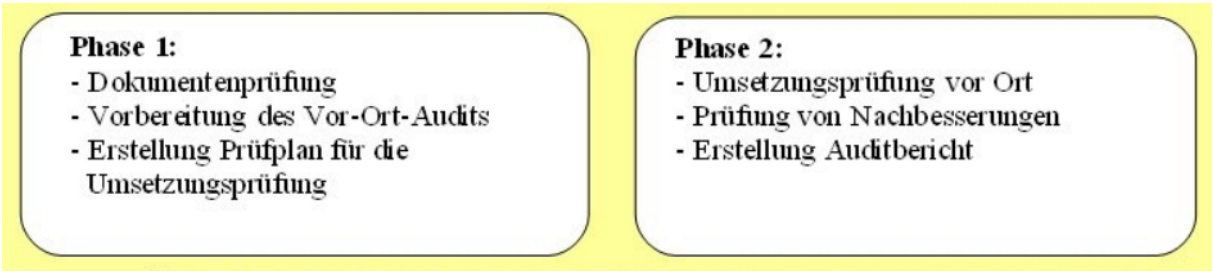
Vorgehensweise

Innerhalb des Audits wurden sowohl der Aufbau als auch die Wirksamkeit des Informationssicherheits-Managementsystems (ISMS) gemäß den o. s. Anforderungen des IT-Grundschutz überprüft und nachvollzogen. Alle aufgebauten Prozesse und etablierten Rollen sowie das IS-Risikomanagement wurden hinsichtlich der normativen Anforderungen an ein ISMS auditiert und auf ihre angemessene Umsetzung bewertet.

Die jeweils verantwortlichen Mitarbeiter wurden in Form von Interviews befragt, zugehörige Dokumente, darunter sowohl Prozessdokumentationen als auch Listen, Protokolle und Dateien eingesehen. Relevante Einzelvorgänge wurden in Form von Stichproben detailliert überprüft und nachvollzogen.

Eventuell aufgedeckte Abweichungen wurden identifiziert, dokumentiert und je nach möglicher Auswirkung klassifiziert.

Für die Bestätigung der Konformität eines Managementsystems für Informationssicherheit (ISMS) gemäß der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz werden im Auditierungsschema die Anforderungen an die Prüfungshandlung des Auditteamleiters und der Mitglieder des Auditteams beschrieben.



Folgende Referenzdokumente bilden die Grundlage für die Auditierung und wurden innerhalb der Phase 1 des Audits geprüft und in Phase 2 die Umsetzung der beschriebenen Maßnahmen verifiziert:

- Leitlinie und Richtlinien für Informationssicherheit (A.0)
- Strukturanalyse (A.1)
- Schutzbedarfsfeststellung (A.2)
- Modellierung des Informationsverbundes (A.3)
- Ergebnis des IT-Grundschutz-Checks (A.4)
- Risikoanalyse (A.5)
- Realisierungsplan (A.6)

Hinweis: A.5 und A.6 nur anteilig, da die Risikoanalyse nicht vollständig abgeschlossen war.

Während des Audits konnte durchgängig erkannt werden, dass

Die Initiierung des Sicherheitsprozesses erfolgreich umgesetzt wurde

- der Kontext der Organisation verstanden und die Erfordernisse und Erwartungen interessierter Parteien – sowohl intern als auch extern – erfüllt werden
- der Anwendungsbereich beschrieben und ein Informationsmanagementsystem auf Basis IT-Grundschutz etabliert wurde
- die von der Geschäftsführung das Thema der Informationssicherheit ausreichend fördert und die festgelegte Informationssicherheitspolitik im Unternehmen bekannt gemacht und implementiert wurde
- relevante vertragliche und gesetzliche Anforderungen regelmäßig ermittelt und Änderungen dokumentiert werden – eingeschränkt auf die Belange einer GmbH.
- die Anforderungen sind allen relevanten Personen und Funktionen zugänglich und verständlich gemacht

- **Die Organisation des Sicherheitsprozesses erfolgreich eingeführt wurde**
  - die Verantwortlichkeiten, Aufgaben und Befugnisse innerhalb des Managementsystems sind festgelegt, dokumentiert und bekannt gemacht wurden

- eine Risikomanagementmethodik beschrieben und angewendet wird, diese wird mit Excel abgebildet.
- resultierend aus der Risikobewertung und IT-GS-Check werden Maßnahmen abgeleitet und im Rahmen des Realisierungsplan (Risikobehandlungsplan, A.6 Dokument) adressiert, dokumentiert, genehmigt und freigegeben sowie kontrolliert umgesetzt. Die Geschäftsführung ist regelmäßig – aktuell wöchentich eingebunden.
- das für den laufenden Betrieb des ISMS benötige Budget, Ressourcen und sonstige Mittel zur Verfügung gestellt werden.

