BYGHT

Einführung eines ISMS gemäß ISO 27001 in kleinen und mittelständischen Unternehmen

White Paper | Juni 2020

Dieses White Paper liefert ein „Erfolgsrezept" zur Einführung eines ISMS in kleinen und mittelständischen Unternehmen (KMU). Die Autoren beschreiben die Kernprozesse eines ISMS und geben wertvolle Tipps aus der Praxis.
Nach dem Lesen dieses White Papers sind Sie bestens für die Planungsphase zum Aufbau eines ISMS gerüstet und gelangen mithilfe eines Fragenkatalogs zu einer ersten Selbsteinschätzung zum Erfüllungsgrad in Ihrer Organisation.

INHALT

Einleitung

EIN GUTES ISMS IST IN ERSTER LINIE WIRKSAM

Die Etablierung eines zertifizierungsfähigen ISMS fordert u. a. die Erstellung vieler neuer Dokumente. Zudem ist das Schaffen von Sicherheitsbewusstsein und die Etablierung neuer Prozesse im Unternehmen unumgänglich. Eine Herausforderung gerade für KMUs, bei denen Ressourcen oft knapp bemessen sind.

Der Markt für Sicherheitsexperten, die die genannten Aufgaben im Unternehmen übernehmen können, ist überschaubar – um es positiv auszudrücken. Eine kostenintensive, externe Beratung und komplexe, teure ISMS-Tools scheinen unumgänglich. In diesem Whitepaper wollen wir einen alternativen Weg aufzeigen und KMUs einen „roten Faden" an die Hand geben, der Ihnen dabei hilft, ein angemessenes ISMS zu etablieren. Getreu dem Motto: „So viel wie nötig, so wenig wie möglich". Das bedeutet nicht, auf angemessene Sicherheit zu verzichten, jedoch sollte ein ISMS dem Kerngeschäft nicht im Wege stehen, sondern dabei unterstützen, es so sicher wie möglich zu gestalten.

Wichtig ist es, anzufangen und nicht den scheinbar unüberwindbaren Berg einer ISO-27001-Zertifizierung vor sich herzuschieben.

Grundsätzlich setzen wir beim Aufbau und Betrieb eines ISMS auf eine kollaborative und agile Arbeitsweise. Weniger komplexe Tools, weniger individuelle Behelfslösungen in riesigen Excel-Sheets. Wichtig ist es, anzufangen und nicht den scheinbar unüberwindbaren Berg einer ISO-27001-Zertifizierung vor sich herzuschieben.

Schließlich geht es darum, sich ständig zu verbessern und nicht zum Zertifizierungsaudit bei 100 % zu sein. Denn eines ist ganz klar: 100 % Sicherheit gibt es nicht. Bei dem Betrieb eines ISMS sollten in erster Linie Verbesserungsmöglichkeiten identifiziert und strukturiert umgesetzt werden. Wenn dem Auditor dieser Antrieb im Audit nachgewiesen werden kann, ist bereits vieles erreicht.

So viel wie nötig, so wenig wie möglich

Neben einer Zertifizierung nach ISO 27001 ist die stetig steigende Bedrohungslage ein weiteres gutes Argument, mehr Zeit und Gedanken in die Sicherheitsstruktur des Unternehmens zu stecken. Wenn es gelingt, durch die Implementierung angemessener technischer sowie organisatorischer Sicherheitsmaßnahmen Unternehmensschäden wie Imageverlust, Datenverlust sowie Ausfälle im Geschäftsbetrieb zu verringern, ist nicht nur der Auditor, sondern auch das Management glücklich. Ein gutes ISMS ist in erster Linie also wirksam, und erst dann geht es darum, alle Normanforderungen zu erfüllen. Ein guter Auditor sieht das und lässt es in die Bewertung einfließen. Wie gesagt, verbessern kann man sich immer noch – bis zum Überwachungsaudit im nächsten Jahr.

Aber natürlich gibt es dennoch einige „harte Fakten", die nötig sind, um ein ISMS-Audit nach ISO 27001 zu bestehen. Die wirklich nötigen und wirksamen werden im Folgenden dargestellt und beschrieben.

Inhalt und Aufbau der ISO 27001

KAPITEL 4–10

Die ISO 27001:2013 ist eine internationale Norm, die die Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS beschreibt.

Die Norm ist in zwei Bereiche aufgeteilt: den obligatorischen Managementrahmen und den Anhang A. Im Gegensatz zu den Controls (Maßnahmen) des Norm-Anhangs A, die im Rahmen der Anwendbarkeitserklärung (siehe unten) begründet abgewählt werden können, ist die Umsetzung der Vorgaben aus den Kapiteln 4–10 verpflichtend. Anhand der folgenden Tabelle können Sie zu einer ersten Selbsteinschätzung des Erfüllungsgrads in Ihrer Organisation gelangen.

Kapitel 4–10

Die Kapitel 1–3 der Norm befassen sich mit grundlegenden Dingen, zu denen keine Notwendigkeit einer Umsetzung besteht. Die Abschnitte 4–10 müssen obligatorisch umgesetzt werden.

HINWEIS: Lassen Sie sich durch die Jahreszahlen in den Versionsnummern der Norm nicht irritieren. Teilweise ist auch von der ISO 27001:2015 oder der ISO 27001:2017 die Rede. Hier sind lediglich die deutschen Übersetzungen gemeint. Grundlage der Zertifizierung ist aber nach wie vor die englische Version aus dem Jahr 2013.

Kapitel	Fragen
4. Kontext der Organisation	1. Wurden interessierte Parteien festgelegt und deren (potenzielle) Auswirkung auf das ISMS dokumentiert? 2. Wurde der Geltungsbereich des ISMS definiert? 3. Wurden die gesetzlichen Anforderungen im Kontext des ISMS identifiziert?
5. Führung	1. Wird die Geschäftsführung ihrer Verpflichtung gerecht, u. a. durch: • die Festlegung einer Strategie zur Informationssicherheit, • die Integration des ISMS in Geschäftsprozesse, • die Zurverfügungstellung der erforderlichen Ressourcen, • die Messung der Wirksamkeit und kontinuierlichen Verbesserung des ISMS und • die Sensibilisierung der Mitarbeiter auf allen Ebenen? 2. Hat die Geschäftsführung eine Leitlinie zur Informationssicherheit verabschiedet und bekannt gemacht? 3. Hat die Geschäftsführung Rollen, Verantwortlichkeiten und Befugnisse im Rahmen des ISMS benannt und erhält Berichte von diesen?

