Cyber Risk Rating & Cyber Trust Label

Schema Policy 2027

Versionskontrolle

Version	Datum	Freigabe
1.0	8. September 2020	KSÖ Cyber Risk Advisory Board
2.0	14. September 2021	KSÖ Cyber Risk Advisory Board
3.0	13. September 2022	KSÖ Cyber Risk Advisory Board
4.0	7. September 2023	KSÖ Cyber Risk Advisory Board
4.1	23. Februar 2024	KSÖ Cyber Risk Advisory Board (Umlaufbeschluss)
5.0	5. September 2024	KSÖ Cyber Risk Advisory Board
5.1	4. März 2025	KSÖ Cyber Risk Advisory Board
6.0	8. September 2025	KSÖ Cyber Risk Advisory Board
7.0	14. September 2026	KSÖ Cyber Risk Advisory Board

Inhaltsverzeichnis

1 EINFÜHRUNG 4
2 GRUNDLEGENDE PRINZIPIEN UND ZIELE 4
3 UMFANG 5
4 CYBER RISK RATING SCHEMA 5
4.1 B Rating 5
4.2 A Rating 6
4.3 A+ Rating 6
4.4 WebRisk Indicator 7
4.5 Cyber Trust Label 7
4.5.1 Cyber Trust Platinum Label 8
4.6 Überwachung 9
4.7 Erneuerungsprozess 9
4.8 Übertragung von Cyber Risk Ratings 10
4.9 Überprüfungs-Audits und Zurückziehung von Ratings 10
5 STEUERUNG DES CYBER RISK SCHEMAS 11
6 DURCHFÜHRUNG DES CYBER RISK RATINGS 12
6.1 Ablauf der Anforderung eines Cyber Risk Ratings 12
6.2 Voraussetzungen für ein Cyber Risk Rating 12
7 SICHERHEIT DER VERARBEITETEN DATEN 12
8 ANHANG A: ANFORDERUNGEN 14
8.1 Anforderungen für B Rating 14
8.2 Anforderungen für A Rating (zusätzlich zu B) 16
8.3 Prüfkriterien für WebRisk Indicator 18
8.4 Anforderungen für das Platinum Label 18
9 ANHANG C: QUALIFIKATIONEN 21
9.1 Mindestanforderung an Auditoren 21
9.2 Mindestanforderung an Validierer 21
10 ANHANG D: BEGRIFFSBESTIMMUNGEN 22

1 Einführung

Das Cyber Risk Rating und das darauf basierende Cyber Trust Label sind ein Schema zur Bewertung des Cyber Risk Status von Organisationen (Unternehmen, Vereinen, etc.). Das vorliegende Dokument beschreibt alle relevanten Aspekte des Schemas. Es soll sowohl den geprüften Organisationen als auch deren Kunden die notwendige Sicherheit (Assurance) in das vom Cyber Risk Rating bzw. vom Cyber Trust Label ausgedrückte, erwartbare Sicherheitsniveau der bewerteten Organisationen vermitteln.

Dieses Dokument basiert auf der internationalen Normenreihe für Konformitätsbewertungen (ISO/IEC 170xx, insbesondere ISO/IEC 17000 und ISO/IEC 17029) und wendet dieses sinngemäß an (siehe Anhang D: Begriffsbestimmungen).

Zielsetzung von Konformitätsbewertungen ist die Bildung von Vertrauen in die bewerteten Organisationen, Produkte oder Prozesse. Eine Konformitätsbewertung zielt darauf ab, die Erfüllung definierter Anforderungen zum Bewertungsobjekt (z.B. einer Organisation) darzulegen (Assurance) und dies in geeigneter Weise zu belegen. Der Wert einer solchen Beurteilung wird bestimmt vom Vertrauen, das in das zugehörige Schema gesetzt wird. Dieses umfasst unter anderem die Anforderungen selbst, die Überprüfungsmethoden sowie die Steuerungsmechanismen zur Prüfung und Weiterentwicklung des Schemas.

2 Grundlegende Prinzipien und Ziele

Die grundlegenden Werte des Cyber Risk Ratings sowie des darauf aufbauenden Cyber Trust Labels sind Sicherheit und Vertrauen, ebenso wie Offenheit, Transparenz und Nachvollziehbarkeit. Das Rating sowie das Label sollen Vertrauen in die bewertete Organisation erzeugen, dass dieses das Thema Cybersicherheit ernst nimmt und in angemessener Weise behandelt. Durch Offenlegung des Schemas und der damit zusammenhängenden Kriterien und Bewertungsmethoden soll sichergestellt werden, dass dies in einer offenen, transparenten und nachvollziehbaren Art und Weise geschieht. Dies trägt wiederum dazu bei, dass die Aussagekraft des Ratings und des Labels gestärkt wird und Unternehmen darauf vertrauen können, dass gut geratete Organisationen sowie Organisationen, welche das Cyber Trust Label tragen, vertrauenswürdige Partner mit einem entsprechend niedrigen Cyber-Risiko sind.

Speziell die Anforderungen des B Ratings stellen Basisanforderungen an die Cybersicherheit dar, die jede Organisation weitgehend erfüllen sollte. Eine starke Verbreitung von Organisationen mit einem guten B Rating bzw. einem Cyber Trust Label ist somit eine positive Aussage über die Cyberresilienz eines Standorts. In diesem Sinne ist es auch eine der Zielsetzungen, durch die Einführung und Verbreitung des Cyber Risk Ratings eine Verbesserung der Cybersicherheit des Wirtschaftsstandorts Österreich zu erreichen.

Für jedes Unternehmen, das die Vertrauenswürdigkeit seiner Lieferanten hinsichtlich Cybersicherheit prüfen will oder prüfen muss, stellt das Cyber Risk Rating eine effiziente und effektive Methode dar, seiner Sorgfaltspflicht beim Third Party Risk Management nachzukommen. Betreiber wesentlicher Dienste sind gemäß § 11 Abs. 1 Z 2 iVm Anlage 1 NISV rechtlich verpflichtet, hinsichtlich des Umgangs mit Dienstleistern, Lieferanten und sonstigen Dritten entsprechende Sicherheitsvorkehrungen zu treffen. Das vorliegende

Schema zielt auf die Erfüllung dieser Anforderung ab, ersetzt aber nicht den notwendigen Nachweis eines Betreibers wesentlicher Dienste gemäß § 17 Abs. 3 NISG.

3 Umfang

Das Cyber Risk Rating bezieht sich immer auf ein konkretes Unternehmen, definiert durch eine Firmenbuchnummer (oder äquivalentes). Die Beantwortung der Fragen bezieht sich auf den Wirkungskreis des eigenen Unternehmens, das heißt die Systeme, Prozesse und das Personal unter der eigenen Kontrolle des Unternehmens. Bei Unternehmen, die IT für Kunden betreiben gilt eine entsprechende Sorgfaltspflicht, aber nur in dem Umfang, in dem das Unternehmen eigenständig über Schutzmaßnahmen für Kundensysteme entscheiden kann.

4 Cyber Risk Rating Schema

Das Cyber Risk Rating Schema beschreibt die Anforderungen, deren Erfüllung im Rahmen der Bewertung zu bestätigen ist, sowie wie die Prüfmethoden und erforderlichen Nachweise, die zur objektiven Bewertung der Erfüllung bzw. Nichterfüllung herangezogen werden.

Das Cyber Risk Rating unterscheidet vier Bewertungsschemata, die sich in Bezug auf ihren Anspruch (*Security Claim*) als auch in Bezug auf die Rigorosität der Überprüfung (*Assurance Level*) unterscheiden: das B Rating, das A Rating, das A+ Rating sowie das Platinum-Schema, das auf der Durchführungs-VO (EU) 2024/2690 aufbaut. Aufbauend auf diesen Ratings wird das Cyber Risk Label angeboten, welches als nach außen sichtbares Qualitätsmerkmal für ein angemessenes Cybersicherheitsniveau steht.

4.1 B Rating

Das B Rating bewertet den Anspruch eines Basissicherheitslevels (Baseline Security Claim) einer Organisation. Die definierten Anforderungen beziehen sich auf ein grundlegendes Schutzniveau, das von jeder Organisation (auch von kleinen) eingehalten werden sollte. Die gestellten Anforderungen und die verlangten Nachweise sind dementsprechend allgemein gehalten, erfordern aber dennoch eine definierte Mindestqualität, um den notwendigen Mindestsicherheitsanspruch zu gewährleisten.

