Chain Horizon GmbH, Kolonnenstraße 8, 10827 Berlin
info@chain-horizon.com | https://chain-horizon.com

Minimale organisatorische Prozesse zur Registrierung eines Unternehmens im BSI-Portal mit dem ELSTER-Organisationszertifikat

Zweck und Zielsetzung

Dieses Dokument dient als Orientierungshilfe für Unternehmen zur Beschreibung minimal notwendiger organisatorischer Prozesse im Zusammenhang mit der Registrierung einer Organisation im BSI-Portal unter Nutzung des ELSTER-Organisationszertifikats. Ziel ist es, Zuständigkeiten, Verantwortlichkeiten und Unterstützungsleistungen transparent und nachvollziehbar zu strukturieren, ohne organisationsspezifische Detailregelungen vorwegzunehmen.

Im Fokus stehen bewusst minimale, aber funktionsfähige Prozesse, die eine sichere, nachvollziehbare und organisatorisch saubere Nutzung des ELSTER-Organisationszertifikats ermöglichen. Das Dokument erhebt keinen Anspruch auf Vollständigkeit oder Allgemeingültigkeit, da sich Unternehmen in Größe, Organisationsform, Verantwortungszuschnitten und Governance-Strukturen unterscheiden können.

Beteiligte Organisationseinheiten

Die beschriebenen Prozesse setzen in der Regel ein Zusammenwirken mehrerer Organisationseinheiten voraus:

- **Finance / Tax**: Fachlich verantwortliche Einheit für die Registrierung der Organisation, die Nutzung des ELSTER-Organisationszertifikats sowie die inhaltliche Durchführung von Meldungen.

- **IT**: Technische Betriebs- und Umsetzungseinheit, insbesondere für Verwahrung des Zertifikats, technische Zugriffe, Berechtigungen und Systemunterstützung.

- **Informationssicherheit / Security (sofern vorhanden)**: Governance-orientierte Unterstützungsfunktion zur Definition von Richtlinien, Mindestanforderungen und Vorgaben zum Umgang mit Informationen, Identitäten und Zugriffsrechten.

In Organisationen ohne dedizierte Informationssicherheitsfunktion können Governance-Aufgaben durch eine andere geeignete Stelle wahrgenommen werden.

Übergeordnete Organisationsverantwortung

Die in diesem Dokument dargestellten Prozesse und RASCI-Zuordnungen beziehen sich auf operative und fachliche Zuständigkeiten innerhalb der Organisation. Die

fachliche Gesamtverantwortung (Accountability) für die Durchführung der beschriebenen Tätigkeiten ist innerhalb der Organisation delegiert.

Unabhängig davon verbleibt die übergeordnete organisatorische und rechtliche Gesamtverantwortung für die ordnungsgemäße Ausgestaltung von Prozessen, Zuständigkeiten und organisatorischen Rahmenbedingungen bei der Geschäftsführung. Die dargestellten Zuordnungen ersetzen diese Gesamtverantwortung nicht, sondern dienen ihrer organisatorischen Umsetzung.

Methodik zur Zuordnung von Zuständigkeiten (RASCI)

Die Zuordnung von Zuständigkeiten innerhalb der beschriebenen Prozesse erfolgt anhand des RASCI-Modells:

- **R –** Responsible: Führt die Tätigkeit operativ aus.
- **A –** Accountable: Trägt die fachliche Verantwortung für Inhalt und Ergebnis.
- **S –** Supportive: Unterstützt operativ oder im Sinne eines Governance Supports.
- **C –** Consulted: Wird fachlich beratend einbezogen.
- **I –** Informed: Wird informiert.

Die Rolle Supportive (S) umfasst sowohl operative Unterstützung (z. B. durch die IT) als auch Governance-bezogene Unterstützungsleistungen. Governance-Funktionen übernehmen weder operative Durchführung noch fachliche oder rechtliche Gesamtverantwortung.

Pro Aktivität ist jeweils nur eine Accountable-Rolle vorgesehen.