Kapitel	Fragen
6. Planung	1. Wurden Maßnahmen im Umgang mit den identifizierten Risiken und Chancen festgelegt? 2. Wurde ein Prozess zur Identifikation, Bewertung und zur Behandlung von Informationssicherheitsrisiken festgelegt? 3. Ist eine Anwendbarkeitserklärung zum Anhang A dokumentiert? 4. Wurden Ziele des ISMS bestimmt und ein Plan zu deren Erreichung festgelegt?
7. Unterstützung	1. Wurden die notwendigen Ressourcen für das ISMS bereitgestellt? 2. Haben die relevanten Personen die erforderlichen Kompetenzen, um ihren Rollen im Rahmen des ISMS gerecht zu werden? 3. Sind alle Mitarbeiter sensibilisiert in Bezug auf • die ISMS-Leitlinie, • ihre Mitwirkungspflicht im Rahmen des ISMS und • die Konsequenzen der Nichterfüllung von ISMS-Vorgaben? 4. Wurde im Rahmen des ISMS die interne und externe Kommunikation bestimmt? 5. Werden die von der Norm geforderten Informationen und Nachweise zur Messung der Wirksamkeit des ISMS dokumentiert und gelenkt?
8. Betrieb	1. Die Organisation muss zur Planung und Steuerung eine Reihe von Prozessen festlegen und diese dokumentieren. Dazu zählt jeweils ein Prozess • zur Erfüllung der Anforderungen der Informationssicherheit, • zur Steuerung von Maßnahmen, • zur Steuerung von Aufgaben, die an Dienstleister ausgelagert wurden und • zur Berücksichtigung der Informationssicherheit innerhalb geplanter Änderungen. 2. Wird in regelmäßigen Abständen und bei signifikanten Anpassungen eine Risikobeurteilung durchgeführt? 3. Wird eine Risikobehandlung durchgeführt?
9. Bewertung der Leistung	1. Gibt es einen Prozess zur Überwachung der Wirksamkeit des ISMS? 2. Werden regelmäßig interne Audits durchgeführt? 3. Ist ein Auditprogramm aufgestellt? 4. Wird regelmäßig eine Managementbewertung durchgeführt, die mindestens die in *Kapitel 9.3 der Norm* enthaltenen Punkte berücksichtigt?
10. Verbesserung	1. Wird adäquat mit Maßnahmen auf eine Nichtkonformität mit den Anforderungen des ISMS reagiert? 2. Werden die festgestellten Maßnahmen im Hinblick auf deren Notwendigkeit bewertet, ggf. eingeleitet und entsprechend ihrer Wirksamkeit überprüft? 3. Wird im Rahmen des ISMS eine kontinuierliche Verbesserung sichergestellt?

Inhalt und Aufbau der ISO 27001

ANHANG A

Neben diesen zehn Kapiteln hat die ISO/IEC 27001:2013 auch einen Anhang A, der 114 spezifische Maßnahmen enthält. Diese sind in die folgenden 14 Kategorien eingeteilt:

Kapitel		Anzahl der Maßnahmen
A.5	Informationssicherheitsrichtlinien	2
A.6	Organisation der Informationssicherheit	7
A.7	Personalsicherheit	6
A.8	Verwaltung der Werte	10
A.9	Zugangssteuerung	14
A.10	Kryptographie	2
A.11	Physische und umgebungsbezogene Sicherheit	15
A.12	Betriebssicherheit	14
A.13	Kommunikationssicherheit	7
A.14	Anschaffung, Entwicklung und Instandhalten von Systemen	13
A.15	Lieferantenbeziehungen	5
A.16	Handhabung von Informationssicherheitsvorfällen	7
A.17	Informationssicherheitsaspekte beim Business Continuity Management	4
A.18	Compliance	8

Erfolgsrezept

DOKUMENTATION UND ORGANISATION

„Dokumentation" bedeutet für ein ISMS nach ISO 27001 insbesondere das Erstellen von Richtlinien zur Informationssicherheit. Es gibt einige obligatorische Richtlinien, die in einem Audit vorgelegt werden müssen.

Über den Umfang dieser Richtlinien sagt die Norm selbst jedoch nichts aus. Ganz im Gegenteil: In der Norm wird explizit erwähnt, dass sich der Umfang dokumentierter Informationen von Organisation zu Organisation unterscheiden kann. Hier kommt es insbesondere auf die Unternehmensgröße und die Art der Produkte und Dienstleistungen an. Das sollte der Verantwortliche für die Informationssicherheit bei einem KMU immer im Hinterkopf haben, wenn es an das Schreiben von Richtlinien geht. Wichtiger als umfangreiche Dokumente ist, dass die Anforderungen, die in den Richtlinien festgehalten werden, auch wirklich im Unternehmen umgesetzt und gelebt werden. Ein Aspekt, der in einem Audit einfach überprüft werden kann und genau deshalb auch oft geprüft wird. Ein Negativbeispiel sind z. B. überzogene Sicherheitsanforderungen an die eigene Softwareentwicklung, die in einer Richtlinie definiert sind, jedoch in der Praxis nicht eingehalten werden können. Es ist wichtig, eine Balance zu finden und solche Dokumente regelmäßig einem Review zu unterziehen und ggf. zu verbessern.

OBLIGATORISCHE RICHTLINIEN

- **Leitlinie zur Informationssicherheit**
- **Richtlinie zum Risikomanagement**
- **Richtlinie zum Umgang mit Sicherheitsvorfällen**
- **Richtlinie Lieferanten, Dienstleister und Fremdfirmen**
- **Richtlinie zur Klassifizierung und Umgang mit Informationen**
- **Richtlinie zum sicheren IT-Betrieb**
- **Richtlinie für Personal- und Berechtigungsmanagement**
- **Allgemeine Regeln zur Informationssicherheit für alle Beschäftigten**

Anwendungsbereich & Anwendbarkeitserklärung

Neben Richtlinien gibt es noch viele andere normspezifische Dokumente, die in einem Audit vorliegen müssen. Hierzu zählen als Erstes der **Anwendungsbereich** und die sogenannte **Anwendbarkeitserklärung (englisch: SoA – Statement of Applicability)**. Zusammen sind sie der erste Anhaltspunkt für den Auditor, um sich ein Bild über den Umfang und die Gegebenheiten des ISMS und des Unternehmens zu machen.