Die Bewertungsmethode ist eine Selbstdeklaration der Organisation, es handelt sich demnach um ein *first-party conformity assessment*. Die Unternehmen bewerten hierbei selbst, inwiefern sie die vom Schema definierten Anforderungen im Rahmen der definierten Kriterien (siehe Anhang A) erfüllen und dies anhand der definierten Nachweise (Evidenzen) im Bedarfsfall auch nachweisen können. Um die Nachvollziehbarkeit und Plausibilisierung der Selbstbewertung zu gewährleisten, müssen die Organisationen zu jeder Frage eine Beschreibung abgeben, wie jede Anforderung in der Organisation konkret erfüllt ist und welche Evidenzen dazu im Bedarfsfall vorgelegt werden können. Im Rahmen der Validierung der vorgelegten Selbstdeklarationen wird von einem qualifizierten Prüfer (Mindestanforderungen an Validierer siehe Anhang) eine Bewertung der Beschreibungen vorgenommen, inwiefern diese die Erfüllung der gestellten Anforderung hinreichend belegen. Abweichungen von den Fragen können in einem gewissen Umfang möglich sein,

wenn sie durch angemessene und akzeptable Maßnahmen kompensiert sind, die das Risiko gemäß Sicherheitsziel in *vergleichbarer* Weise adressieren. Die Einschätzung der Angemessenheit und Vergleichbarkeit liegt bei den Validierern bzw. Auditoren.
Um eine neutrale Bewertung sicherzustellen, werden Selbstdeklarationen gegenüber dem Validierer anonymisiert. Sollte eine Beschreibung unvollständig oder unklar sein oder Fragen bezüglich der tatsächlichen Erfüllung offen lassen, so erfolgt eine Anfrage zur Klärung bei der bewerteten Organisation. Diese ist innerhalb zwei Wochen seitens der Organisation zu beantworten. Einmalig kann eine zusätzliche Nachfrist von maximal zwei Wochen gewährt werden. Sollte die geforderte Beantwortung unterbleiben oder die Klarstellung nicht in der erforderlichen Qualität erfolgen, so wird die gegenständliche Frage als nicht erfüllt bewertet. Spätere Klarstellungen können nur im Rahmen einer gänzlich neuen Risikobewertung vorgenommen werden. Um die Qualität der Selbstbewertung weiter zu erhöhen, verpflichten sich die bewerteten Organisationen im Rahmen der Rating-Vereinbarung, dem mit der Validierung betrauten Unternehmen bzw. einem Auditor auf Anfrage Zugang zu den beschriebenen Nachweisen (Evidenzen) zu gewähren. Dies kann stichprobenartig im Rahmen der Validierung beziehungsweise im Rahmen eines Überprüfungs-Audits bei Verdacht auf Unregelmäßigkeiten erfolgen, zum Beispiel nach einem bekannt gewordenen schwerwiegenden Sicherheitsvorfall. Die bewertete Organisation muss demnach jederzeit in der Lage sein, auf Anfrage die Nachweise für die in der Selbstdeklaration getätigte Selbstbewertung vorlegen zu können.
Auf Basis der finalen validierten Selbstbewertung wird das B Rating berechnet und der bewerteten Organisation mitgeteilt. Das Rating wird weiters in der KSV1870 Rating-Datenbank gespeichert.

Sollte sich herausstellen, dass im Rahmen der Selbstbewertung vorsätzlich oder grob fahrlässig Falschangaben gemacht wurden, treten die im Kapitel 4.9 beschriebenen Maßnahmen in Kraft. Jede Falschangabe stellt einen Verstoß gegen die Rating-Vereinbarung dar und kann zu einer Aussetzung des Ratings und (sofern vergeben) zu einem Entzug der Label-Nutzungslizenz führen.

4.2 A Rating

Das A Rating bewertet den Anspruch eines **fortgeschrittenen Sicherheitslevels** einer Organisation (Advanced Security Claim). Die definierten Anforderungen beziehen sich auf ein erhöhtes Schutzniveau, das von jeder Organisation eingehalten werden sollte, die aufgrund ihres Tätigkeitsfeldes einen erhöhten Sicherheitsanspruch hat.

Die Bewertungsmethode ist eine **Selbstdeklaration** der Organisation und erfolgt analog zu 4.1.

4.3 A+ Rating

Das A+ Rating bewertet ebenfalls den Anspruch eines **fortgeschrittenen Sicherheitslevels** einer Organisation (Advanced Security Claim). Es beruht auf denselben Anforderungen wie 4.2.

Die Bewertungsmethode ist ein **unabhängiges Audit** der Organisation, es handelt sich demnach um ein *third-party conformity assessment*. Die Organisation wird hierbei von

einem unabhängigen qualifizierten Auditor überprüft, inwiefern es die vom Schema definierten Anforderungen im Rahmen der definierten Kriterien (siehe Anhang A) erfüllt. Die Prüfung, welche zeitnahe[1] nach dem Rating erfolgen muss, erfolgt anhand der definierten Nachweise (Evidenzen), welche dem Auditor vorgelegt und plausibel gemacht werden müssen. Es obliegt der sachverständigen Bewertung des Auditors, ob die vorgelegten Evidenzen vollständig und stichhaltig sind, um die geforderten Anforderungen zu erfüllen. Es liegt weiters im Ermessen des Auditors, im Bedarfsfall weitere Evidenzen einzufordern oder stichprobenartige Überprüfungen vorzunehmen, um die Wirksamkeit der geforderten Anforderungen sicherzustellen (Mindestanforderungen an Auditoren siehe Anhang). Auf Basis des durchgeführten Audits erstellt der Auditor einen Audit-Bericht, welcher zu jeder Anforderung festhält, ob diese - seiner sachverständigen Bewertung entsprechend - erfüllt ist oder nicht. Dieser Audit-Bericht wird der bewerteten Organisation zugänglich gemacht, worauf es innerhalb einer Frist von zwei Wochen die Möglichkeit des Einspruchs und des Begehrens auf Richtigstellung hat. Dazu sind dem Auditor gegebenenfalls weitere Evidenzen vorzulegen. Die Letztentscheidung der Bewertung liegt beim Auditor. Nach Durchführung des Audits übermittelt der Prüfer eine Information an den KSV1870 bzw. an Cyber Trust Austria, ob das ermittelte Risk Rating durch die Prüfung bestätigt werden konnte oder nicht. Der Audit-Bericht selbst wird aus Sicherheitsgründen nicht übermittelt. Wenn es beim Audit zur Feststellung von Abweichungen vom zuvor ermittelten Cyber Risk Rating kommt, dann muss der Auditor dem KSV1870 bzw. Cyber Trust Austria mitteilen, bei welchen Fragen es zu einer (positiven oder negativen) Abweichung gekommen ist. Auf Basis dessen wird das Rating in der Datenbank des KSV1870 entsprechend angepasst.

4.4 WebRisk Indicator

Der WebRisk Indicator ist eine externe Sicherheitsprüfung, welche aus dem Internet zugängliche Anwendungen einer Organisation auf nicht intrusive Weise überprüft und aufgrund dessen Rückschlüsse auf die zugrundeliegende technische und organisatorische Cybersicherheit in diesem Bereich ermöglicht. Die zur Organisation gehörigen Domänen, welche Bestandteil dieser Überprüfung sind, müssen bei der Beantragung bekannt gegeben werden und werden durch technisch zuordenbare, aus dem Internet zugängliche Anwendungen ergänzt. Der WebRisk Indicator wird bei der Validierung der B- und A Ratings als Indikator berücksichtigt und extra ausgewiesen. Falls die bewertete Organisation Einsprüche gegen den WebRisk Indicator hat, kann es diese innerhalb einer Frist von zwei Wochen einbringen.

4.5 Cyber Trust Label

Das Cyber Trust Label baut auf dem Cyber Risk Rating bzw. der DVO 2024/2690 auf. Es gibt vier Arten von Cyber Trust Labels: das Cyber Trust Standardlabel, das Cyber Trust Silber Label das Cyber Trust Gold Label sowie das Cyber Trust Platinum Label (siehe dazu Kapitel 4.5.1 Cyber Trust Platinum Label). Das Recht zur Nutzung der Labels setzt das Erreichen einer gewissen Punktezahl beim Cyber Risk Rating bzw. der DVO 2024/2690 voraus:

[1] Die Gültigkeitsdauer des Ratings (und ggf. des darauf basierenden Labels) bezieht sich grundsätzlich auf den Zeitpunkt der Rating-Erstellung. Sofern zwischen Rating und Audit mehr als acht Wochen verstreichen, ist eine erneute Beantwortung des Fragebogens erforderlich, dafür fällt ggf. eine Bearbeitungsgebühr an.

Label	Logo	Voraussetzung
Cyber Trust Standardlabel	CYBER TRUST AUSTRIA	Vorliegen eines gültigen B Ratings von 190 oder besser
Cyber Trust Silber Label	CYBER TRUST AUSTRIA	Vorliegen eines gültigen A Ratings von 190 oder besser
Cyber Trust Gold Label	CYBER TRUST AUSTRIA	Vorliegen eines gültigen A+ Ratings[2] von 190 oder besser
Cyber Trust Platinum Label	CYBER TRUST AUSTRIA	Erreichung von >= 85% bei der validierten Selbstdeklaration gemäß Durchführungs-VO (EU) 2024/2690 der EU-Kommission

Das erreichte Label darf nach Erfüllung der Voraussetzungen und Bezahlung der Label Gebühr auf Printmedien und elektronischen Dokumenten sowie auf allen angegebenen Domänen der qualifizierten Organisation zu Informations- und Werbezwecken angezeigt werden.