Management-Erläuterung zur Rolle der Informationssicherheitsfunktion:

Informationssicherheits- oder Security-Funktionen nehmen innerhalb der Organisation eine zentrale Rolle bei der Erkennung, Bewertung und Einordnung von IT- und sicherheitsrelevanten Vorfällen ein. Sie stellen fachliche Expertise bereit, bewerten Risiken und unterstützen andere Organisationseinheiten durch qualifizierte Zuarbeit. Die formelle Abgabe von Meldungen mit organisatorischer oder rechtlicher Wirkung erfolgt jedoch durch die fachlich verantwortliche Stelle im Rahmen der durch die Geschäftsführung delegierten Zuständigkeit. Diese Trennung stellt sicher, dass sicherheitsfachliche Bewertung, organisatorische Verantwortung und formelle Erklärung klar voneinander abgegrenzt bleiben und dem Prinzip einer sauberen Governance entsprechen.

Die dargestellte Rollenverteilung stellt eine beispielhafte, praxisnahe Ausgestaltung dar. Abhängig von Größe, Organisationsform und Governance-Struktur eines Unternehmens können einzelne Aufgaben abweichend zugeschnitten oder

zusammengefasst sein. Die grundlegende Trennung von fachlicher Verantwortung, technischer Unterstützung und Governance-Unterstützung bleibt hiervon unberührt.

Prozesse und RASCI-Zuordnungen

1. Eigentümerschaft & Governance
Ziel: Klare Festlegung fachlicher Zuständigkeiten und organisatorischer Verantwortlichkeiten.

Aktivität	*Finance / Tax*	*IT*	*InfoSec / Security*
Governance und Zuständigkeiten festlegen	**A**	**S**	**S**

Begründung der Rollenverteilung:

Die Festlegung von Governance-Strukturen und Zuständigkeiten ist eine fachlich-organisatorische Aufgabe mit unternehmensweiter Wirkung. Die fachliche Verantwortung liegt daher bei der zuständigen Fachfunktion (Finance / Tax), die im Auftrag der Geschäftsführung handelt.

Die dargestellte Rollenverteilung trägt dem Prinzip der Separation of Duties Rechnung, indem fachliche Verantwortung, technische Bereitstellung der Informationstechnologie sowie Governance-bezogene Leitplanken bewusst auf unterschiedliche Organisationseinheiten verteilt werden.

Die IT unterstützt in diesem Zusammenhang, indem sie die informationstechnischen Rahmenbedingungen bereitstellt, die für den Betrieb des BSI-Portals, die Nutzung des ELSTER-Organisationszertifikats sowie für Zugriffs- und Berechtigungskonzepte erforderlich sind.

Sofern eine Informationssicherheits- oder Security-Funktion vorhanden ist, wirkt diese unterstützend im Sinne eines Governance Supports, insbesondere durch die Definition und Bereitstellung von Richtlinien, Mindestanforderungen und Vorgaben zum Umgang mit Informationen, Identitäten und Zugriffsrechten. Sie übernimmt dabei keine fachliche oder operative Verantwortung, sondern schafft organisatorische Leitplanken für die Ausgestaltung der Prozesse.

2. Verwahrung des ELSTER-Organisationszertifikats
Ziel: Sichere, zentrale Verwahrung und kontrollierte technische Nutzung.

Aktivität	*Finance / Tax*	*IT*	*InfoSec / Security*
Zertifikat verwahren	**I**	**R / A**	**S**
Technische Zugriffssicherung	**I**	**R / A**	**S**

Begründung der Rollenverteilung:

Die Verwahrung des ELSTER-Organisationszertifikats ist eine primär technische Aufgabe, da sie sichere Speicherorte, Zugriffsbeschränkungen und technische Schutzmaßnahmen erfordert. Die Verantwortung und Durchführung liegen daher bei der IT. Finance / Tax wird informiert, da das Zertifikat fachlich genutzt wird, jedoch nicht technisch betrieben werden sollte. Informationssicherheitsfunktionen unterstützen durch Governance-Vorgaben und Mindestanforderungen zur sicheren Verwahrung.