Die Anforderungen müssen im Unternehmen umgesetzt und gelebt werden.

Die Anwendbarkeitserklärung ist ein Dokument, das alle 114 Controls aus dem Anhang A der ISO 27001 abbildet. Im Rahmen der Anwendbarkeitserklärung ist zu prüfen und zu dokumentieren, welche Controls angewendet werden und deren Auswahl zu begründen. Alternativ können Controls auch begründet abgewählt werden, wenn die Vorgaben auf den Anwendungsbereich des ISMS nicht anwendbar sind. Beispielsweise können Organisationen das Control *„A.14.2.1 Richtlinie für sichere Entwicklung"* abwählen, wenn diese keine eigene Entwicklung von Software vornehmen. In der Praxis werden aber oft alle Controls angewendet und es ist nur vereinzelt sinnvoll bzw. möglich, Controls abzuwählen.

Control		Anwendbarkeit	Abwahlgrund	Auswahlgrund	Verknüpfte Dokumente
A.5	Informationssicherheitsleitlinien				
A.5.1	Vorgaben der Leitung für Informationssicherheit				
A.5.1.1	Informationssicherheitsrichtlinien	✓		Übernommene Best Practices	Leitlinie zur Informationssicherheit
A.5.1.2	Überprüfung der Informationssicherheitsrichtlinien	✓		Übernommene Best Practices	Richtlinie Organisation der Informationssicherheit
A.6	Organisation der Informationssicherheit				
A.6.1	Interne Organisation				
A.6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	✓		Übernommene Best Practices	Richtlinie Organisation der Informationssicherheit
A.6.1.2	Aufgabentrennung	✓		Übernommene Best Practices	Richtlinie Organisation der Informationssicherheit
A.6.1.3	Kontakt mit Behörden	✓		Übernommene Best Practices	Richtlinie zur Informationssicherheit
A.6.1.4	Kontakt mit speziellen Interessensgruppen	✓		Übernommene Best Practices	Richtlinie zur Informationssicherheit
A.6.1.5	Informationssicherheit im Projektmanagement	✓		Übernommene Best Practices	Richtlinie zur Informationssicherheit

Auszug aus einer Anwendbarkeitserklärung

Um zu verstehen, welche der 114 Controls Anwendung finden, ist es wichtig, sich vorab Gedanken über den Anwendungsbereich zu machen. Der Anwendungsbereich, oft auch Geltungsbereich oder Scope genannt, beschreibt in Textform, wo die Grenzen und die Anwendbarkeit des ISMS liegen. So ist es in größeren Organisationen üblich, lediglich einzelne Geschäftsbereiche zu zertifizieren, anstatt der kompletten Organisation. Aber auch in kleineren Firmen ist es möglich, einzelne Bereiche auszuschließen. Wenn z. B. der Standort im Ausland, über den lediglich Vertrieb stattfindet, nicht durch das ISMS abgedeckt ist, so muss das im Anwendungsbereich beschrieben werden.

BEISPIELE FÜR INFORMATIONSSICHERHEITSZIELE

- Sensibilisierung aller Beschäftigten in Bezug auf das Thema Informationssicherheit
- Gewährleistung der Zutrittssicherheit zum Datacenter
- Verfügbarkeit von 99,9 % der Datenanbindungen
- Frühzeitiges Erkennen von Sicherheitsvorfällen
- Stetige Steigerung des ISMS-Reifegrads
- Erfüllung der Kundenforderungen an die Vertraulichkeit seiner Daten
- Vollständige Dokumentation der Betriebsverfahren zur Sicherstellung der Verfügbarkeit
- Zuverlässige Unterstützung der Geschäftsprozesse durch die Informationstechnologien
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation
- Kontinuierliche Identifizierung, Bewertung und Behandlung von Risiken für die Informationssicherheit

Die Beschreibung des Geltungsbereichs ist daher auch für die eigenen Kunden und andere interessierte Parteien des Managementsystems interessant, da hier nachvollzogen werden kann, welche Bereiche und Themen durch das ISMS abgedeckt sind und welche nicht.

Neben den eigenen Kunden gibt es weitere interessierte Parteien (Stakeholder) die Erwartungen und Anforderungen an das ISMS haben. Dazu zählen z. B. die eigenen Mitarbeiter sowie die Geschäftsführung, der Gesetzgeber, Aufsichtsbehörden oder Dienstleister. All diese **interessierten Parteien und deren Anforderungen** sind in einem weiteren Dokument festzuhalten. Um die Übersicht zu behalten, bietet sich für dieses Dokument eine einfache Tabelle an. Wie für alle Dokumente gilt auch hier, die Informationen regelmäßig auf Aktualität zu prüfen und ggf. anzupassen.

Ein weiterer Aspekt, in den es sich lohnt Gedanken zu investieren, sind **Ziele der Informationssicherheit**. Die von der Unternehmensleitung festgelegte Unternehmensstrategie dient als Grundlage für die Ausgestaltung bzw. Festlegung der Ziele für die Informationssicherheit. Vor allem zu Beginn einer ISMS-Implementierung empfiehlt es sich, zunächst wenige aber für die jeweilige Organisation sinnvolle Informationssicherheitsziele zu definieren. Diese sollten im Verhältnis von Umsetzungsaufwand und Nutzen ausgewogen sein. Die festgelegten Informationssicherheitsziele sollten darüber hinaus möglichst messbar sein.

Neben den beschriebenen Dokumenten sind weitere Dokumente in einem Audit verpflichtend. Eine Übersicht über diese Dokumente liefert der folgende Infokasten.

OBLIGATORISCHE ISMS-DOKUMENTE

- **Anwendungsbereich** (auch Geltungsbereich oder Scope genannt)
- **Anwendbarkeitserklärung (engl.: SoA - Statement of Applicability)**
- **Interessierte Parteien und deren Anforderungen**
- **Ziele der Informationssicherheit**
- Planung der ISMS-Ressourcen
- ISMS-Rollen und -Verantwortlichkeiten
- Gesetzliche und regulatorische Anforderungen
- Interne und externe Kommunikation im ISMS
- Auditprogramm
- Managementbericht
- Risikobehandlungsplan

Erfolgsrezept

RISIKOMANAGEMENT

Die Anforderungen an ein Risikomanagement gemäß ISO 27001 sind im Managementrahmen der Norm beschrieben. Grundsätzlich wird gefordert, einen Prozess zu schaffen, in dessen Rahmen die Informationssicherheitsrisiken identifiziert und bewertet werden, um damit „die analysierten Risiken für die Risikobehandlung zu priorisieren".