Die Nutzung des Cyber Trust Labels ohne gültigen Label-Nutzungsvertrag und aufrechten Voraussetzungen (gültiges, nicht-zurückgezogenes Mindestrating, siehe 4.9) stellt einen Verstoß gegen geltende Lizenz- und Markenrechte dar und wird zivilrechtlich geahndet.

4.5.1 Cyber Trust Platinum Label

Das Cyber Trust Platinum Label baut im Gegensatz zu den anderen Labels direkt auf der Durchführungs-VO (EU) 2024/2690 der Kommission vom 17. Oktober 2024 auf. Diese Durchführungs-VO umfasst insgesamt 50 Anforderungen, welche analog zum Vorgehen bei den Cyber Risk Ratings im Rahmen einer validierten Selbstdeklaration von Validierern geprüft und qualifiziert bewertet werden. Bei jeder Frage gibt es nur „Erfüllt“ oder „Nicht Erfüllt“, wobei die Entscheidung ob die gemachten Angaben ausreichend sind, um die geforderten Anforderungen adäquat zu erfüllen, beim Validierer liegen. Sollte es Ablehnungen geben werden diese begründet und mit Empfehlungen versehen. Der Validierer kann bei Bedarf in seinem eigenen Ermessen Artefakte (Evidenzen) des bewerteten Kunden einfordern, wenn er dies für die ausreichende Plausibilisierung der Fragen als notwendig erachtet.

[2] Nur im ersten Jahr und dann jedes dritte Jahr, dazwischen A Rating von 190 oder besser (siehe 4.7 Erneuerungsprozess)

Wenn die Summe der als erfüllt bewerteten Fragen 85% übersteigen (dies ist analog zu einem CRR <= 190), dann gilt die Qualifikation für ein Platinum Label erfüllt und ein solches wird ausgestellt. Die Gültigkeitsdauer beträgt ebenfalls ein Jahr, danach muss die Bewertung erneuert werden, wobei eine Delta-Betrachtung aufbauend auf dem Resultat des Vorjahres erfolgt.

4.6 Überwachung

Die Überwachung des Cyber Risk Ratings erfolgt jährlich. Dem entsprechend hat ein Cyber Risk Rating eine Gültigkeitsdauer von einem Jahr, danach muss es erneut ermittelt werden. Dies gilt sowohl für das B Rating als auch für das A/A+ Rating. Das auf den Cyber Risk Ratings basierende Cyber Trust Label muss daher ebenfalls jährlich erneuert werden.

4.7 Erneuerungsprozess

Das Cyber Risk Rating und das darauf basierende Cyber Trust Label haben eine Gültigkeitsdauer von einem Jahr. Danach muss das jeweilige Rating erneuert werden. Inhaber des Cyber Trust Labels werden 1 Monat vor Ablauf der Gültigkeit daran erinnert, den Rating-Prozess erneut zu durchlaufen. Für eine durchgängige Gültigkeit des Labels mit demselben Stichtag ist ein Abschluss des erneuten Ratings (für Standard Label: Abschluss des CRR bzw. für Gold Label: Abschluss des Audits) in einer Periode bis zu 4 Wochen *vor* und 8 Wochen *nach* dem Gültigkeitsstichtag zulässig. Wenn das Rating 8 Wochen nach dem Gültigkeitsstichtag noch nicht erneuert ist, wird es in der Datenbank auf *inaktiv* (grau) gesetzt; wenn es 6 Monate nach dem Gültigkeitsstichtag noch nicht erneuert ist, wird es aus der Label Datenbank gelöscht.

Bei einer Erneuerung des Ratings kann dieses als *Delta-Betrachtung* durchgeführt werden. Das überprüfte Unternehmen kann sich – aufbauend auf den im Vorjahr gemachten Angaben – darauf beschränken, allfällige Änderungen gegenüber den im Vorjahr gemachten Angaben bekannt zu geben. Bei Veränderungen der Fragen des Schemas bzw. Anpassungen der Definitionen der Anforderungskriterien muss jedenfalls auf die neuen/ geänderten Anforderungen in der Beantwortung eingegangen werden. Wenn sich weder im Unternehmen noch bei einer Frage etwas verändert hat, kann die Beantwortung des Vorjahres einfach fortgeschrieben werden, muss jedoch erneut bestätigt werden.

Bei der Erneuerung eines Gold Labels wird ein erneutes externes Audit erst wieder nach drei Jahren notwendig. Die erneute Beantwortung der Fragen – im Sinne der oben beschriebenen Delta-Betrachtung – ist aber auch hier jedes Jahr erforderlich. Der Zyklus bei Gold Labels ist somit:

- Jahr 1 (erstmalige Ausstellung des Gold Labels): A-Rating plus externes Audit (= A+)
- Jahr 2: A-Rating
- Jahr 3: A-Rating
- Jahr 4: A-Rating plus externes Audit (= A+)
- Jahr 5: A-Rating
- Jahr 6: A-Rating
- Jahr 7: A-Rating plus externes Audit (= A+)
- usw.

4.8 Übertragung von Cyber Risk Ratings

Grundsätzlich bezieht sich ein Cyber Risk Rating immer auf eine definierte Firma mit einer definierten Firmenbuchnummer. Es ist aber in Ausnahmefällen möglich, Ratings innerhalb einer Firmengruppe oder eines Firmenverbundes zu *übertragen*, unter folgenden Voraussetzungen:

- Die Sicherheitsvorschriften und Prozesse sind für alle genannten Firmen gleich
    - Dies muss im Geltungsbereich der internen Security-Policy ausdrücklich entsprechend festgehalten sein
- Die Sicherheits-Anlagen und die handelnden Personen müssen ebenfalls dieselben sein

Dies muss durch das Unternehmen schriftlich und mit firmenmäßiger Zeichnung bestätigt sein.

4.9 Überprüfungs-Audits und Zurückziehung von Ratings

Der Wert eines Schemas bemisst sich an dem Vertrauen, das in dieses gesetzt wird. Dafür werden nach bestem Wissen und Gewissen die oben beschriebenen Prüfmechanismen eingesetzt. Kein Bewertungsschema kann jedoch eine hundertprozentige Aussage zum tatsächlichen Status Quo treffen, ebenso wie keine Sicherheitsmaßnahme hundertprozentige Sicherheit garantieren kann. Aus diesem Grund ist es wichtig, klare Regeln für den Umgang mit Vorfällen, Verdachtsfällen und Verstößen gegen die Rating-Vereinbarung festzulegen.

Grundsätzlich verpflichtet sich jede Organisation, die sich einem KSV1870 Cyber Risk Rating unterzieht, bereits vorab, einem allfälligen Überprüfungs-Audit zuzustimmen. Überprüfungs-Audits beziehen sich ausschließlich auf die Vorlage von Evidenzen betreffend die Fragen aus dem Schema, es besteht somit kein *allgemeines* Audit-Recht. Überprüfungs-Audits können notwendig werden, wenn es einen schwerwiegenden Sicherheitsvorfall bei einer gerateten Organisation gegeben hat oder wenn es Verdachtsmomente zu Missbrauch oder Falschinformationen gibt. Weiters können Überprüfungs-Audits stichprobenartig ohne Angabe von Gründen durchgeführt werden. Die Entscheidung über die Durchführung eines Überprüfungs-Audits liegt beim KSV1870. Bei wahrheitsgemäßer Beantwortung der Fragen in der Selbstdeklaration sollte ein Überprüfungsaudit auch das gleiche Risk Rating ergeben. Kleinere Abweichungen werden im Sinne von Ermessensspielräumen akzeptiert. Sollte die Abweichung im Risk Rating zwischen Selbstdeklaration und Überwachungsaudit jedoch signifikant sein (im negativen Sinne), dann ist von vorsätzlichen oder grob fahrlässigen Falschangaben in der Selbstdeklaration auszugehen. In diesem Fall wird das Rating *zurückgezogen* und ein neues Ratingverfahren kann frühestens nach einer Cool-Off-Periode von 6 Monaten – auf Kosten der Organisation – erneut durchgeführt werden. In der Zwischenzeit wird in der KSV1870 Rating-Datenbank das Rating der Organisation als „Zurückgezogen“ gekennzeichnet. Weiters werden alle KSV1870 Kunden, die in den letzten 12 Monaten das Rating der betroffenen Organisation abgefragt hatten, über den Status „Zurückgezogen“ des zugehörigen Ratings informiert. Wenn das Rating zurückgezogen wird, erlischt auch das

allfällige Nutzungsrecht des Cyber Risk Labels und dieses muss innerhalb von Monatsfrist von allen Unterlagen der Organisation entfernt werden.
Wenn bei einer Organisation zweimal signifikante negative Abweichungen festgestellt werden, so werden von dieser Organisation ab dann nur noch A+ Ratings akzeptiert.

