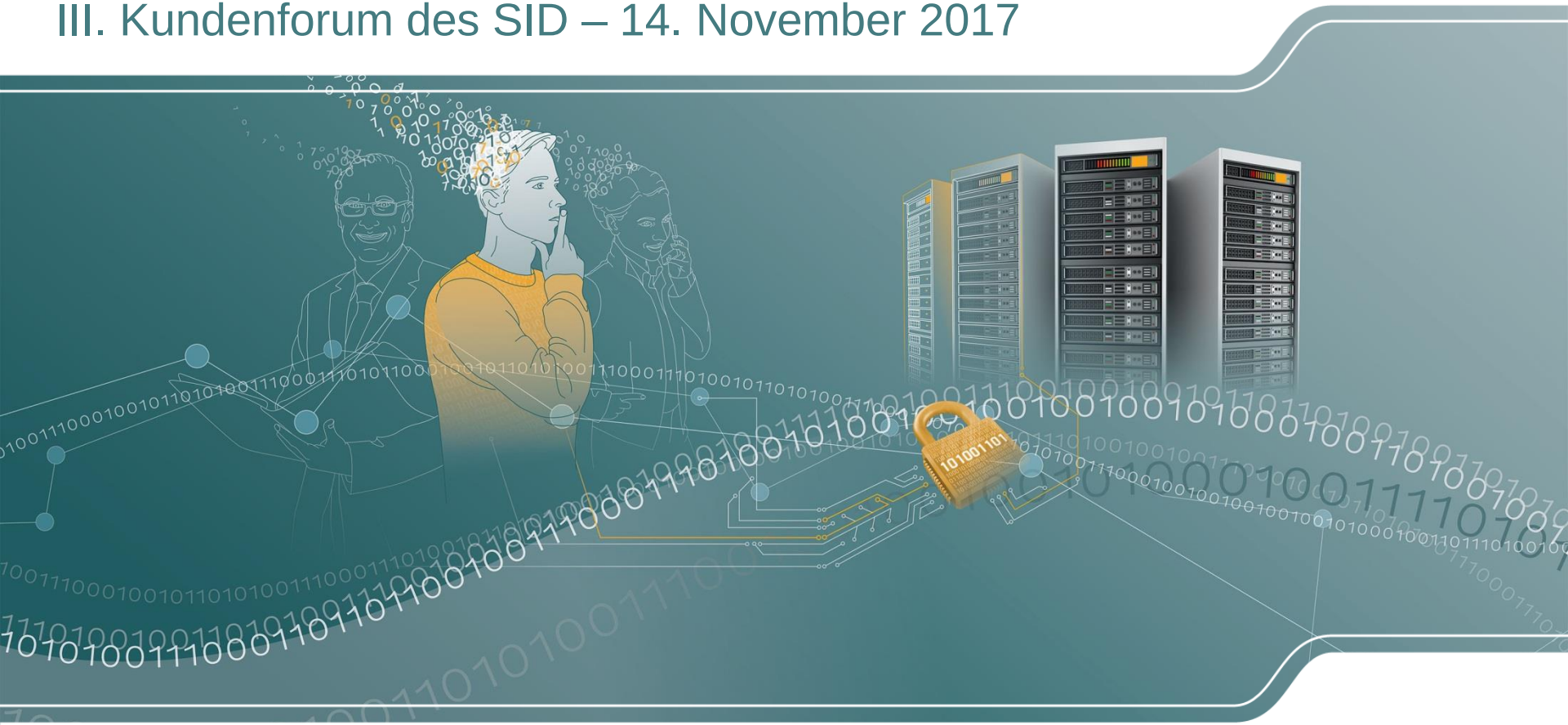
STAATSMINISTERIUM FÜR UMWELT UND LANDWIRTSCHAFT | Freistaat SACHSEN

STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE | Freistaat SACHSEN

Zertifizierung der EU-Zahlstelle – nach dem Audit ist vor dem Audit

III. Kundenforum des SID – 14. November 2017



AGENDA

1. Die EU-Zahlstelle Sachsen
2. Ablauf einer Erst-Zertifizierung
3. Lessons Learned – Erfahrungen aus dem Audit
4. Vorteile einer Zertifizierung
5. Nach dem Audit ist vor dem Audit…