Das Ganze muss natürlich auch bei Wiederholung zu „konsistenten, gültigen und vergleichbaren Ergebnissen" führen. Dafür ist es im ersten Schritt wichtig, das eigene Vorgehen zum Risikomanagement in einer Richtlinie festzulegen. Die Richtlinie sollte dabei mindestens die folgenden Punkte beinhalten.

Identifizieren – bewerten – behandeln

Über die Methode zur Risikoanalyse schweigt sich die ISO 27001 ansonsten größtenteils aus, was einem in der Umsetzung viele Freiheiten bietet – aber eben auch wenig Unterstützung. Hilfe kann hier die ergänzende ISO 27005 oder das Bundesamt für Sicherheit in der Informationstechnologie (BSI) mit seiner Methode im BSI-IT-Grundschutz bieten. Für KMU bietet sich eine Kombination dieser beiden Methoden an. So kann von der Flexibilität der ISO-Normen und den Vorlagen sowie den unterstützenden Informationen des BSI profitiert werden. Ein möglichst schlanker Prozess, der aber eben zu „konsistenten, gültigen und vergleichbaren Ergebnissen" führt könnte grob so aussehen:

INHALT DER RICHTLINIE ZUM RISIKOMANAGEMENT

1. Ermittlung der Risiken
2. Bewertung der Risiken
3. Risikobehandlung
4. Berichtswesen / Reporting

Risikomanagement Prozess

Risiken identifizieren

Überlegen Sie zuerst welche Informationen, Geschäftsprozesse oder IT-Systeme für Ihren Geschäftsbetrieb besonders kritisch sind. Fragen Sie dann ihre internen Experten und nutzen Sie zusätzlich Gefährdundungskataloge, wie den des BSI, um relevante Risiken zu identifizieren.

Risiken bewerten

Im zweiten Schritt geht es darum, die identifizierten Risiken zu bewerten. Schätzen Sie dafür die Schadenshöhe und die Eintrittswahrscheinlichkeit für jedes Risiko ab.

Der Risikowert ergibt sich aus der Eintrittswahrscheinlichkeit und der Schadenshöhe und kann in einer so genannten Risikomatrix ermittelt werden.

Risiken behandeln

Für die Risiken mit dem höchsten Wert sollte eine Behandlungsstrategie festgelegt und dokumentiert werden.

Eintrittswahrscheinlichkeit und Schadenshöhe

Wichtig ist, sich vorab Gedanken über ein Bewertungsschema der Risiken zu machen. Nur so kann man zu vergleichbaren Ergebnissen kommen und eine Priorisierung der identifizierten Risiken für die Risikobehandlung erreichen. Zur Bewertung gibt es in der ISO-27001-Norm tatsächlich auch grobe Vorgaben. Und zwar geht es darum, die Folgen bei Eintritt (Schadenshöhe) sowie die Eintrittswahrscheinlichkeit der identifizierten Risiken abzuschätzen. Weiter ins Detail geht die Norm an dieser Stelle nicht. Gängig und auch vom BSI vorgeschlagen ist ein vierstufiges Modell zur Bewertung der beiden Einflussgrößen Schadenshöhe und Eintrittswahrscheinlichkeit (siehe folgender Infokasten). Um eine Vergleichbarkeit der Risiken zu erreichen, können diese in einer Risikomatrix eingestuft werden. Der so ermittelte Risikowert gibt einen Hinweis darauf, welche Risiken bei der Behandlung bevorzugt werden sollten.

Ein risikobasiertes Vorgehen zur Behandlung bedeutet, sich zuerst den größten Risiken zu widmen. Eine sinnvolle Herangehensweise wäre, sich auf die „hohen" und „sehr hohen" Risiken zu konzentrieren und die übrigen Risiken als akzeptiert zu betrachten.

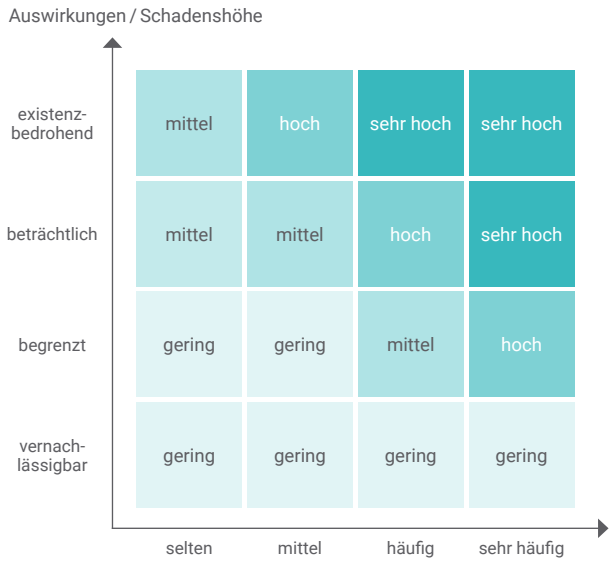
Klassische Möglichkeiten zum Umgang mit einem Risiko sind:

- **Risikovermeidung** (Einstellen bzw. Anpassen einer Tätigkeit)
- **Risikoreduktion** (Ermittlung von Sicherheitsmaßnahmen)
- **Risikotransfer** (z. B. Versicherung)
- **Risikoakzeptanz** (die Geschäftsführung trägt die Risiken)

Für jedes hohe und sehr hohe Risiko sollte eine der genannten Behandlungsoptionen in einem Risikobehandlungsplan festgelegt werden.

Die Ergebnisse des Risikomanagements sowie der Behandlungsplan sollten Bestandteil der jährlichen ISMS-Berichterstattung an die Geschäftsführung sein.

Risikomatrix



Eintrittshäufigkeit /Beschreibung

selten: Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.

mittel: Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.

häufig: Ereignis tritt einmal im Jahr bis einmal pro Monat ein.

sehr häufig: Ereignis tritt mehrmals im Monat ein.