5 Steuerung des Cyber Risk Schemas

Der Owner des Cyber Risk Schemas ist das **Kompetenzzentrum Sicheres Österreich** als neutraler und überparteilicher Verein, der der Erhöhung der Cybersicherheit in Österreich verpflichtet ist. Das KSÖ betreibt dazu gemäß eigener Geschäftsordnung das Cyber Risk Advisory Board, welches sich aus Repräsentanten der NIS-Sektoren zusammensetzt. Diese Repräsentanten sind fachlich qualifiziert und nehmen in ihrem jeweiligen Unternehmen eine verantwortliche Rolle zum Thema Cyber-Risiko ein. Sie bringen ihre Erfahrung und ihr Know-How zur Gestaltung und Weiterentwicklung des Cyber Risk Schemas ein, um dieses bestmöglich an den Sicherheitsanforderungen aus Sicht Betreiber wesentlicher Dienste auszurichten. Der Beschluss des Schemas erfolgt durch das Cyber Risk Advisory Board.
Das operative Management des Schemas erfolgt durch das Cyber Risk Management Board, welches sich aus drei Vertretern der beteiligten Partner zusammensetzt (KSV1870, KSÖ, Cyber Trust Services). Das Cyber Risk Management Board agiert als erste Eskalationsinstanz. Das Cyber Risk Advisory Board ist die zweite und letzte Eskalationsinstanz.

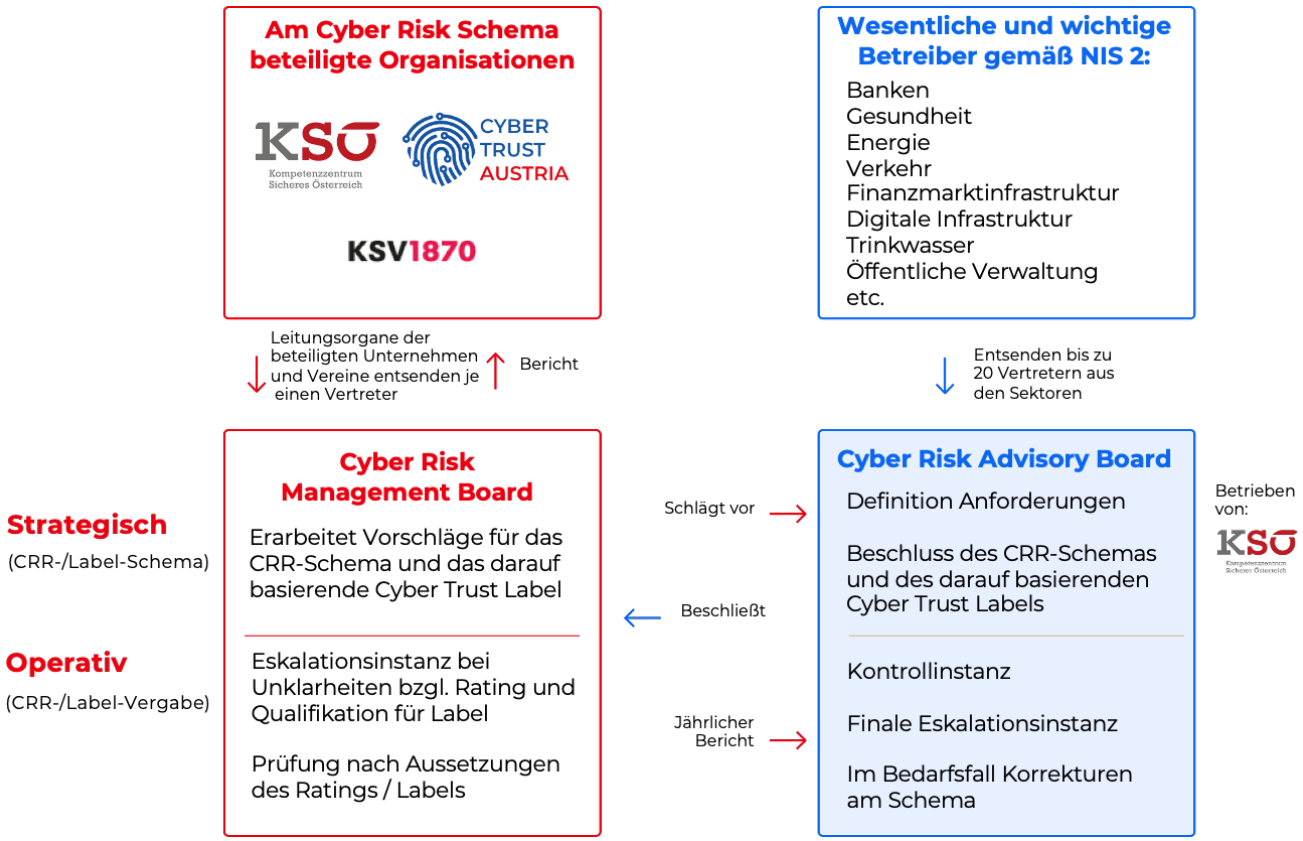

Abb. 1 Governance Modell des Cyber Risk Rating Schemas

6 Durchführung des Cyber Risk Ratings

Grundsätzlich kann jede Organisation einem Cyber Risk Rating unterzogen werden. Die Organisation kann dies selbst anfordern oder es kann von einer anderen Organisation angefordert werden (zum Beispiel im Rahmen einer Lieferantenüberprüfung). Die Teilnahme am Rating ist freiwillig. Wenn eine Organisation einwilligt, unterwirft sie sich der Rating-Vereinbarung mit dem KSV1870 entsprechend der vorliegenden Policy.

6.1 Ablauf der Anforderung eines Cyber Risk Ratings

Wenn ein Dritter das Cyber Risk Rating eines Unternehmens beim KSV1870 anfordert (zum Beispiel im Rahmen seines Lieferantenrisikomanagements) und dieses liegt bisher nicht in der Datenbank vor, so erhält das betroffene Unternehmen ein E-Mail des KSV1870 mit der Bitte, den entsprechenden Fragebogen auszufüllen. Der Name des anfordernden Dritten kann dabei genannt werden. Der KSV1870 bemüht sich nach besten Möglichkeiten, den geeigneten Ansprechpartner zu identifizieren und diesem den Zweck und die Notwendigkeit sowie den Ablauf zu erklären.

- Wenn das Unternehmen mit der Beantwortung der Fragen einverstanden ist, erhält es einen Link zum Portal des KSV1870 und der weitere Ablauf erfolgt wie im Kapitel 3 beschrieben. Das Unternehmen beantwortet alle Fragen nach bestem Wissen und Gewissen und beschreibt zu jeder positiv beantworteten Frage kurz, aber präzise die Art der Umsetzung. Nach erfolgter Validierung erhält das Unternehmen die Möglichkeit auszuwählen, ob in der KSV-Datenbank auch das A Rating angezeigt werden soll (bei Label Kunden ergibt sich dies aus dem angeforderten Label).
- Sofern auch nach dreimaligen telefonischen und elektronischen Kontaktversuchen keine oder eine abschlägige Antwort durch das Unternehmen erfolgt, sendet der KSV1870 als letzte Maßnahme einen eingeschriebenen Brief an die Geschäftsführung mit Darlegung der Sachlage und Bitte, der Aufforderung nachzukommen. Erfolgt auch auf dieses Schreiben innerhalb von zwei Wochen keine positive Reaktion, dann erhält das Unternehmen ein „Null-Rating“ in der Cyber Risk Datenbank, welches entsprechend ausgewiesen wird.

6.2 Voraussetzungen für ein Cyber Risk Rating

Folgende Informationen müssen von einer Organisation, die sich einem Rating unterzieht, verpflichtend angegeben werden:

- Eindeutige Identifikation der bewerteten Organisation (Name, Sitz der Organisation, Firmenbuchnummer bzw. Vereinsnummer o.ä.)
- Ansprechpartner in der Organisation (Name, Funktion, Telefon, E-Mail)
- Angabe aller bekannten, zugehörigen qualifizierten Internet-Domänen (für WebRisk Indicator)

7 Sicherheit der verarbeiteten Daten

Sicherheits- und Risikobewertungen von Organisationen stellen sensible und schützenswerte Daten dar. Dementsprechend werden zum Schutz dieser Daten von allen

beteiligten Partnern des Cyber Risk Ratings entsprechend hohe Sicherheitsmaßnahmen eingehalten. Die detaillierten Bewertungsunterlagen inklusive der vom Kunden zur Verfügung gestellten Angaben werden für die Dauer der Bewertung verschlüsselt auf dem System des KSV1870 gespeichert. Nach Vorliegen des finalen Ratings werden diese Daten der bewerteten Organisation verschlüsselt und signiert zugesandt; gemäß Rating-Vereinbarung ist die bewertete Organisation verpflichtet, diese Unterlagen (ebenso wie die dazugehörigen Evidenzen) zumindest ein Jahr über den Gültigkeitszeitraum des Ratings hinaus aufzubewahren und bei Bedarf vorzuweisen. Die detaillierten Bewertungsunterlagen werden 2 Wochen nach dem Download durch die bewertete Organisation beim KSV1870 gelöscht. Das Rating (sowie die bei Antragstellung getätigten Bestätigungen des Kunden) wird in der Cyber Risk Rating Datenbank des KSV1870 gespeichert und die Berechtigung für das Label samt Nutzungsdauer in der Label-Datenbank der Cyber Trust Services GmbH. Es werden somit keine über den Ansprechpartner hinausgehenden personenbezogenen Daten im Zusammenhang mit dem Cyber Risk Rating oder dem Cyber Trust Label gespeichert. Auditoren werden mittels eines Code of Conduct dazu verpflichtet, ebenfalls alle erhaltenen Unterlagen vertraulich zu behandeln, ausschließlich im Rahmen des Audits zu verwenden und nach Abschluss der Bewertung auf all ihren Systemen zu löschen.