Die EU-Zahlstelle Sachsen

VERORDNUNG (EU) Nr. 1306/2013 des Europäischen Parlaments und des Rates

- **Artikel 7 – Zulassung und Entzug der Zulassung der Zahlstellen ...**

  (1) Zahlstellen sind Dienststellen oder Einrichtungen der Mitgliedstaaten, die für die Verwaltung und Kontrolle der Ausgaben gemäß Artikel 4 Absatz 1 (EGFL) und Artikel 5 (ELER) zuständig sind

- Die Zuständigkeit im Freistaat Sachsen liegt beim Staatsministerium für Umwelt und Landwirtschaft (SMUL)

Anforderungen Informationssicherheit Zahlstellen

DELEGIERTE VERORDNUNG (EU) Nr. 907/2014 der Kommission

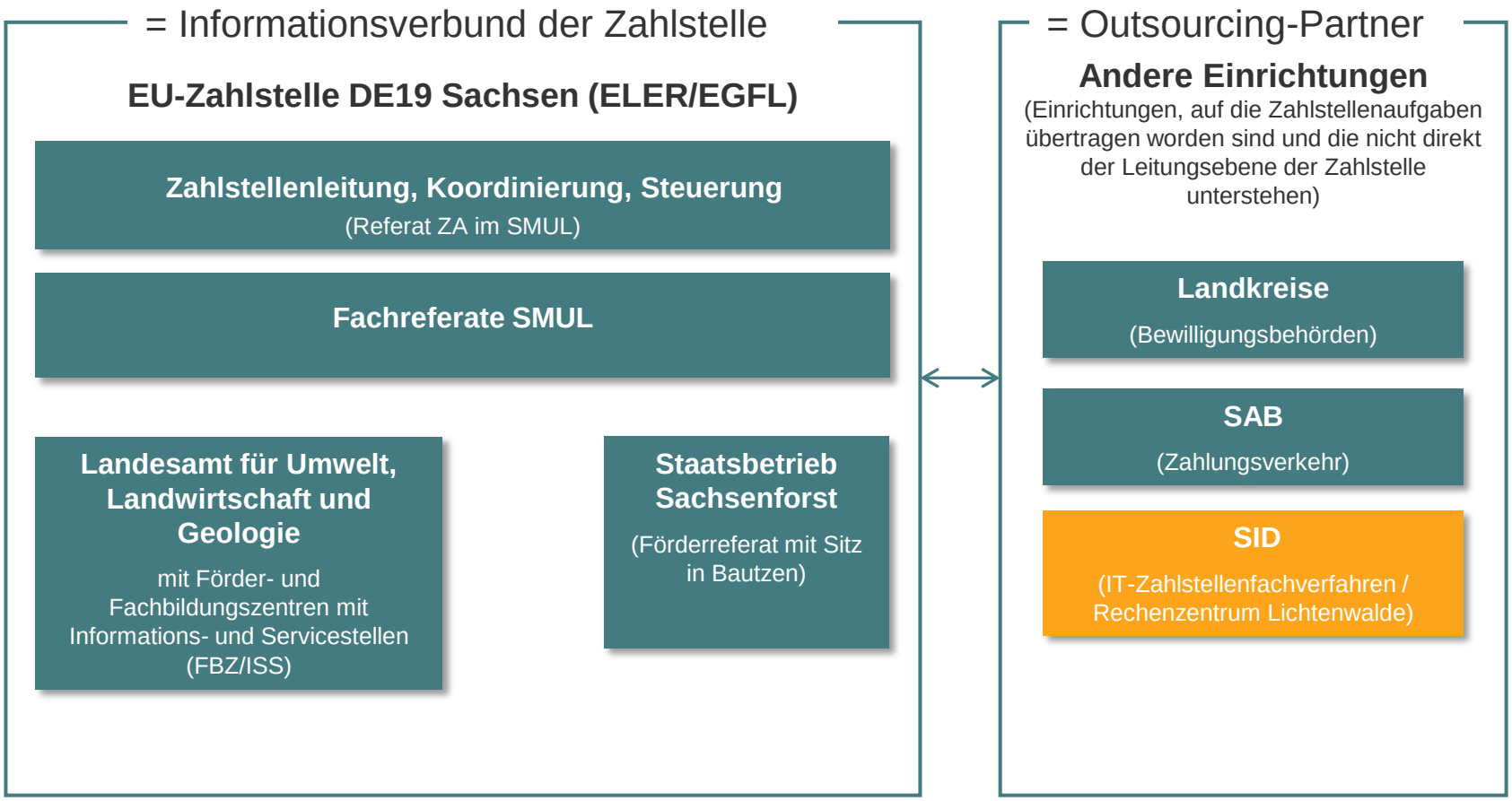
Anhang I Nr. 3 B. Sicherheit der Informationssysteme