Schadenshöhe/Schadensauswirkungen

vernachlässigbar: Die Schadensauswirkungen sind gering und können vernachlässigt werden.

begrenzt: Die Schadensauswirkungen sind begrenzt und überschaubar.

beträchtlich: Die Schadensauswirkungen können beträchtlich sein.

existenzbedrohend: Die Schadensauswirkungen können ein existenziellbedrohliches, katastrophales Ausmaß erreichen.

Quelle: BSI Standard 200-3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html (Zuletzt aufgerufen am 04.05.2020)

Erfolgsrezept

INTERNE AUDITIERUNG

Da interne Audits oft nicht zum Tagesgeschäft gehören, gilt es zunächst einmal, einige Begrifflichkeiten zu klären. Über allem steht das Auditprogramm. Für die einzelnen Audits ist die Erstellung eines Auditplans und eines Auditberichts sinnvoll.

Im **Auditprogramm** werden alle anstehenden Audits dokumentiert. Neben internen Audits sollten hier auch Lieferantenaudits und externe Audits (z. B. Zertifizierungsaudits oder Kundenaudits) aufgelistet werden. Lassen Sie sich das Auditprogramm für die nötige Rückendeckung von der Unternehmensleitung offiziell freigeben.

Wenn das Auditprogramm dann steht, geht es um die Vorbereitung des ersten internen Audits. Die Vorbereitung findet in dem sogenannten **Auditplan** statt. Dieser dient einerseits der Planung (Nennung des auditierten Bereichs/Objekts, des Datums, der Zeit und Räumlichkeiten) und andererseits der Koordination und Information aller Auditteilnehmer.

Im internen Audit selbst geht es dann im Wesentlichen um die Identifizierung von Verbesserungsmöglichkeiten. Sorgen Sie von Anfang an für eine positive Auditatmosphäre, um relevante Verbesserungsmöglichkeiten zu identifizieren. Qualität geht vor Quantität. Wenn Sie Ihre eigenen Kollegen auditieren, ist Fingerspitzengefühl gefragt. Auch wenn es in erster Linie um Schwachstellen bzw. Verbesserungsmöglichkeiten geht, sollten auch positive Erkenntnisse aus dem Audit unbedingt in den **Auditbericht** mit aufgenommen werden.

Der Umfang eines Audits hängt stark von dem zu auditierenden Bereich oder Objekt ab. Nehmen Sie sich aber mindestens einen halben Tag Zeit, um Dokumente zu sichten, Interviews zu führen und IT-Systeme in Augenschein zu nehmen. Zwischen den Sessions ist es sinnvoll, ein wenig Zeit einzuplanen, um Ihre Gedanken zu sortieren und Notizen für den Auditbericht niederzuschreiben.

Verstehen Sie interne Audits als Werkzeug, um für eine Verbesserung der Informationssicherheit im Unternehmen zu sorgen. Nutzen Sie Auditberichte, um den Feststellungen den nötigen Nachdruck zu verleihen. Fangen Sie einfach an. Schon bald werden Sie sehen, dass die internen Audits von Mal zu Mal routinierter ablaufen.

Checkliste für die Durchführung interner Audits

Tätigkeit	Zeitpunkt
Erstellen des Auditplans	4 Wochen vor Audit
Abstimmung mit dem zu auditierenden Bereich • Terminfindung • Benennung der Ansprechpartner	2–4 Wochen vor Audit
Bereitstellung des finalisierten Auditplans	2 Wochen vor Audit
Durchführung des Audits	Audit
Abstimmung von Maßnahmen und Terminen mit dem auditierten Bereich	2 Wochen nach Audit
Bereitstellung des Auditberichts	3 Wochen nach Audit
Überführung der Maßnahmen ins interne Ticketsystem	4 Wochen nach Audit

Erfolgsrezept

INFORMATIONSSICHERHEITS-VORFÄLLE

Eine 100-prozentige Sicherheit gibt es nicht. Ein Sicherheitsvorfall kann zu jedem Zeitpunkt dazu führen, dass beispielsweise Informationen nicht im erforderlichen Maße zur Verfügung stehen oder auch in falsche Hände geraten.

Zwei Beispiele: Der Webshop muss aufgrund eines Cyberangriffs vorübergehend abgeschaltet werden, oder; Eine Mail mit wichtigen Unterlagen wurde an einen falschen Empfänger geschickt.

Für Informationssicherheitsvorfälle schreibt die Norm daher einige Dinge vor, allen voran eine systematische Herangehensweise bei deren Meldung und Erfassung. Dafür sollte im Unternehmen ein Prozess verankert werden, der klare Vorgaben macht, wann ein Sicherheitsvorfall an welche Stelle zu melden ist. Entscheidend ist, dass alle Mitarbeiter ihre Verantwortung zur Meldung kennen, denn nur so kann umgehend reagiert werden.

Entscheidend ist, dass alle Mitarbeiter ihre Verantwortung zur Meldung kennen, denn nur so kann umgehend reagiert werden.

Hier ergibt es keinen Sinn, das Rad neu zu erfinden. Wenn es bereits bestehende Meldeprozesse im Unternehmen gibt, z. B. einen zentralen Helpdesk in der IT, sollten diese Prozesse und Stellen bei der Etablierung des Prozesses berücksichtigt werden. Der Helpdesk kann dann z. B. gemeldete Sicherheitsvorfälle priorisieren und zielgerichtet bestimmte Stellen wie den Informationssicherheitsbeauftragen oder auch die Geschäftsführung mit hinzuziehen.

Mehr als alles andere gilt hier: Der Prozess und die Meldewege bringen Ihnen nichts, wenn die Kollegen im entscheidenden Moment nicht darüber Bescheid wissen. Schulen Sie Ihre Mitarbeiter also regelmäßig und nutzen Sie auch bestehende Schulungen und Trainings, um an die Meldewege zu erinnern.

Erkenntnisse gewinnen

Der Prozess ist etabliert. Und nun? Auch wenn die bedrohlichen Vorfälle hoffentlich ausbleiben, sollte der Prozess nicht zum Papiertiger verkommen. Denn eine Anforderung der Norm bleibt noch: Gewinnen Sie Erkenntnisse aus vergangenen Vorfällen. Schauen Sie sich retrospektiv die Sicherheitsvorfälle an und ziehen Sie in diesem Rahmen Schlüsse, was Sie zukünftig verbessern können. Sicherheitsvorfälle passieren. Das Ziel sollte aber sein, die Fehler nicht zu wiederholen.