- **Die Durchführung des Sicherheitsprozesses konnte in der Prüfung festgestellt werden**
  - alle innerhalb des Geltungsbereichs befindlichen Personen ihren Aufgaben und Rollen entsprechende Weiterbildung und Trainings erhalten
  - im Unternehmen im Hinblick auf die Erfüllung der Informationssicherheitspolitik und der Ziele alle relevanten Abläufe und Tätigkeiten ermittelt werden, die Abläufe werden geplant und überwacht
  - die Verwirklichung, Aufrechterhaltung und Wirksamkeit des ISMS anhand jährlich geplanter Audits gemessen werden **soll**, die Detailplanung der Audits wird bis zum Q3/2025 abgeschlossen sein. Aktuell noch in der Planung zur Einführung des IT-GS enthalten.
  - das Unternehmen eine Prozessanweisung hinsichtlich der Lenkung von Dokumenten hat, die angemessen ist und ist kommuniziert wird

Die Umsetzung und Wirksamkeit des Managementsystems (Basis-Absicherung) sowie die Prozesse zur Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme und entsprechen dem Stand der Technik.

Geprüfte Bausteine des Informationsverbunds

Im Rahmen des internen Audits und der Prüfung des umgesetzten IT-Grundschutz (Basis-Absicherung) wurden u. s. Bausteine in Stichproben auf den Umsetzungsstand geprüft.

- ISMS.1
- ORP.1, 2, 3, 5
- CON.8
- APP.6
- DER.3.1
- APP.3.6
- SYS.3.3
- INF.11

Ergebnisse des Audits

Die Ergebnisse sind als positive Feststellungen, Verbesserungshinweise und Abweichungen im nachfolgenden Bericht eingestuft worden.

Feststellung: Das ISMS ist gut entwickelt und erfüllt alle Anforderungen der Basis-Absicherung des IT-Grundschutz. Das Testat für die erfolgreiche Umsetzung der Basis-Absicherung auf Basis IT-Grundschutz wird erteilt.
Zur Erlangung eines ISMS-Zertifikates (Nativ oder IT-Grundschutz) sind die Abweichungen zu schließen.

Positive Feststellungen
P1: Der Informationsverbund wird nach den Vorgaben und Beispielen des BSI modelliert und beinhaltet alle für die Dienstleistung (Durchführung von Penetrationstests) erforderlichen Prozesse und Objekte.

P2: Das Awarenessprogramm ist vorbildlich aufbereitet und durch qualifizierte Wissensprüfungen erfolgt eine Erfolgskontrolle.

P3: Umgang mit Externen- das Prinzip „Security by Design“ wird gut umgesetzt. Grundsätzlich haben nur festangestellte Mitarbeiter Zutritt zu den Büros.

Hinweise/Verbesserungspotenzial
VP1: Die Dokumentenstruktur sollte ggf. in der Dokumentenlenkung näher beschrieben werden – u. a der Vorgabecharakter und Zweck von Informationen und die Word/Pdf-Dokumente der Richtlinien und Verfahren.

VP2: Die Nachweisführung u. a. bei der Berechtigungsprüfung und Logfileprüfung sollte verschriftlicht werden. Geeignet wären z. B. Checklisten oder automatische Prüfungen mit Einträgen in z. B. einem Ticketsystem.

VP3: Es sollte eine Agenda eingeführt werden um sicherzustellen, dass alle Anforderungen an den Informationsbedarf abgedeckt sind. U. a. auch Einbindung der ISB in die Prozesse und Organisationsänderungen. (ISMS.1.A15, ISMS.1.A4)

VP4: Beim vereinfachten Netzplan sollte der Schutz (z. B. https, VPN) der einzelnen Verbindungen direkt ersichtlich sein.

VP5: Der Syslog-Server sollte im Netzplan direkt benannt werden (nicht nur über die Asset-Kennung)

VP6: Die diversen Kontrollen (Clientprüfung) sollten geplant und in den Auditplan eingefügt werden. Die Vorgehensweise und wie die Prüfung geeignet dokumentiert wird, sollte kurz beschrieben werden, ggf. auch Verwendung von Checklisten.