Die gesamte Kommunikation mit der bewerteten Organisation erfolgt verschlüsselt (sofern der Kunde dies unterstützt):

- über TLS verschlüsselte Webseiten bzw.
- über S/MIME verschlüsselte E-Mails.

8 Anhang A: Anforderungen

8.1 Anforderungen für B Rating

Anforderung	Anforderungskriterien
B1 Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für ihr Unternehmen gültig ist?	Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27001/27002, NIST 800, IT-Grundschutz, WKO Basismaßnahmen für Informationssicherheit im Unternehmen). Die Richtlinie muss von der Geschäftsführung freigegeben und für alle Mitarbeiter verfügbar sein. Zumindest alle zwei Jahre muss eine Überprüfung der Aktualität, der Eignung und Wirksamkeit der Sicherheitsmaßnahmen stattfinden und ggf. die Richtlinie angepasst werden.
B2 Schulen Sie ihre Mitarbeiter regelmäßig in Informationssicherheit?	Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen: - Sicherer Umgang mit Computern und Informationen - Passwörter richtig auswählen und verwalten - Sicherer Umgang mit internetbasierenden Diensten und bei Social Media - Sichere Nutzung von KI - E-Mails, Spam und Phishing - Gefährliche Schadprogramme - Verhalten und Vorgehen bei Verdacht auf IT-Sicherheitsvorfall Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.
B3 Gibt es in ihrem Unternehmen eine oder mehrere benannte Personen, die für das Thema Informationssicherheit zuständig sind?	Es muss zumindest eine benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt, sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben und sich laufend über Cyberrisken informieren. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.
B4 Pflegen Sie regelmäßig ein Verzeichnis all ihrer IT-Assets und -Services (inkl. Cloud-Dienste) sowie der damit verbundenen Verantwortlichkeiten?	- Es muss ein Verzeichnis aller verwendeten IT-Assets (Hardware, Software, Netzwerkkomponenten, Dienste, Datenbanken – in der Cloud und on premise; physische und virtuelle Systeme) geben. Dieses Verzeichnis muss zumindest Name und Version des Systems enthalten und den dafür Verantwortlichen. - Das Verzeichnis muss vollständig und aktuell gehalten werden.

B5 Verwalten Sie den Zugang zu ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?	- Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben (Need-to-know). - Es gibt eine dokumentierte Vorgehensweise zur Vergabe und Entzug von Berechtigungen. - Systemadministratoren verfügen über separate, privilegierte Benutzerkonten für administrative Aufgaben (getrennt von ihrem Benutzerkonto für den täglichen Zugriff, E-Mails, Internet etc.).
B6 Setzen Sie angemessene Authentifizierungsmaßnahmen ein?	- Es muss klar beschriebene Sicherheitskriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, keine Mehrfachverwendung von Passworten etc.). Referenz: BSI, NIST 800, etc. - Zumindest bei kritischen Systemen muss MFA (Multi-Faktor Authentisierung) in Verwendung sein.
B7 Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all ihrer IT-Systeme?	Es muss ein Dokument geben, dass die Anforderungen an die sichere Konfiguration der eingesetzten Systeme beschreibt. Verweise auf Herstellerempfehlungen sind ausreichend. Diese Einstellungen müssen auch auf allen verwendeten Geräten - soweit technisch möglich - tatsächlich umgesetzt sein. Alternativ wird ein Schwachstellenscan vor Inbetriebnahme nachweislich durchgeführt.
B8 Überprüfen Sie - sofern vorhanden - individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme (ODER Sie verwenden eine solche Software gar nicht)?	Individualsoftware (zB. angepasste Open-Source-Software, aber nicht Standardsoftware), die aus dem Internet erreichbar ist, muss vor Inbetriebnahme durch einen - auf die Individualsoftware angepassten - Penetration Test (bzw. Code Review) auf Schwachstellen geprüft werden. Wenn Sie solche Software nicht verwenden, dann beantworten Sie diese Frage bitte mit „Ja“ und machen Sie einen kurzen erklärenden Kommentar dazu.
B9 Aktualisieren Sie alle IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?	- Regelmäßige Aktualisierung der Systeme mit Updates, die vom Hersteller zur Verfügung gestellt werden. Kein Sicherheitsupdate darf länger als ein Quartal überfällig sein (außer es gibt einen dokumentierten Grund, warum ein Update nicht eingesetzt werden kann). - Kritische Schwachstellen (CVSS Base Score ≥ 9.0) in exponierten (von außen erreichbaren) Systemen und -Anwendungen werden innerhalb von max. 14 Tagen nach Release gepatcht oder alternativ mitigiert. - Systeme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden, werden rechtzeitig außer Betrieb genommen bzw. es gibt definierte Ausnahmeprozesse inklusive einer Abweichungsliste und kompensierender Maßnahmen.
B10 Sichern Sie ihr Netzwerk vor unberechtigtem Zugriff von außen ab?	Es ist eine Netzwerk-Segmentierungseinrichtung (zB. Firewall, Router, etc.) im Einsatz, die auf Basis möglichst restriktiv gesetzter Regeln den Netzwerkverkehr aus dem Internet in das interne Netzwerk beschränkt.
B11 Überwachen Sie ihre IT-Systeme auf Malware?	Es muss zumindest eine Endpoint Protection im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware überprüft. Diese ist so konfiguriert, dass gefährliche Protokolle, Prozesse und Dateien blockiert und reported werden. Die Software muss laufend aktualisiert werden und diese Aktualisierung zumindest einmal monatlich zentral geprüft

	werden. Es gibt einen bekannten Ablauf zur Behandlung von Sicherheitsvorfällen.
B12 Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?	- Es muss die Möglichkeit bestehen, Dateien verschlüsselt zu übertragen, entweder per E-Mail (zB. S/MIME, PDF verschlüsselt, mandatory enforced TLS, etc.) oder per verschlüsseltem Upload. - Formulardaten auf der Webseite werden ausschließlich über https hochgeladen.
B13 Protokollieren Sie die Nutzung ihrer IT-Systeme, um Sicherheitsvorfälle nachvollziehbar zu machen?	- Es müssen zumindest die Standardprotokolle der Betriebssysteme aktiviert sein, welche sicherheitsrelevant sind. Die Protokolle müssen dem Unternehmen zur Verfügung stehen. - Es existiert eine Übersicht aller aktiven Systemprotokolle die nicht lokal gespeichert werden. - Die Server-Protokolle werden zumindest 90 Tage aufbewahrt, die Client-Protokolle zumindest 60 Tage.
B14 Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?	Der Notfallplan (inkl. Backupkonzept) muss beschreiben, wie auf einen schwerwiegenden IT-Sicherheitsvorfall reagiert wird. Schwerwiegende Sicherheitsvorfälle sind zum Beispiel: - Ausfall der Systeme, - Schadsoftware-Befall (inkl. Ransomware) sowie - Data Leakage - Brand, Wassereintritt und andere physische Vorfälle Die Pläne müssen mindestens alle zwei Jahre getestet werden. Der Test muss zumindest die Daten- und Servicewiederherstellung umfassen.

8.2 Anforderungen für A Rating (zusätzlich zu B)

Anforderung	Anforderungskriterien
A1 Überprüfen Sie IT-Systeme in ihrem Netzwerk auf Sicherheitslücken?	- Ein Tool zum Schwachstellenscannen muss im Einsatz sein und muss mindestens einmal pro Monat verwendet werden. - Der Scan muss alle Geräte der internen IT-Netze sowie aus dem Internet erreichbare IT-Systeme prüfen. - Die Prüfung muss auch nicht-autorisierte Geräte identifizieren. - Es muss einen Prozess geben, der die Erkennung, Entgegennahme und Behandlung von identifizierten Schwachstellen sicherstellt - Aus den gefundenen Sicherheitslücken werden Maßnahmen abgeleitet und umgesetzt.
A2 Haben Sie Mechanismen im Einsatz, die bei der Erstellung bzw. dem Erwerb von individuell entwickelter Software deren Sicherheit überprüfen?	Es gibt eine Policy zur sicheren Software-Entwicklung, welche Sicherheitsanforderungen, Secure-Coding-Rules sowie ein Testkonzept umfasst. Die Policy zur sicheren Software-Entwicklung muss auch das Thema Software Bill of Materials (SBOM) adressieren (es muss klar sein, was in der selbstentwickelten Software verwendet wird). Für den Erwerb von Software gibt es eine Sicherheitsanforderungsliste und einen Prozess zur Risikoanalyse des Anbieters/Herstellers.
A3 Führen Sie in ihrer Systemlandschaft Penetration Tests durch?	- Zumindest alle zwei Jahre werden Penetration Tests durchgeführt, welche die Angreifbarkeit des Unternehmens prüfen. - Aus den gefundenen Schwachstellen werden Maßnahmen abgeleitet und umgesetzt.