Erfolgsrezept

AWARENESS

Spätestens seit Angriffen wie z. B. der Chef-Masche (auch CEO Fraud genannt) ist bei allen angekommen, dass die Sensibilisierung von Mitarbeitern bezüglich der Informationssicherheit einer der wichtigsten Verteidigungsmechanismen ist.

Entsprechend wird diese selbstverständlich auch durch die ISO 27001 gefordert. Die Norm lässt dabei jedoch viele Freiheiten zur Ausgestaltung. Als Mindestmaß hat sich etabliert, dass die Mitarbeiter mindestens einmal im Jahr eine Schulung oder z. B. ein Onlinetraining zur Informationssicherheit durchlaufen sollten und auch neue Mitarbeiter beim Eintritt eine entsprechende Schulung bekommen.

Zahlreiche Materialien zu Best Practices und Tipps zur Informationssicherheit finden sich mit Netz, auch öffentlich zugängliche, z. B. vom BSI. Es empfiehlt sich darüber hinaus unbedingt, die Schulungen auch dafür zu nutzen, um den Mitarbeitern Dokumente wie die Leitlinie und wichtige Inhalte der relevanten Richtlinien vorzustellen. Nutzen Sie die Schulungen außerdem dazu, um Prozesse, die für alle Mitarbeiter wichtig sind, bekannt zu machen. Beispielsweise für die Bekanntmachung von Meldewegen bezüglich Informationssicherheitsvorfällen.

Zuletzt sollten Sie nicht vergessen, Teilnahmelisten unterschreiben zu lassen oder andere Nachweise zu pflegen, damit Sie dem Auditor auch nachweisen können, dass Schulungen stattgefunden haben.

Beispiel eines Posters zur Bekanntmachung von Meldewegen bei Sicherheitsvorfällen.

Erfolgsrezept

ISMS SELFASSESSMENT

Insgesamt 114 Maßnahmen umfasst der Anhang A der ISO 27001. Diese sind grundsätzlich alle zu erfüllen, es sei denn Sie können im Rahmen der Anwendbarkeitserklärung argumentieren, warum einzelne Anforderungen auf Ihr Unternehmen nicht zutreffen.

Damit Sie sicherstellen, dass Sie alle relevanten Anforderungen der Norm auch sicher erfüllen, empfiehlt sich ein sogenanntes Selfassessment. Dieses hat sich längst als Best Practice etabliert, auch wenn es nicht unmittelbar von der Norm vorgeschrieben ist.

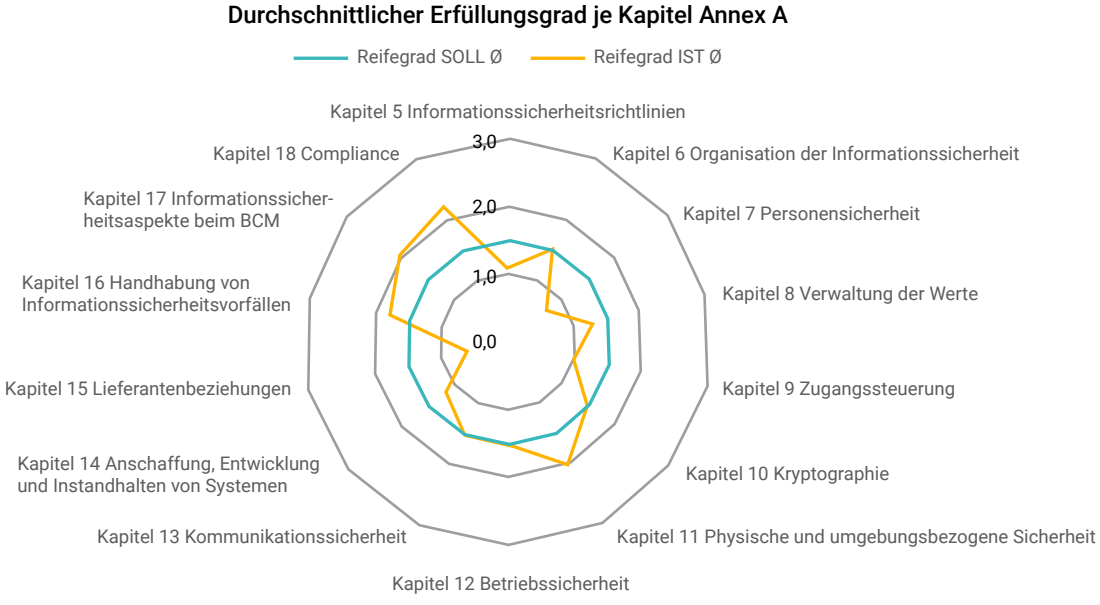
Im Rahmen eines Selfassessments bewerten Sie Ihren aktuellen Stand bezüglich der einzelnen Maßnahmen. Ermitteln Sie dazu einen Erfüllungsgrad, z. B. auf einer Skala von 0 bis 10, in Prozent oder nach einem etablierten Reifegradmodell. Dokumentieren Sie am besten zeitgleich Nachweise, die die Erfüllung einer Maßnahme dokumentiert und halten Sie notwendige To-dos fest. Die Nachweise können im späteren Zertifizierungsaudit als Gedankenstütze sehr hilfreich sein, damit Sie dem Auditor die entsprechende Dokumentation vorweisen können, wenn er danach fragt.

Integrieren Sie außerdem das Selfassessment als „internes Audit" in das Auditprogramm. Methodisch unterscheidet sich das Selfassessment zwar vom klassischen Audit, kann aber ebenfalls als Überprüfung angeführt werden und macht sich gut im Zertifizierungsaudit.

Ein weiterer Vorteil von Selfassessments ist, dass Sie damit auf einfachem Wege eine leicht messbare und wirksame Kennzahl etablieren können. Sie können z. B. je nach Kapitel des Anhangs A einen Reifegrad oder Umsetzungsgrad anhand des Selfassements berechnen und entsprechend der folgenden Grafik darstellen. Reporten Sie diese Kennzahl auch an die Geschäftsführung und steuern Sie mit ihrer Hilfe Ihr ISO-27001-Implementierungsprojekt sowie die weiteren Verbesserungen über die kommenden Zertifizierungszyklen.

