Verband der deutschen Internetwirtschaft e. V.

IMT

6. Paderborner Tag der IT-Sicherheit

17. März 2011, Universität Paderborn

Workshop 5:
Physikalische und umgebungsbezogene Sicherheit im Rechenzentrum

... aus Sicht integrierter Managementsysteme (Qualität, Prozesse, Informationssicherheit)

- → Anforderungen
- → Ziele
- → Maßnahmen
- → Anleitung zur Umsetzung

Agenda

1. Situation / Szenarien / Anforderungen
2. Managementsysteme
   → Ziele, Maßnahmen, Anleitung zur Umsetzung
3. DCSA (Datacenter Star Audit)
4. Sicherheit am Arbeitsplatz
5. Fazit / Zusammenfassung

Verband der deutschen Internetwirtschaft e. V.

1	2	3	4
Angriff von Außen auf Plattformen im Internet	Eindringen von außen in interne Netze und Anwendungen	Info- Abfluss durch Innentäter, Geschäftspartner und Wettbewerber im internen Netz	Verlust von Daten und Infrastruktur durch Katastrophen

Warum benötigen wir Informationssicherheit?

Die Informationsressourcen sind für ein wissensbasiertes Unternehmen von unschätzbarer Wichtigkeit.

Informationssicherheit

Kundenanforderungen

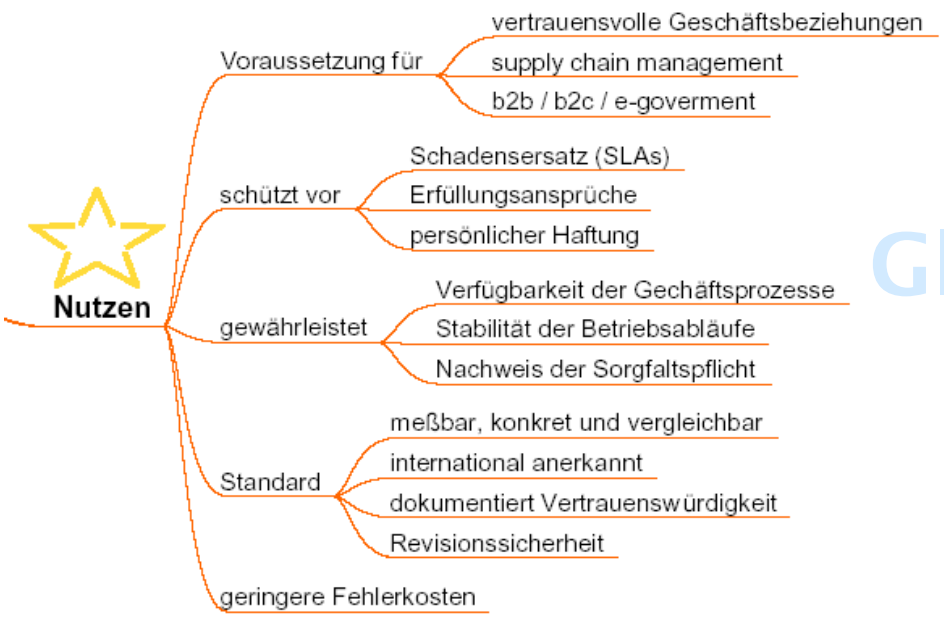
- öffentliche Kunden
- Zuverlässige Serviceleistungen
- sichere Infrastrukturen
- E-Business
- Entwicklungspartnerschaft
- Know-how Schutz

Rechtliche Vorgaben

- Risk Management z.B. KontraG
- Datenschutz
- Haftungsfragen
- Regulierung (z.B. FDA, HIPAA)
- Corp. Governance (z. B. Sarb.-Oxley, Basel II)

Eigeninteresse

- Schutz von Informationen und Wissen
  Schutz der Infrastrukturen
- Kooperation mit Wettbewerbern
  Image in der Öffentlichkeit



Wirtschaftlichkeit

Kompetenz

Glaubwürdigkeit

Bedrohungen erkennen

Vertrauen

Werte sichern

Akzeptanz

Wettbewerbsvorteil

- **Risiken erkennen**
  - → Sicherung der Geschäftskontinuität
- **Haftungsrisiko reduzieren** (§ 276 BGB)
  - → aus Verträgen, aus Delikten, aus Verpflichtungen (§ 9 BDSG)
- **Nachweis für Wirtschaftsprüfer**
  - → Bestandsführung, Sorgfaltspflicht
- **Aussenwirkung**
  - → Orientierung an internationalen Standard