A4 Überwachen Sie ihre Systemlandschaft auf ungewöhnliche Aktivitäten und Anomalien?	Es muss mindestens eine Technologie im Einsatz sein, die in der Lage ist, in der Systemlandschaft (Netzwerk, Endpoint, Clients, Server, Cloud) Intrusions oder Anomalien zu erkennen und zentral zu melden.
A5 Haben Sie Whitelisting und Cloud Access Security Broker (CASB) im Einsatz, um die Ausführung nicht autorisierter Prozesse und Anwendungen zu unterbinden?	- Auf allen Clients und Servern muss eine Technologie aktiv sein, damit nur freigegebene Prozesse und Anwendungen ausgeführt werden können. - Nur freigegebene Cloud-Anwendungen können ausgeführt werden (zB. über einen CASB, SASE, o.ä.). - Nicht bekannte Aktivitäten werden verhindert, gemeldet und den Meldungen wird nachgegangen.
A6 Schützen Sie Identitäten, Zugriffe und Berechtigungen in geeigneter und nachvollziehbarer Weise?	- Eine Identitäts- und Berechtigungsverwaltung ist im Einsatz, die alle Identitäten und deren Berechtigungen eindeutig auf Personenbasis nachvollziehbar macht. - Die Berechtigungsverwaltung muss auch administrative Berechtigungen sowie Berechtigungen für Zugänge zu Kundensystemen umfassen. - Verwendung von Multifaktor-Authentifizierung, insbesondere für alle von extern erreichbaren Systemen wie zB. VPN, Jumphosts, Remote Support Tools, Webmail und andere Webservices sowie für alle privilegierten Accounts. - Bei Zugriff auf Unternehmensressourcen von Geräten, die nicht vom Unternehmen gemanagt werden, muss dies über Jumphosts oder virtualisierte Systeme erfolgen.
A7 Haben Sie Technologie im Einsatz, die die Log Files ihrer Systeme automatisiert korreliert und analysiert?	Es ist eine Technologie (zB. SIEM) im Einsatz, an die zumindest die kritischen Netzwerk- und Sicherheitssysteme angeschlossen sind und deren Logfiles laufend korreliert und auf Unregelmäßigkeiten analysiert werden. Die Systemzeiten der genutzten Systeme müssen über gängige Mechanismen synchronisiert sein und dürfen nicht mehr als eine Sekunde abweichen.
A8 Haben oder nutzen Sie ein Security Operations Team?	- Die notwendigen qualifizierten Daten für das Monitoring müssen zur Verfügung stehen. - Es müssen Mitarbeiter mit nachgewiesenen Qualifikationen im Bereich IT-Sicherheit im Unternehmen beschäftigt sei, die die laufende und zeitnahe Überwachung und Bewertung von Security-Events wahrnehmen oder es muss ein SLA/Vertrag mit einem entsprechenden Unternehmen bestehen, das die laufende Überwachung übernimmt. - Es ist sicherzustellen, dass auch neue Angriffsmuster und Bedrohungen durch das SOC erkannt werden - Verdachtsfälle müssen untersucht werden und bei bestätigten Vorfällen muss eine Alarmierung stattfinden sowie – sofern relevant – betroffene Kunden informiert werden.
A9 Können Sie bei einem schwerwiegenden Sicherheitsvorfall auf qualifizierte Ressourcen zurückgreifen?	Es müssen Mitarbeiter mit nachgewiesenen Qualifikationen in den Bereichen vertiefte Incident Response und IT-Forensik im Unternehmen beschäftigt sein oder es muss ein SLA/Vertrag mit einem entsprechenden Unternehmen bestehen, bzw. der Zugriff auf ein solches muss über eine Cyberversicherung gedeckt sein.
A10 Stellen Sie über ein getestetes Resilienzkonzept oder eine resiliente	- Es muss ein geeignetes Resilienzkonzept dokumentiert sein welches sicherstellt, dass Businessservices (auch bei Kompromittierung in der Cloud) wiederhergestellt werden können.

Architektur ihre Betriebskontinuität sicher?	- Das Resilienzkonzept muss auf einer Szenarioanalyse basieren und präventive und reaktive Maßnahmen umfassen, um auf für das Unternehmen relevante schwere IT-Sicherheitsvorfälle reagieren zu können und somit Betriebskontinuität sicherzustellen. Schwerwiegende IT-Sicherheitsvorfälle sind unter anderem: - Ausfall der Systeme (inkl. Stromausfall, Ausfall der Internetanbindung) - Ausfälle durch physische Einflüsse (zB. Feuer oder Wasser im RZ) - Schadsoftwarebefall (inkl. Kryptolocker) - Data Leakage - Zielgerichtete Hackingangriffe (z.B. APTs) - Das Backup muss auch gegen Kompromittierung geschützt sein - Bei Betrieb kritischer Anwendungen in der Cloud müssen diese Maßnahmen und Tests vom Cloud-Betreiber nachgewiesen werden (zB. über ISAE 3402-Berichte). - Tests müssen mindestens einmal jährlich durchgeführt und notwendige Verbesserungsmaßnahmen umgesetzt werden.
A11 Haben Sie einen Prozess zum Management ihrer Lieferantenrisiken?	Es muss einen dokumentierten Prozess geben, welcher vorab und laufend sicherstellt, dass Lieferanten ihre Cyberrisiken ebenfalls angemessen managen.

8.3 Prüfkriterien für WebRisk Indicator

1. Indikatoren für IT-Sicherheitsvorfälle
    - Malwareverteilung
    - Defacements
2. Indikatoren für Qualität der Verschlüsselung
    - SSL-Ciphersuite
    - SSL-Gültigkeit
    - SSL-Hostname
    - SSL-Trustlevel
3. Prüfung auf effektive Nutzung Indikatoren für Mitigation von IT-Sicherheitsvorfällen
    - Security-Header Implementierung
4. Indikatoren für IT-Reputation
    - Blacklisting von eigenen Domains
    - Blacklisting von fremden Domains, auf die eigene Domains verlinken

8.4 Anforderungen für das Platinum Label

Nr.	Anforderung
1.1	Bitte beschreiben Sie ihr **Regelwerk** (zB. Informationssicherheitsrichtlinie, Policy o.ä.), und inwiefern dieses die Ziele der Sicherheit ihrer Netz- und Informationssysteme inklusive Maßnahmen zur Umsetzung adressiert, allen Mitarbeitern bekannt und von der obersten Geschäftsleitung formal beschlossen ist.
1.2	Bitte beschreiben Sie ihre **Rollen und Verantwortlichkeiten** für Informationssicherheit und ob eine Person gegenüber den Leitungsorganen direkt für Fragen der Sicherheit von Netz- und Informationssystemen verantwortlich ist.