Auswertung eines Selfassessment

Der Erfüllungsgrad der einzelnen Maßnahmen wurde von 0 bis 3 gemessen und wird hier auf Kapitel-Ebene aggregiert dargestellt. Die grüne Linie stellt den SOLL-Reifegrad dar, die orange den IST-Reifegrad.



Erfolgsrezept

REPORTING

In einem gesunden Managementsystem trägt die Geschäftsführung die Verantwortung und trifft dafür wegweisende Entscheidungen, legt die Strategie fest, initiiert wesentliche Anpassungen und passt Ziele des ISMS an.

Um der Geschäftsführung diese Aufgaben zu ermöglichen, muss sie regelmäßig eine Berichterstattung über den Status des ISMS in Form einer sogenannten „Managementbewertung" erhalten.
Eine solche Berichterstattung an die Geschäftsführung sollte quartalsweise oder halbjährlich, mindestens aber einmal im Jahr erfolgen. Stimmen Sie die Frequenz mit der Geschäftsführung ab, aber nehmen Sie sich erst einmal nicht zu viel vor.

Bezüglich der Ausgestaltung gibt die Norm eine Reihe von Inhalten der Managementbewertung unmittelbar vor. Das umfasst z. B. den Status von Maßnahmen, Ergebnisse aus internen Audits sowie dem Risikomanagement und einiges mehr (siehe ISO 27001, Kapitel 9.3).

Die Inhalte für die Managementbewertung sind theoretisch schnell zusammengetragen. Jedoch müssen sie vollständig und in einer Form vorliegen, die Ihnen eine Berichterstattung ermöglicht. Tools können dabei helfen, Ergebnisse und Dokumentation zentral vorzuhalten und nach Möglichkeit automatisiert in einen Bericht zusammenzuziehen.

In der Praxis zeigt sich, dass die Inhalte oftmals bereits vorhanden sind, jedoch oft genug unvollständig oder nicht in einer Form, in der sie auch reported werden können. Daher sollte bei den unterjährigen Aktivitäten im ISMS bereits berücksichtigt werden, dass gewisse Themen am Ende auch mit geringem Aufwand in die Managementbewertung überführt werden können. Ist die Dokumentation in einem Meer aus Word-Dokumenten, Excel-Tabellen und E-Mails verteilt, führt dies zu hohen Arbeitsaufwänden oder im Ergebnis zu einem unvollständigen, inkonsistenten oder fehlerhaften Bericht.

Behalten Sie bei der Durchführung der Prozesse also an den entscheidenden Stellen bereits im Auge, dass die Ergebnisse zentral und vollständig vorliegen. Es empfiehlt sich, dies insbesondere an folgenden Stellen zu tun:

- Beim Messen von Kennzahlen und Zielen der Informationssicherheit
- Bei der Steuerung von Maßnahmen
- Bei der Dokumentation von Sicherheitsvorfällen
- Im Risikomanagement, zu den jeweiligen Risiken sowie deren Behandlung
- Bei der Dokumentation der Ergebnisse von internen Audits
- Bei der Auswertung des Selfassessments

Es gibt darüber hinaus zwei Dinge, die unbedingt in die Managementbewertung gehören, jedoch nicht in bereits bestehenden Prozessen generiert werden:

1. Die Rückmeldung von interessierten Parteien, beispielsweise wenn sich ein Kunde, eine Behörde o. ä. in Bezug auf Themen der Informationssicherheit bei Ihnen meldet.
2. Die Themen, die einen signifikanten Einfluss auf das ISMS haben. Das können beispielsweise Neuprodukte oder wesentliche Änderungen an Produkten, neue Kerngeschäftsprozesse, neue Standorte oder eine neu eingeführte Sicherheitslösung wie ein SIEM sein.

Machen Sie sich also zu diesen beiden Themen bereits im Berichtszeitraum Notizen, steht einer erfolgreichen Managementbewertung nichts mehr im Wege.
Ist alles zur Managementbewertung zusammengetragen, wird diese gemeinsam mit der Geschäftsführung besprochen. Machen Sie sich hierbei Notizen, denn auch die Rückmeldung der Geschäftsführung, z. B. zu neuen oder angepassten Zielen, neuen Maßnahmen usw., gehören mit in die Managementbewertung. Ergänzen Sie diese im Nachgang und lassen Sie die Managementbewertung von der Geschäftsführung unterschreiben.

Erfolgsrezept

KONTINUIERLICHER VERBESSERUNGSPROZESS (KVP)

Der Aufbau eines Managementsystems für Informationssicherheit ist keine einmalige Aufgabe. Das ISMS muss kontinuierlich auf Eignung, Angemessenheit und Wirksamkeit geprüft werden.

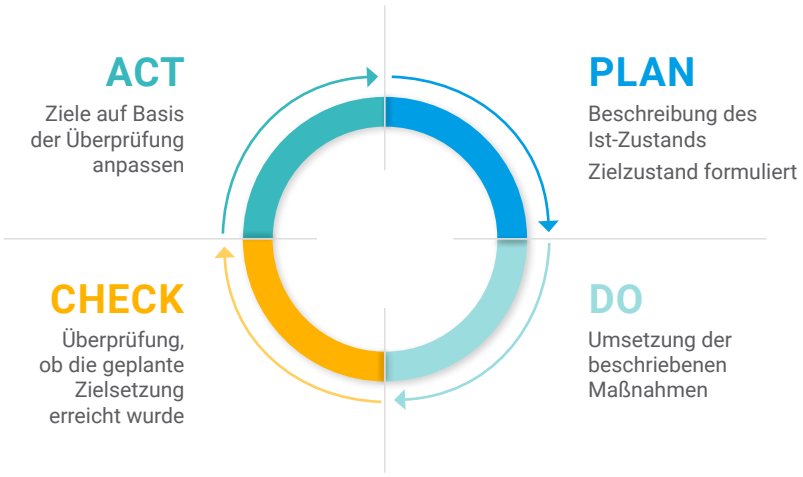
Für eine erfolgreiche Zertifizierung muss dem Auditor genau das nachgewiesen werden. Identifiziere ich Schwachstellen in meiner Informationssicherheit? Unterliegt mein ISMS und damit die Informationssicherheit einer ständigen Verbesserung? Genau diese Verbesserungen werden erreicht, indem die oben genannten Praktiken angewendet werden. Verbesserungspotential wird z. B. in der Risikoanalyse, im ISMS Selfassessment oder in einem „Lessons Learned" zu Sicherheitsvorfällen identifiziert. Entscheidend ist, dass diese Verbesserungspotenziale in Maßnahmen überführt und nachgehalten werden.