3. Erstregistrierung und Initial-Login im BSI-Portal
Ziel: Kontrollierte Erstregistrierung der Organisation.

Aktivität	Finance / Tax	IT	InfoSec / Security
Registrierung fachlich vorbereiten	**R / A**	**S**	**S**
Initial-Login und Abschluss der Registrierung	**R / A**	**S**	**S**

Begründung der Rollenverteilung:

Der Bedarf zur Registrierung im BSI-Portal ergibt sich regelmäßig aus regulatorischen oder sicherheitsbezogenen Anforderungen und wird häufig durch Informationssicherheits- oder Security-Funktionen identifiziert und fachlich eingeordnet. Die Entscheidung zur Durchführung sowie die Delegation der Aufgabe erfolgen durch die Geschäftsführung.

Die operative Vorbereitung und Durchführung der Registrierung liegen bei der fachlich verantwortlichen Stelle (Finance / Tax oder äquivalente beauftragte Einheit), da die Registrierung unter Nutzung des ELSTER-Organisationszertifikats erfolgt und rechtlich-organisatorische Wirkung entfaltet.

IT- und Informationssicherheitsfunktionen unterstützen diesen Prozess im Sinne des RASCI-Modells. Die IT unterstützt bei technischen Fragestellungen sowie bei Zugriffs- und Systemthemen. Informationssicherheits- oder Security-Funktionen unterstützen praktisch und fachlich, insbesondere im Hinblick auf sicherheitsrelevante Aspekte der Registrierung, die Nutzung von Identitäten und Berechtigungen sowie die Einhaltung organisatorischer Sicherheitsvorgaben. Sie übernehmen dabei keine fachliche Verantwortung für die Registrierung, leisten jedoch aktiven Support im Sinne eines Governance Supports.

4. Rollenvergabe und Delegation
Ziel: Anlage und Beschränkung operativer Benutzer und Rollen.

Aktivität	Finance / Tax	IT	InfoSec / Security
Rollen fachlich definieren	**R / A**	**S**	**C**
Technische Umsetzung	**A**	**R**	**S**

Begründung der Rollenverteilung:

Die Definition zulässiger Rollen und Berechtigungen ist eine fachliche Entscheidung, da sie den Umfang der Nutzung und die inhaltlichen Handlungsmöglichkeiten bestimmt. Diese Verantwortung liegt bei Finance / Tax, die im Auftrag der Geschäftsführung handelt. Die technische Umsetzung der Rollen erfolgt durch die IT, da sie die erforderlichen System- und Berechtigungsmechanismen verwaltet.

Die dargestellte Rollenverteilung folgt dem Prinzip der Separation of Duties, indem fachliche Rollendefinition und technische Umsetzung bewusst getrennt werden. Dadurch wird vermieden, dass eine Organisationseinheit sowohl über die inhaltliche Ausgestaltung als auch über die technische Umsetzung von Berechtigungen entscheidet. Informationssicherheits- oder Security-Funktionen unterstützen beratend im Sinne eines Governance Supports, insbesondere im Hinblick auf Prinzipien wie Least Privilege und angemessene Aufgabentrennung.

5. Durchführung von Meldungen
Ziel: Fachlich korrekte Erstellung und Abgabe von Meldungen.

Aktivität	*Finance / Tax*	*IT*	*InfoSec / Security*
Fachliche Meldung durchführen	**R / A**	**I**	**S**
Technische Unterstützung	**A**	**S**	**S**

Begründung der Rollenverteilung:

Die Erstellung und Abgabe von Meldungen im BSI-Portal ist eine fachliche Tätigkeit mit rechtlich-organisatorischer Wirkung. Die fachliche Verantwortung sowie die operative Durchführung liegen daher bei der fachlich zuständigen Einheit (Finance / Tax oder äquivalente beauftragte Stelle) im Rahmen der durch die Geschäftsführung delegierten Zuständigkeit.

IT- und Informationssicherheitsfunktionen sind in diesen Prozess ausdrücklich einbezogen, soweit technische, sicherheitsrelevante oder organisatorische Sachverhalte betroffen sind. Sie haben eine Unterstützungspflicht im Sinne des RASCI-Modells.

Die IT unterstützt insbesondere bei technischen Fragestellungen, Systemstörungen und Zugriffsproblemen. Informationssicherheits- oder Security-Funktionen unterstützen fachlich bei der Erstellung der Meldung, insbesondere durch die Einordnung sicherheitsrelevanter Sachverhalte, die Bewertung von Vorfällen sowie durch inhaltliche Zuarbeit. Sie übernehmen dabei keine fachliche Verantwortung für den Meldeinhalt, stellen jedoch den erforderlichen fachlichen und organisatorischen Support sicher.