Agenda

1 Situation / Szenarien / Anforderungen

2 **Managementsysteme**
→ Ziele, Maßnahmen, Anleitung zur Umsetzung

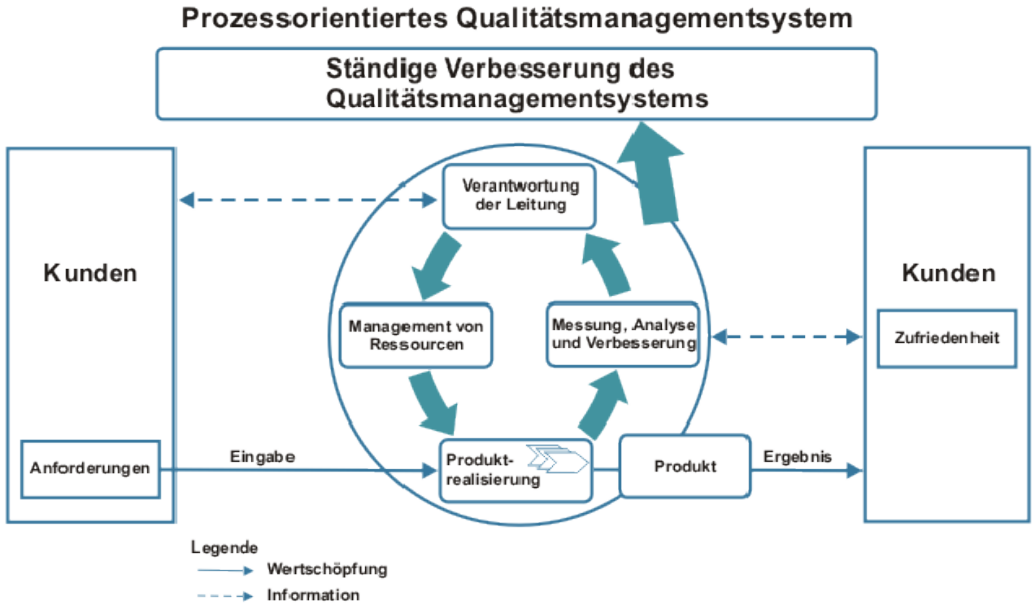
3 DCSA (Datacenter Star Audit)

4 Sicherheit am Arbeitsplatz

5 Fazit / Zusammenfassung

Qualitätsmanagements

- Kundenorientierung
- Mitarbeiterorientierung
- Prozessorientierung
- Lieferantenmanagement
- Messbarkeit der Ziele
- Ständige Verbesserung



Die Norm DIN EN ISO 9001 stellt in den Abschnitten 4 bis 8 konkrete Forderungen an ein Qualitätsmanagementsystem. Diese Forderungen umfassen die Aspekte:

4) Qualitätsmanagementsystem

5) Verantwortung der Leitung

6) Management von Ressourcen

7) Produktrealisierung

8) Messen, Analyse und Verbesserungen

4) Qualitätsmanagementsystem

5) Verantwortung der Leitung

6) Management von Ressourcen

7) Produktrealisierung

8) Messen, Analyse und Verbesserungen

Die Organisation muss die erforderlichen Ressourcen festlegen und bereitstellen, die benötigt werden, um das QM-System zu verwirklichen und die Wirksamkeit ständig zu verbessern sowie um die Kundenzufriedenheit durch die Erfüllung der Kundenanforderung zu erhöhen.

Dazu gehören:

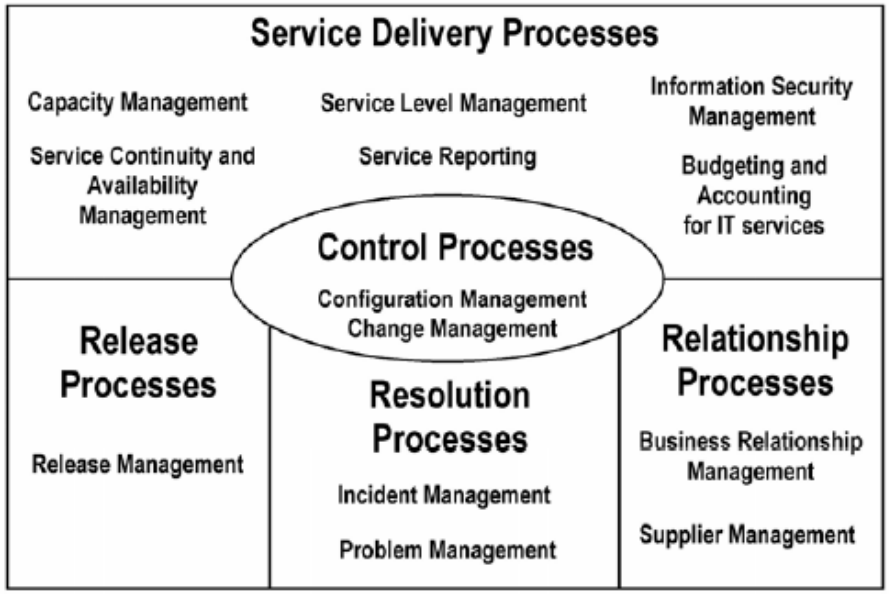
- ✓ **qualifiziertes Personal**
- ✓ **geeignete Schulungsmaßnahmen**
- ✓ **die erforderliche Infrastruktur einschl. Hard- und Software und unterstützende Dienstleistungen**
- ✓ **geeignete Arbeitsumgebung**

ISO 20000 – IT Service Management

- **Die ISO/IEC 20000 ist ein international anerkannter Standard zum IT-Service-Management, in dem die Anforderungen für ein professionelles IT-Service-Management dokumentiert sind.**

- **Folgende Prozesse sind relevant:**

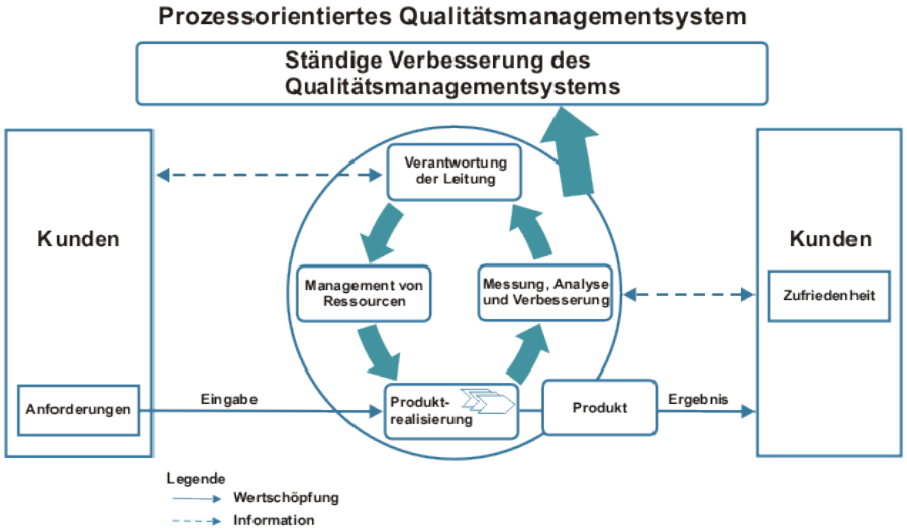
  - **Service Level Management**
  - **Service Reporting**
  - **Availability und Service Continuity Management**
  - **Budgeting and accounting for IT services**
  - **Capacity Management**
  - **Information Security Management**
  - **Business Relationship Management**
  - **Incident Management**
  - **Problem Management**
  - **Configuration Management**
  - **Change Management**
  - **Release Management**
  - **Supplier Management**



Grundsätze eines ISMS*

Ein ISMS hat zum Ziel, Risiken für das Unternehmen zu identifizieren, zu analysieren und durch entsprechende Maßnahmen beherrschbar zu machen.

Das Regelwerk ISO27001 lehnt sich in seinem Aufbau an die von ISO 9001 bekannte Vorgehensweise des PDCA-Regelkreises (Plan-Do-Check-Act) an und bietet die Möglichkeit der einfachen Integration eines ISMS in ein bestehendes Managementsystem.