Nutzen Sie dafür nach Möglichkeit bestehende Ticketsysteme oder Aufgabenplanungstools, um Verantwortlichkeiten und Zieldaten zu dokumentieren. Für das Reporting empfiehlt es sich, die Maßnahmen aus der Informationssicherheit mit Flags oder Tags auswertbar und selektierbar zu machen. Als Alternative zu einem Ticketsystem bieten auch die gängigen ISMS Lösungen am Markt, um die Funktion und Maßnahmen zu erfassen und zu steuern.

Die ISO 27001 fordert zwar kein konkretes Mindestlevel in Bezug auf Informationssicherheit, dafür aber ganz deutlich, dass das Managementsystem und damit die Sicherheit im Unternehmen einem kontinuierlichen Verbesserungsprozess unterliegen muss.

Ein konkretes Modell zur Umsetzung der kontinuierlichen Verbesserung wird nicht vorgeschrieben. Am weitesten verbreitet hat sich jedoch der PDCA-Zyklus (auch Deming Cycle genannt). Demnach müssen die geplanten (plan) und umgesetzten (do) Aktivitäten im Managementsystem nach dem Plan-Do-Check-Act-Kreislauf ständig auf ihre Wirksamkeit hin geprüft (check) und gegebenenfalls angepasst (act) werden.

PDCA-Zyklus



Fazit

EIN ZEICHEN FÜR DIE SICHERHEIT

Ein zertifiziertes ISMS nach ISO 27001 wird zunehmend zum Wettbewerbsvorteil. Sie setzen damit ein starkes Zeichen für die Sicherheit von Informationen, Daten und Systemen. Als zukunftsfähiges Unternehmen müssen Sie sich schließlich auf eine belastbare IT verlassen können. Und nicht nur Sie, sondern auch Ihre Kunden.

Nutzen Sie die Chance und sehen Sie das ISMS als ein ganzheitliches Werkzeug, um die Informationssicherheit im Unternehmen Stück für Stück zu verbessern und durch die geschaffenen Prozesse auf Bedrohungen und technische Entwicklungen schnell und angemessen reagieren zu können.

Schrecken Sie nicht vor den zahlreichen Anforderungen der Norm zurück. Oft existieren im Unternehmen bereits viele Sicherheitsmaßnahmen, die für das Audit lediglich noch beschrieben werden müssen. Nutzen Sie auch bereits existierende Prozesse, um z. B. Maßnahmen zu steuern und Vorfälle zu melden. Das Rad muss nicht neu erfunden werden.

Insbesondere bei der Erstzertifizierung geht es darum, die notwendige Dokumentation sowie die Prozesse nachzuweisen. Die Sicherheitsmaßnahmen aus dem Anhang A der Norm müssen nicht lückenlos umgesetzt sein. Jedoch müssen notwendige Maßnahmen identifiziert und ein Weg aufgezeigt werden, wie und wann diese umgesetzt werden.

ISMS-Lösungen für KMUs

Bei der Einführung eines ISMS kann ein entsprechendes ISMS-Tool helfen um z. B. Risiken zu steuern, die Dokumentation zu erstellen und dem Unternehmen einen Leitfaden zur Etablierung des Managementsystems zu geben. Achten Sie bei der Beschaffung darauf, dass die Lösung auch auf KMU ausgelegt ist. Oft genug entpuppen sich ISMS-Lösungen in der Nutzung als zu komplex für KMUs, in denen die Informationssicherheit eine One-Man-Show ist.

Außerdem reduziert es den Arbeitsaufwand des Informationssicherheitsbeauftragten enorm, wenn das ISMS-Tool bereits Vorlagen für Richtlinien und andere normspezifische Dokumente mitbringt. Im Idealfall müssen solche Dokumente zur Verwendung nur noch an den eigenen Unternehmenskontext angepasst werden. Dem Verantwortlichen für die Informationssicherheit bleibt so mehr Zeit für die Implementierung der Vorgaben im Unternehmen.

Schrecken Sie nicht vor den zahlreichen Anforderungen der Norm zurück. Nutzen Sie auch bereits existierende Prozesse: Das Rad muss nicht erfunden werden.

Um die Akzeptanz der Richtlinien bei den Mitarbeitern zu erhöhen, ist es sinnvoll, betroffene Mitarbeiter frühzeitig mit in den Schaffensprozess einzubinden. Lassen Sie z. B. technische Richtlinien vor der Freigabe von den eigenen Administratoren gegenlesen und kommentieren – und nehmen Sie das Feedback ernst. Nur so kann es gelingen, dass das ISMS im Unternehmen auch wirklich gelebt wird.

Über Byght

WIR GEHEN NEUE WEGE – IMMER SMART, IMMER EINFACH

JOHANNES MATTES

Lange Zeit als Network- and Security Engineer bei einem Hamburger Internet Service Provider unterwegs gewesen. Mit reichlich Erfahrung als Informationssicherheitsbeauftragter, CISO und Security-Architect, immer mit Freude an anderen Arbeitsmethoden.

Qualifikationen

- Information Security Officer - ISO (TÜV)
- ISMS Auditor/Lead Auditor ISO/IEC 27001
- CISSP

E-Mail: johannes@byght.de | Telefon: 040 - 66892413

LUCA GRAF

Als Consultant in kleinen Unternehmen und internationalen Konzernen diverser Branchen mit Fokus auf ganzheitlicher Informationssicherheit tätig gewesen. Erfahrung als Spezialist für Informationssicherheit in der Finanzbranche, mit viel Leidenschaft für organisatorische und prozessuale Themen sowie Governance.

Qualifikationen

- M.Sc. Global Management & Governance
- ISO (TÜV) & ISMS Auditor/Lead Auditor ISO/IEC 27001

E-Mail: luca@byght.de | Telefon: 040 - 66892613

BYGHT

Byght GmbH
Christians-Platz 8, 22844 Norderstedt

www.byght.de

Autoren: Johannes Mattes, Alexander Luca Graf