- Ab **16. Oktober 2016 erfolgt die Zertifizierung** der Informationssysteme nach der ISO-Norm 27001: Informationssicherheits-Managementsysteme – Anforderungen

- Die Kommission kann die Mitgliedstaaten ermächtigen, die Sicherheit ihrer Informationssysteme **nach anderen anerkannten Normen zu zertifizieren**, sofern diese Normen **ein Schutzniveau gewährleisten**, das zumindest dem der **ISO-Norm 27001 gleichwertig** ist

Bundesamt für Sicherheit in der Informationstechnik

Übersicht Informationsverbund



IT-Grundschutz Bausteine und Maßnahmen

(Stand Oktober 2016)

48

IT-Grundschutz-Bausteine wurden für den Informationsverbund EU-Zahlstelle modelliert

42

IT-Grundschutz-Bausteine wurden für den Informationsverbund SID Zahlstelle modelliert

4106

Sicherheitsmaßnahmen ergeben sich aus der Modellierung für den Informationsverbund EU-Zahlstelle

3793

Sicherheitsmaßnahmen ergeben sich aus der Modellierung für den Informationsverbund SID Zahlstelle

AGENDA

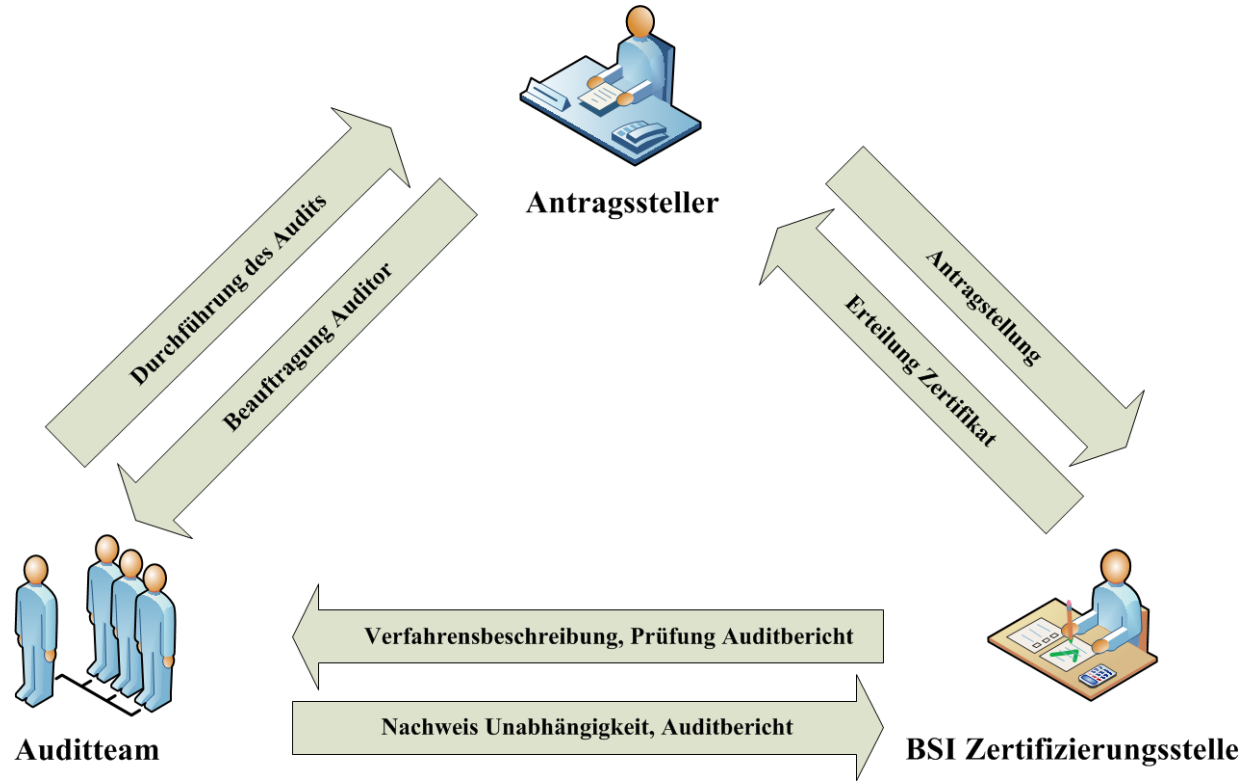
1. Die EU-Zahlstelle Sachsen
2. Ablauf einer Erst-Zertifizierung
3. Lessons Learned – Erfahrungen aus dem Audit
4. Vorteile einer Zertifizierung
5. Nach dem Audit ist vor dem Audit…