2.1	Bitte beschreiben Sie ihr **Informationssicherheits-Risikomanagementsystem**, und inwiefern dieses in das Gesamtrisikomanagement des Unternehmens integriert ist und dabei sämtliche für das Unternehmen relevanten Informationssicherheitsrisiken identifiziert, bewertet und in angemessener Weise behandelt.
2.2	Bitte beschreiben Sie, ob und wie Sie regelmäßig die **Einhaltung ihrer Konzepte, Vorgaben und Richtlinien** zur Informationssicherheit überprüfen und ob Sie die Ergebnisse an ihre oberste Geschäftsleitung berichten.
2.3	Bitte beschreiben Sie, ob und wie Sie regelmäßig **unabhängige Überprüfungen** ihres Ansatzes für das Management der Sicherheit von Netz- und Informationssystemen und dessen Umsetzung vornehmen lassen und die Ergebnisse an ihre oberste Geschäftsleitung berichten.
3.1	Bitte beschreiben Sie ihr Konzept bzw. ihren **Prozess zur Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen**, die zugehörigen Verantwortlichkeiten, und wie sie dies in regelmäßigen Abständen testen und aktualisieren.
3.2	Bitte beschreiben Sie, welche **Protokollierungsmaßnahmen** bei ihren Systemen eingerichtet sind, welche Ereignisse diese umfassen und ob und wie sie diese in kontinuierlicher Art und Weise überwachen? Bitte machen Sie dabei auch Angaben zur Aufbewahrungsdauer der Protokolle.
3.3	Bitte beschreiben Sie den Mechanismus wie verdächtige Ereignisse bei ihnen **gemeldet** werden können und inwiefern Anbieter und Kunden über diesen Mechanismus zur Einmeldung informiert werden.
3.4	Bitte beschreiben Sie ihren Mechanismus zur **Bewertung und Klassifizierung von Ereignissen**.
3.5	Bitte beschreiben Sie wie Sie zeitnahe auf **Sicherheitsvorfälle reagieren**, ihre Reaktion dokumentieren und dabei ihren eigenen Verfahrensrichtlinien bei Sicherheitsvorfällen gemäß 3.1 folgen.
3.6	Bitte beschreiben Sie, ob und wie Sie nach Sicherheitsvorfällen eine **Nachbetrachtung** durchführen, dabei die Ursachen des Vorfalls und die Angemessenheit ihrer Reaktion betrachten und daraus ggf. Verbesserungen für die Zukunft ableiten.
4.1	Bitte beschreiben Sie ihren **Notfallplan** für die Aufrechterhaltung und Wiederherstellung des Betriebs, und inwiefern dieser auf einer Szenarioanalyse und einer Auswirkungsanalyse (BIA) beruht sowie regelmäßig getestet und aktualisiert wird.
4.2	Bitte beschreiben Sie ihr **Backup- und Redundanz-Konzept**, das ihnen die gemäß Risikoanalyse erforderlichen Wiederherstellungszeiten ermöglicht und inwiefern sie die Wirksamkeit testen.
4.3	Bitte beschreiben Sie ihr **Krisenmanagement** inklusive geeigneter Rollen und Verantwortlichkeiten und Kommunikationsmittel und inwiefern dieses regelmäßig getestet und aktualisiert wird.
5.1	Bitte beschreiben Sie ihr Vorgaben bzw. **Prozess für die Sicherheit der Lieferkette** und inwiefern dieses auf Basis einer Risikobewertung die Qualität und Resilienz der IKT-Produkte und -Dienste im Bereich der Cybersicherheit bei ihren direkte Lieferanten überprüft und auch vertraglich einfordert.
5.2	Bitte beschreiben Sie ihr **Verzeichnis ihrer Anbieter und Diensteanbieter** und inwiefern dieses alle IKT-Produkte, -Dienste und -Prozesse umfasst.
6.1	Bitte beschreiben Sie ihr Verfahren zur Sicherstellung geeigneter **Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten**, inklusive definierter Sicherheitsanforderungen.
6.2	Bitte beschreiben Sie ihre Vorgaben und zugehörigen **Prozess zur sicheren Softwareentwicklung**, und inwiefern dieser alle Entwicklungsphasen umfasst, einschließlich Spezifikation, Konzeption, Entwicklung, Umsetzung und Tests.
6.3	Bitte beschreiben Sie ihr **Konfigurationsmanagement**, und inwiefern dieses Sicherheitskonfigurationen von Hardware, Software, Diensten und Netzen festlegt, dokumentiert, umsetzt und überwacht.
6.4	Bitte beschreiben Sie ihr **Änderungsmanagement**, und inwiefern dieses geplante und ungeplante Änderungen (Emergency Changes) an den Netz- und Informationssystemen vor ihrer Umsetzung auf ihre Risiken überprüft.

6.5	Bitte beschreiben Sie ihre **Vorgaben und Verfahren für Prüfungen** der Sicherheit, inwiefern dieses auf Basis einer Risikobewertung (gemäß 2.1) beruht und daraus ggf. Risikominderungsmaßnahmen angewendet werden.
6.6	Bitte beschreiben Sie ihr **Sicherheits-Patchmanagement** und inwiefern dieses die Anwendung von Sicherheits-Patches innerhalb einer angemessenen Frist sicherstellt.
6.7	Bitte beschreiben Sie ihre **Maßnahmen für Netzwerksicherheit** und inwiefern diese die Kommunikation innerhalb ihres Netzes sowie den Zugriff von außen auf das notwendige Minimum beschränken und dabei auch die Integrität und Vertraulichkeit auf Netzwerkebene sicherstellen.
6.8	Bitte beschreiben Sie wie sie eine **Netzwerksegmentierung** umgesetzt haben und inwiefern diese in geeigneter Weise Systeme unterschiedlicher Sicherheitsanforderungen voneinander trennt.
6.9 a	Bitte beschreiben Sie inwiefern sie Software zur **Erkennung und Verhinderung von Schadsoftware** verwenden.
6.9 b	Bitte beschreiben Sie inwiefern sie Software zur **Erkennung und Verhinderung von nicht genehmigter Software** verwenden.
6.10	Bitte beschreiben Sie ihre Verfahren zur **Erkennung, Bewertung und Behandlung von Schwachstellen**.
7.1	Bitte beschreiben Sie ihre Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Cybersicherheit.
8.1	Bitte beschreiben Sie ihre **Sensibilisierungsmaßnahmen** und inwiefern diese sicherstellen, dass sich ihre Mitarbeiter, einschließlich der Mitglieder von Leitungsorganen, der Risiken der Cybersicherheit bewusst sind und grundlegende Verfahren der Cyberhygiene anwenden.
8.2	Bitte beschreiben Sie ob und inwiefern sie **rollenspezifische Sicherheitsschulungen** durchführen, welche alle für die jeweilige Rolle erforderlichen sicherheitsrelevante Fähigkeiten und Fachkenntnisse vermitteln.
9.1	Bitte beschreiben Sie ihre Konzepte und Verfahren in Bezug auf **Kryptografie** und inwiefern diese Art, Stärke und Qualität der kryptografischen Maßnahmen sowie des Schlüsselmanagements definieren.
10.1	Bitte beschreiben Sie wie Sie gewährleisten, dass ihre Mitarbeiter und gegebenenfalls ihre direkten Anbieter und Diensteanbieter ihre **Verantwortlichkeiten** gemäß ihrer Rollen im Bereich der Sicherheit verstehen und einhalten.
10.2	Bitte beschreiben Sie ob und wie Sie **Backgroundchecks** ihrer Mitarbeiter durchführen, wenn dies für ihre Rolle erforderlich ist.
10.3	Bitte beschreiben Sie ihre **vertraglichen Festlegungen** mit ihren Mitarbeitern betreffend Sicherheit und Vertraulichkeit und ob diese auch nach Beendigung des Beschäftigungsverhältnisses oder des Vertrags gültig bleiben.
10.4	Bitte beschreiben Sie ob und welche **Verfahren** sie für den Umgang mit Verstößen gegen die Konzepte für die Sicherheit von Netz- und Informationssystemen haben.
11.1	Bitte beschreiben Sie ihr Konzept für die **logische und physische Kontrolle des Zugangs** zu ihren Netz- und Informationssystemen für alle Personen und wie dieses eine angemessene Authentifizierung vorsieht.
11.2	Bitte beschreiben Sie ob und inwiefern sie ein dokumentiertes und protokolliertes **Management von Zugangs- und Zugriffsrechten** haben, welches Rechte nur gemäß von „Need-to-know“ und „Need-to-use“ vergibt und auch wieder entzieht.
11.3	Bitte beschreiben Sie ihr Konzept zum **Management von privilegierten Konten** und Systemverwaltungskonten haben, welches Systemverwaltungsrechte so weit wie möglich individuell festlegt und einschränkt und starke Authentifizierungsverfahren (zB. Multifaktor-Authentifizierung) vorsieht.
11.4	Bitte beschreiben Sie ob sie **Systemverwaltungssysteme** ausschließlich für die Zwecke der Systemverwaltung verwenden und wie sie den Zugang zu diesen durch Authentifizierung und Verschlüsselung schützen.

11.5	Bitte beschreiben Sie ob und inwiefern sie **Identitäten** über ihren gesamten Lebenszyklus hinweg verwalten und sicherstellen, dass jede Kennung immer mit einem eindeutigen Nutzer verbunden ist bzw. bei (unbedingt erforderlichen) gemeinsamen Kennungen eine Genehmigung und Nachvollziehbarkeit der Verwendung gewährleistet ist.
11.6	Bitte beschreiben Sie welche sichere **Authentifizierungsverfahren** sie verwenden und inwiefern diese Authentifizierungsverfahren der Kritikalität der zugegriffenen Assets angemessen sind.
11.7	Bitte beschreiben Sie ob und inwiefern sie **Multifaktor-Authentifizierung** verwenden, wenn es der Kritikalität der zugegriffenen Assets angemessen ist.
12.1	Bitte beschreiben Sie wie sie eine laufende **Asset-Klassifizierung** durchführen, welche für alle Assets auf Basis von Vertraulichkeits-, Integritäts-, Authentizitäts- und Verfügbarkeitsanforderungen den entsprechend ihrer Kritikalität und ihres Risikos erforderlichen Schutz angibt.
12.2	Bitte beschreiben Sie ihr Konzept für die ordnungsgemäße Behandlung von Assets (einschließlich Informationen) über ihren gesamten **Lebenszyklus** (einschließlich Erwerb, Verwendung, Speicherung, Transport und Entsorgung) hinweg, auf Basis der Klassifikation der Assets.
12.3	Bitte beschreiben Sie ihr Konzept für das **Management von Wechseldatenträgern** im Hinblick auf Sicherheit.
12.4	Bitte beschreiben Sie wie sie ein vollständiges, genaues, aktuelles und kohärentes **Inventar ihrer Assets** pflegen.
12.5	Bitte beschreiben Sie wie Sie die Abgabe, **Rückgabe oder Löschung von Assets** bei Beendigung von Beschäftigungsverhältnissen auf dokumentierte Weise sicherstellen.
13.1	Bitte beschreiben Sie ihr Konzept und ihre **Maßnahmen zur Verhinderung der Unterbrechungen ihres Betriebs** aufgrund des Ausfalls bzw. der Störung unterstützender Versorgungsleistungen wie zum Beispiel Strom und Telekommunikation und inwiefern sie diese regelmäßig testen.
13.2	Bitte beschreiben Sie ihr **Konzept zum Schutz vor physischen Bedrohungen und Bedrohungen** aus dem Umfeld und inwiefern sie dieses regelmäßig testen.
13.3	Bitte beschreiben Sie ob und inwiefern sie ihren **Perimeter** schützen und mit geeigneten Maßnahmen unbefugten physischen Zutritt zu, Beschädigungen von und Eingriffe in ihre Netz- und Informationssysteme verhindern und inwiefern sie diese Schutzmaßnahmen regelmäßig testen.