6. Notfall- und Eskalationsprozess
Ziel: Sicherstellung der Handlungsfähigkeit bei Frist- oder Sicherheitsvorfällen.

Aktivität	*Finance / Tax*	*IT*	*InfoSec / Security*
Fachliche Notfallmeldung	**R / A**	**S**	**S**
Technische Wiederherstellung	**I**	**R / A**	**S**

Begründung der Rollenverteilung:

Notfall- und Eskalationssituationen betreffen regelmäßig sowohl fachliche, technische als auch sicherheitsrelevante Aspekte. Die fachliche Notfallmeldung sowie die Eskalation gegenüber externen Stellen liegen bei der fachlich zuständigen Einheit (Finance / Tax oder äquivalente beauftragte Stelle), da diese Meldungen rechtlich-organisatorische Wirkung entfalten und im Rahmen der durch die Geschäftsführung delegierten Zuständigkeit erfolgen.

Die IT ist für technische Wiederherstellungs- und Stabilisierungsmaßnahmen verantwortlich, insbesondere bei Systemstörungen, Zugriffsproblemen oder Verfügbarkeitsvorfällen.

Informationssicherheits- oder Security-Funktionen unterstützen den Notfall- und Eskalationsprozess aktiv im Sinne des RASCI-Modells. Sie leisten fachlichen Support bei der Einordnung von Sicherheitsvorfällen, der Bewertung von Auswirkungen und Risiken sowie bei der Abstimmung geeigneter Maßnahmen. Sie übernehmen dabei keine fachliche oder rechtliche Verantwortung für die Notfallmeldung, stellen jedoch den erforderlichen sicherheitsfachlichen und organisatorischen Support sicher.

7. Jährliche Überprüfung (Minimal-Compliance)
Ziel: Regelmäßige Überprüfung der Nutzung und Rollenverteilung.

Aktivität	Finance / Tax	IT	InfoSec / Security
Review der Nutzung und Rollen	**A**	**R**	**S**
Ergebnis dokumentieren	**R / A**	**S**	**C**

Begründung der Rollenverteilung:

Die regelmäßige Überprüfung der Nutzung des BSI-Portals und der vergebenen Rollen dient der organisatorischen Selbstkontrolle und der Sicherstellung fortbestehender Angemessenheit. Die fachliche Verantwortung liegt bei Finance / Tax, während die IT die hierfür notwendigen technischen Auswertungen und Informationen bereitstellt. Informationssicherheitsfunktionen unterstützen durch fachliche Einordnung und Empfehlungen.

Unterstützung bei der Umsetzung

Die in diesem Dokument dargestellten Prozesse und Rollenmodelle stellen eine beispielhafte, organisationsunabhängige Referenz dar. Die konkrete Ausgestaltung kann je nach Unternehmensgröße, Governance-Struktur und regulatorischem Umfeld variieren.

Chain Horizon unterstützt Unternehmen bei der Konzeption, Anpassung und organisatorischen Verankerung solcher Modelle – insbesondere an der Schnittstelle zwischen Fachbereichen, IT und Informationssicherheit. Der Fokus liegt auf einer praxisnahen, minimalen und prüfbaren Ausgestaltung organisatorischer Prozesse.

Für eine erste Einordnung der eigenen Organisation bietet **Chain Horizon** ein **unverbindliches Erstgespräch** an.

Kontakt: info@chain-horizon.com

Hinweis / Disclaimer
Dieses Dokument stellt keine Rechtsberatung, keine steuerliche Beratung und keine verbindliche Compliance- oder Revisionsvorgabe dar. Die dargestellten Prozesse und RASCI-Zuordnungen dienen ausschließlich als unverbindliche Orientierungshilfe. Sie ersetzen weder eine rechtliche Prüfung noch eine organisationsspezifische Bewertung durch interne oder externe Fachstellen.

Die Verantwortung für die konkrete Ausgestaltung, Umsetzung und Wirksamkeit der beschriebenen Prozesse liegt beim jeweiligen Unternehmen.