Ablauf einer Erst-Zertifizierung

Initiierung
- Abgabe Zertifizierungsantrag
- Abgabe Unabhängigkeitser-klärung der Auditoren

Min. 1 Monat | Max. 3 Monate | Max. 3 Monate

Rollen im Zertifizierungsverfahren



Quelle: Zertifizierungsschema des BSI, Version 1.2

Ablauf einer Erst-Zertifizierung

Initiierung
- Abgabe Zertifizierungsantrag
- Abgabe Unabhängigkeitser-klärung der Auditoren

Beginn der Auditierung

Auditphasen

Phase 1: Dokumentenprüfung

- Prüfung der Referenzdokumente

Phase 2: Umsetzungsprüfung vor Ort

- Prüfung der Strukturanalyse – auf tatsächliche Gegebenheiten
- Prüfung der Basis-Sicherheitschecks - Überprüfung des angegebenen Umsetzungsstatus
- Kontrollgänge - Gebäude, Serverräume, Technikräume und Arbeitsplätze

Ablauf einer Erst-Zertifizierung

Initiierung
- Abgabe Zertifizierungsantrag
- Abgabe Unabhängigkeitser-klärung der Auditoren

Beginn der Auditierung

Abgabe Auditbericht an BSI

Min. 1 Monat | Max. 3 Monate | Max. 3 Monate

Ergebnis der Auditierung – der Auditbericht

- **Prüfergebnisse** der Dokumenten- und Vor-Ort-Prüfung werden im Auditbericht festgehalten
- **Erkannte Abweichungen** werden in Listenform aufgeführt
- Mögliche Abweichungen:
  - Empfehlung (E),
  - geringfügige Abweichung (AG),
  - schwerwiegende Abweichung (AS)

Lauf. Nr.	*Abweichung*	*Abweichungstyp (E/AG/AS)*	*Behebungsfrist/ Nachweis*	*Status der Behebung*
1	[illegible]	AG 1: eine geringfügige Abweichung	Bis zum 1. Ü-Audit	offen
2	[illegible]	AG 2: eine geringfügige Abweichung	Bis zum 1. Ü-Audit	offen
3	[illegible]	E 1: eine Empfehlung	Bis zum 1. Ü-Audit	offen
4	[illegible]	AG 3: eine geringfügige Abweichung	Während des Vor-Ort-Audits behoben	korrekt

Ablauf einer Erst-Zertifizierung

Initiierung
- Abgabe Zertifizierungsantrag
- Abgabe Unabhängigkeitser-klärung der Auditoren

Beginn der Auditierung

Abgabe Auditbericht an BSI

Erteilung Zertifikat

Ergebnis der Zertifizierung

Ziel: Zertifizierung der EU-Zahlstelle nach ISO 27001 auf Basis von IT-Grundschutz