9 Anhang C: Qualifikationen

9.1 Mindestanforderung an Auditoren

Auditoren müssen benannte Mitarbeiter von Unternehmen sein, die gemäß Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz (Verordnung über qualifizierte Stellen – QuaSteV) vom Bundesministerium für Inneres akkreditiert sind.

9.2 Mindestanforderung an Validierer

Die Validierung der Selbstdeklarationen erfolgt durch die Cyber Trust Services GmbH. Mit der Validierung befasste Personen müssen mindestens eine gängige Personenzertifizierung im Bereich Cybersicherheit besitzen und über mindestens 3 Jahre Berufserfahrung in diesem Bereich verfügen.

10 Anhang D: Begriffsbestimmungen

Cyber Risk Rating
Kennzahl, die sich aus der Auswertung der Konformitätsbewertung ergibt und eine Aussage über den Cyber Risiko Status des bewerteten Unternehmens gibt. Der Eigentümer der Cyber Risk Ratings ist der KSV1870.

Cyber Trust Austria Label
Gütesiegel, das auf Basis des Cyber Risk Ratings erstellt und vergeben wird, sofern die erforderlichen Anforderungen erfüllt sind. Der Eigentümer und Issuer des Cyber Trust Austria Labels ist die CTS Cyber Trust Services GmbH.

Eigentümer (Scheme-Owner)
Organisation, die für die Entwicklung und Instandhaltung des Programmes (Schemas) verantwortlich ist. Schema Owner des Cyber Risk Ratings und des darauf basierenden Cyber Trust Labels ist das Kompetenzzentrum Sicheres Österreich (KSÖ).

Rating-Vereinbarung
Rechtlich verbindliche Vereinbarung zwischen dem Eigentümer des Cyber Risk Ratings und dem bewerteten Unternehmen, welche die Rechte und Pflichten des bewerteten Unternehmens hinsichtlich der Konformitätsbewertung im Rahmen der Cyber Risk Rating Erstellung und der Überwachung festhalten.

Label-Nutzungsvertrag
Vertragliche Vereinbarung zwischen dem Eigentümer des Cyber Trust Austria Labels und dem bewerteten Unternehmen, welche die Bedingungen zur Nutzung des Labels rechtsverbindlich festlegen.

Anforderung (Specified requirement)
Erfordernis oder Erwartung, das oder die niedergelegt ist. Im Rahmen des Cyber Risk Rating sind die Anforderungen in den Fragekatalogen für das A- bzw. B Rating spezifiziert.

Audit (Audit)
Prozess zum Erlangen relevanter Informationen über einen Gegenstand der Konformitätsbewertung und zu dessen objektiver Auswertung, um zu ermitteln, inwieweit die festgelegten Anforderungen erfüllt sind. Ein Audit erfolgt im Rahmen einer Inspektion.

Bewertung (Review)
Erwägung, ob die Auswahl- und Ermittlungstätigkeiten und deren Ergebnisse hinsichtlich der Erfüllung der festgelegten Anforderungen durch den Gegenstand der Konformitätsbewertung geeignet, angemessen und wirksam sind. Beim Cyber Risk Rating erfolgt die Bewertung im Rahmen der Validierung der Selbstdeklaration bzw. des Audits der bewerteten Organisation.

Validierung (Validation)
Bestätigung der Plausibilität eines bestimmten Anwendungszwecks durch Bereitstellung eines objektiven Nachweises, dass die festgelegten Anforderungen erfüllt sind. Im Rahmen des Cyber Risk B Ratings bezieht sich die Validierung auf die Selbstdeklaration der bewerteten Organisation. Im Rahmen des Cyber Risk A Ratings bezieht sich die Validierung auf den durch den Audit-Partner erstellten Bericht zur Konformität der bewerteten Organisation.

Überwachung (Surveillance)
Systematisch sich wiederholende Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Konformitätsaussage. Im Rahmen des CRR-Schemas sind die Konformitätsbewertungen einmal jährlich zu erneuern.

Inspektion (Inspection)
Untersuchung eines Gegenstands der Konformitätsbewertung und Ermittlung seiner Konformität mit detaillierten Anforderungen, auf der Grundlage einer sachverständigen Beurteilung.

Konformitätsbewertung (Conformity assessment)
Darlegung, dass festgelegte Anforderungen erfüllt sind. Konformitätsbewertung beruht auf überprüfenden Tätigkeiten, wie unter anderem Inspektion und Validierung.

Konformitätsbewertungsprogramm (Conformity assessment scheme)
Regeln und Verfahren, die den Gegenstand der Konformitätsbewertung beschreiben, die festgelegten Anforderungen identifizieren und die Vorgehensweise zur Durchführung der Konformitätsbewertung beschreibt. Die vorliegende Schema-Policy beschreibt das Konformitätsbewertungsprogramm (Schema) für das Cyber Risk Rating (CRR) und das Cyber Trust Label.

Gegenstand der Konformitätsbewertung (Object of conformity assessment)
Einheit, auf die sich die definierten Anforderungen beziehen. Dies können unter anderem Produkte, Prozesse oder Organisationen sein. Im Rahmen des CRR-Schemas ist der Gegenstand der Konformitätsbewertung immer eine Organisation (ein Unternehmen), definiert durch ihre Firmenbuchnummer.

Konformitätsbewertungsstelle (Conformity assessment body)
Stelle, die Konformitätsbewertungstätigkeiten durchführt. Im Rahmen des CRR-Schemas werden die Validierungstätigkeiten auf Basis der Selbstdeklarationen von der CTS Cyber Trust Services GmbH durchgeführt. Die dem A Rating zugrundeliegenden Audits werden durch qualifizierte Audit Partner durchgeführt, welche gemäß NIS-Verordnung als qualifizierte Stellen akkreditiert sind.

Konformitätsbewertungstätigkeit durch eine erste Seite (First-party conformity assessment activity)
Tätigkeit, durchgeführt von der Organisation, die Gegenstand der Konformitätsbewertung ist. Im Rahmen des Cyber Risk B Ratings ist dies die Selbstdeklaration durch die bewertete Organisation (das Unternehmen) selbst.

Konformitätsbewertungstätigkeit durch eine dritte Seite (Third-party conformity assessment activity)
Tätigkeit, durchgeführt von einer Person oder einer Organisation, die nicht Gegenstand der Konformitätsbewertung ist und von dieser unabhängig ist und somit kein Interesse als Kunde oder Lieferant an dieser Organisation hat. Im Rahmen des Cyber Risk A Ratings ist dies ein Audit durch einen unabhängigen qualifizierten Audit-Partner.

Einspruch (Appeal)
Verlangen des Gegenstandes der Konformitätsbewertung (bewerteter Organisation) gegenüber einer Konformitätsbewertungsstelle, ihre Entscheidung bezüglich dieses Gegenstandes zu überprüfen

Aussetzung (Suspension)
Vorübergehende Beschränkung der Konformitätsaussage durch die Stelle, die die Konformitätsaussage erstellt hat. Zu einer Aussetzung kommt es bei begründetem Zweifel an der Stichhaltigkeit der Bewertung.

Zurückziehung (Withdrawal)
Widerruf der Konformitätsaussage durch die Stelle, die die Konformitätsaussage erstellt hat. Zu einer Zurückziehung kommt es, wenn begründete Zweifel an der Stichhaltigkeit der Bewertung nicht ausgeräumt werden können.

Ablauf (Expiry)
Ende der Validität der Konformitätsaussage nach einem festgelegten Zeitraum. Das reguläre Ablaufdatum beträgt ein Jahr nach Ausstellung der Bewertung.

Wiederherstellung (Restoration)
Wiedereinsetzung der vollständigen oder teilweisen Konformitätsaussage nach Aussetzung.