VP7: Prüfungen (Stichproben) durch die ISB bzgl. durchgeführter Kontrollen sollten geplant und dokumentiert werden – Auditprogramm/Prüfplan für die Dauer der Testat-/Zertifikatsgültigkeit 24 bzw. 36 Monate

VP9: Need-to-know-Prinzip sollte geprüft werden, ob dies aktuell angemessen angewendet wird.

VP10: Versionierung der Dokumente sollte nur bei inhaltlichen Überarbeitungen oder Freigaben geändert werden. Neue Dokumentenversionen erzeugen, um den Reviewstatus abzubilden sollte vermieden werden.
VP11: Die vorhandene Liste für die Referenzdokumente sollte um weitere Einträge (Zeilen-weitere Dokumente des ISMS) und Angaben zur Version und Reviewstatus (Spalten z. B. "Art des Dokuments", "Beschreibung" oder "Owner") ergänzt werden.

Abweichungen/Nichtkonformität

AW1: Ein Auditprogramm liegt noch nicht vollständig (Abdeckung 24/36 Monate nach Zertifizierung) vor– es finden Prüfungen durch die Fachverantwortlichen, externe Prüfer (ATM-Consulting) und der Informationssicherheitsbeauftragten statt. Diese sind auch teilweise verschriftlicht. Diese Prüfungen sollten risikobasiert, näher geplant und zusammenhängend verschriftlicht werden.

AW2: Ein formales Managementreview wurde bisher nicht durchgeführt – Ansätze sind in den IT-GS-Einführungsprojekt sichtbar. Dieser Auditbericht bildet eine wesentliche Basis für das Managementreview. Für die Erteilung des IT-GS-Testats (Basis-Absicherung) ist der Umsetzungsgrad angemessen.

Feststellungen:

Planung für interne Kontrollen und Dokumentation der Nachweisführung

☒ Eine Abschlussbesprechung gemäß DIN ISO/IEC 17021 und ISO/IEC 27006 wurde beim Kunden durchgeführt.

☐ Es wurden keine Abweichungen vom Regelwerk festgestellt.

☒ Zahl und Art der Abweichungen vom Regelwerk siehe Bericht.

☐ Die Abweichungen wurden noch nicht behoben.

☒ Die Abweichungen wurden zwischenzeitlich behoben.

☐ Die Zertifikatserteilung bzw. der Fortbestand der Gültigkeit des Zertifikates wird nicht empfohlen.

☐ Die Anforderungen der ISO/IEC 27001 werden mit Ausnahme der im Abweichungsbericht aufgeführten Einschränkungen erfüllt. Die Zertifikatserteilung bzw. der Fortbestand der Gültigkeit des Zertifikates wird nach Behebung der Abweichungen empfohlen.
(Die Bestätigung zur Behebung der Abweichungen wird nach erfolgtem Nachweis, spätestens aber drei Monate nach Feststellung der Abweichung nachgereicht.)

☒ Die Anforderungen des IT-Grundschutz auf Basis ISO/IEC 27001 für Basis-Absicherung ISO/IEC 27001 werden erfüllt und damit die Ausstellung eines Testats nach IT-Grundschutzes empfohlen.

Sämtliche Bewertungsschlussfolgerungen dieses Audits beruhen auf Stichproben von Auditnachweisen der verfügbaren Informationen. Im Hinblick auf den Stichprobencharakter des Audits ist darauf hinzuweisen, dass Schwachstellen und Nichtkonformitäten vorhanden sein können, die während des Audits nicht festgestellt worden sind. Daher entbindet das Ergebnis des Audits das

Unternehmen nicht von der Verantwortung, die Erfüllung der einschlägigen Vorschriften und Normforderungen sicherzustellen. Das Unternehmen behält die volle Haftung für seine ausgeübten Tätigkeiten.

Dieser Bericht und alle zugehörigen Dokumente wurden ausschließlich für das Unternehmen erstellt und dürfen für andere Zwecke nicht verwendet werden. ATM Consulting übernimmt keinerlei Verantwortung (rechtlich oder anderweitig) oder Haftung für oder in Zusammenhang mit irgendeinem anderen Zweck, für den der Bericht vielleicht verwendet wird oder für irgendeine andere Person, der dieser Bericht gezeigt wird oder in deren Hände er vielleicht gelangen könnte. Auch sind keine anderen Personen berechtigt, sich auf den Bericht zu beziehen.

Das Eigentumsrecht am Auditbericht mit allen zugehörigen Dokumenten verbleibt bei der ATM-Consulting.

Ingelheim, 06.08.2023
Ort, Datum

Unterschrift Audit-Leiter