… wurde erreicht

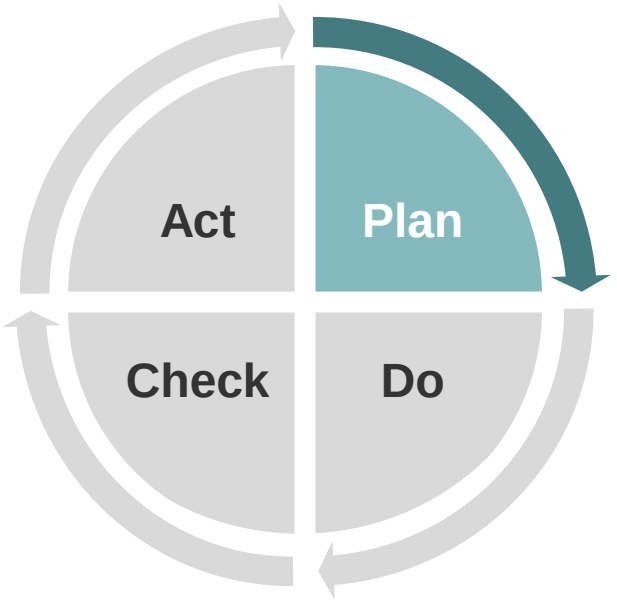
AGENDA

1. Die EU-Zahlstelle Sachsen
2. Ablauf einer Erst-Zertifizierung
3. Lessons Learned – Erfahrungen aus dem Audit
4. Vorteile einer Zertifizierung
5. Nach dem Audit ist vor dem Audit…

Lessons Learned – Erfahrungen aus dem Audit

Informationssicherheit ist kein Projekt

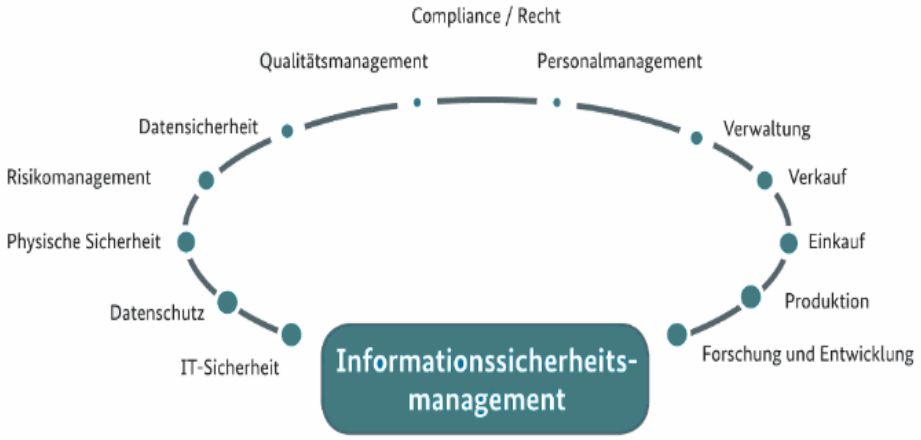
- Informationssicherheit ist ein dauerhafter Prozess
- Kontinuierliche Verbesserung (PDCA-Zyklus) ist sehr wichtig
- Initiale Erstellung eines Sicherheitskonzeptes kann in Form eines Projektes erfolgen



Lessons Learned – Erfahrungen aus dem Audit

Informationssicherheit ist nicht nur Aufgabe der IT

- Informationssicherheit liegt in der Verantwortung der Leitungsebene
- Umsetzung erfordert die Mitwirkung vieler Fachbereiche (Organisation, Personal, IT, …)
- Mitarbeiter müssen ihren Beitrag zur Informationssicherheit leisten und sensibilisiert werden



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Lessons Learned – Erfahrungen aus dem Audit

Verhältnismäßigkeit bei der Umsetzung von Sicherheitsmaßnahmen

- Es müssen nicht alle Maßnahmen 1:1 umgesetzt werden
- Bei der Umsetzung sollte das zugrundeliegende Risiko betrachtet werden
- Wirtschaftlichkeit ist ein wichtiger Faktor

AGENDA

1. Die EU-Zahlstelle Sachsen
2. Ablauf einer Erst-Zertifizierung
3. Lessons Learned – Erfahrungen aus dem Audit
4. Vorteile einer Zertifizierung
5. Nach dem Audit ist vor dem Audit…

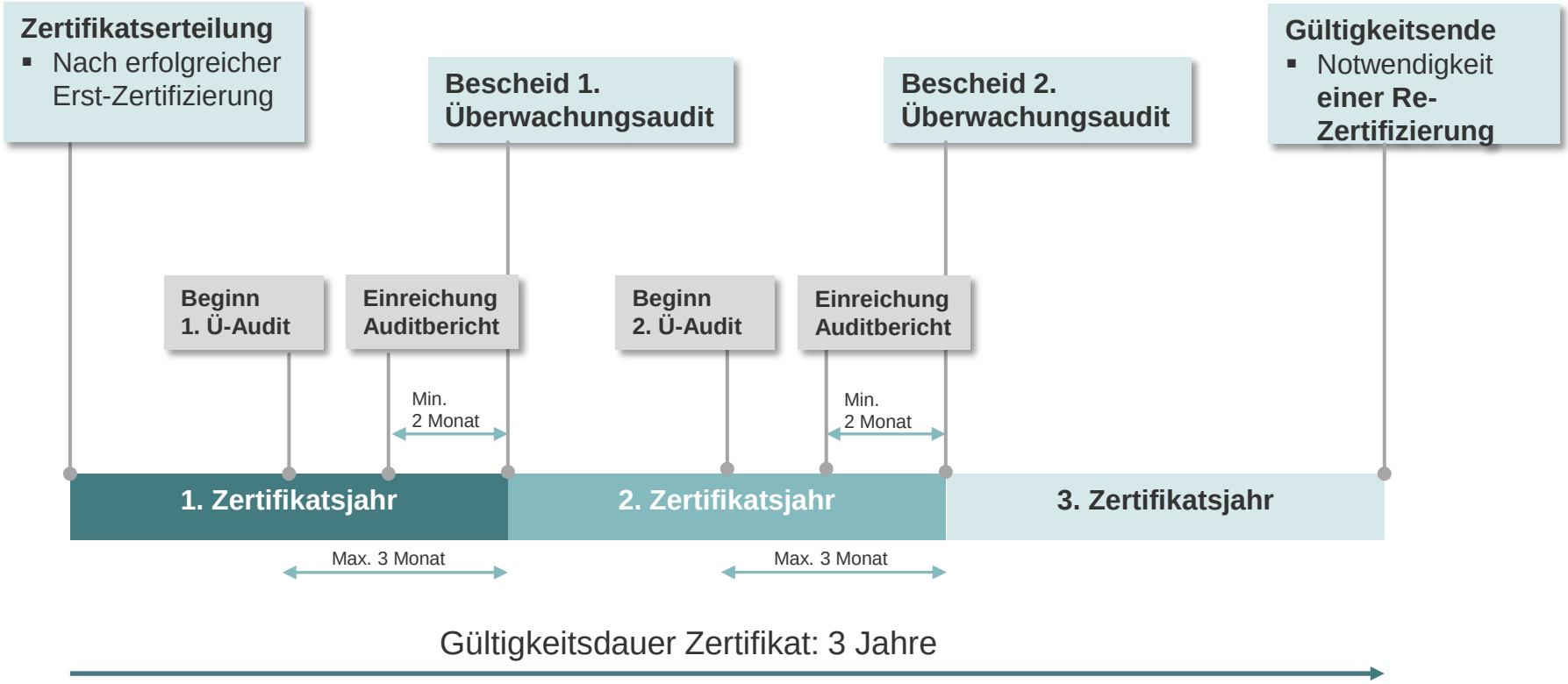
Vorteile einer Zertifizierung

- **Mehr Akzeptanz** für das Thema Informationssicherheit auf Leitungsebene
- **Stärkere Sensibilisierung** der Mitarbeiter für das Thema Informationssicherheit
- **Verbesserung der Abläufe** in vielen Bereichen der Institution und Erhöhung der **Transparenz** der Geschäftsprozesse
- **Nachweis in Haftungsfragen / Haftungsprozessen** (Prüfbehörden und Aufsichtsbehörden)

AGENDA

1. Die EU-Zahlstelle Sachsen
2. Ablauf einer Erst-Zertifizierung
3. Lessons Learned – Erfahrungen aus dem Audit
4. Vorteile einer Zertifizierung
5. Nach dem Audit ist vor dem Audit…

Nach dem Audit ist vor dem Audit…



Erfahren Sie mehr…

Sie finden uns unter:
www.sid.sachsen.de

Riesaer Straße 7
01129 Dresden
Telefon 0351 3264 5101
Telefax 0351 3264 5109