*ISMS = Informations-Sicherheits-Management-System

- 4 Informations-Sicherheits-Management-System Anforderungen => ISMS
- 5 Verantwortung der Leitung
- 6 Internes ISMS Audit
- 7 Managementbewertung des ISMS
- 8 Verbesserung des ISMS

Management Handbuch

Managementteil

Annex A Überwachung und Ziele

- A.5 Sicherheits-Politik
- A.6 Organisation der Sicherheit
- A.7 Management von Werten
- A.8 Personelle Sicherheit
- A.9 Physische und umgebungsbezogene Sicherheit
- A.10 Management der Kommunikation und des Betriebs
- A.11 Zugangskontrolle
- A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen
- A.13 Management von Informationssicherheitsvorfällen
- A.14 Management des kontinuierlichen Geschäftsbetriebes
- A.15 Einhaltung der Verpflichtungen

Kontrollen

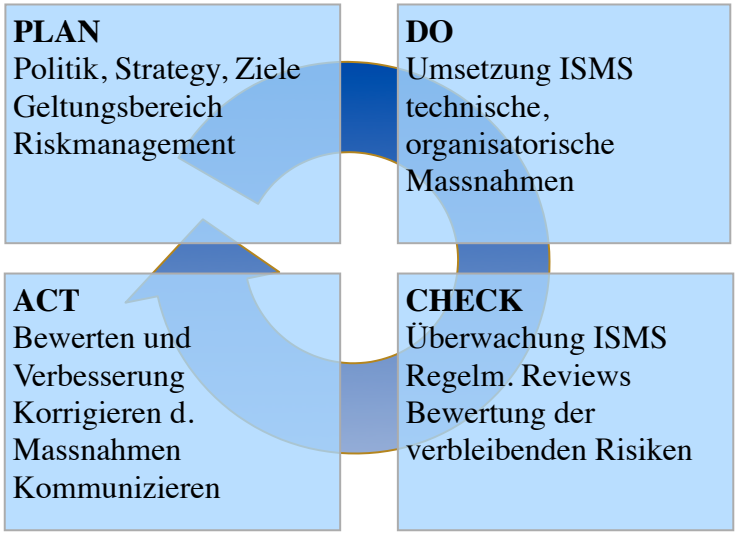
11 Managementgebiete („clauses“)
39 Maßnahmenziele („main security categories“)
133 Maßnahmen („baseline controls“)

IS-Regelwerk

- 4 **I**nformations-**S**icherheits-**M**anagement-**S**ystem Anforderungen => **ISMS**
- 5 Verantwortung der Leitung
- 6 Internes ISMS Audit
- 7 Managementbewertung des ISMS
- 8 Verbesserung des ISMS

Plan	Do	Check	Act
ISMS entwickeln	**ISMS in Kraft setzen und betreiben**	**ISMS überwachen und überprüfen**	**ISMS fortschreiben und verbessern**
Definition Anwendungs-bereich des ISMS	Rahmenbedingungen Implementation schaffen	Fehler / Verstöße des ISMS überwachen	Ursachen ermitteln
ISMS Politik definieren	Umsetzung der Schutzmaßnahmen	Review des ISMS durchführen	Verbesserungs-möglichkeiten zuweisen
Definition / Fortschreib. IT-Sicherheitsarchitektur	Mitarbeiter sensibilisieren/ausbilden	Review akzept. /restl. Risiken durchführen	
Definition Vorgehen f.d. Risk Assessment	Schutzmaßnahmen in Kraft setzen	IT-Audits durchführen	
Risk Assessment durchführen	Schutzmaßnahmen betreiben	Internes Audit des ISMS	
Risiken managen	Incidents / Events entdecken / behandeln	Managementprüfung durchführen	
Schutzmaßnahmen planen			

- 4 Informations-Sicherheits-Management-System Anforderungen => ISMS
- 5 Verantwortung der Leitung
- 6 Internes ISMS Audit
- 7 Managementbewertung des ISMS
- 8 Verbesserung des ISMS



- Festlegung der Sicherheitspolitik und -ziele, der relevanten Sicherheitsprozesse und Verfahren
- Festlegung der Vorgehensweise zur Risikoeinschätzung, zur Identifikation, Einschätzung und Behandlung der Risiken
- Genehmigung des Restrisikos

- Umsetzung des ISMS gemäß der beschlossenen Sicherheitspolitik, Maßnahmen, Prozesse und Verfahren
- Einbindung der Mitarbeiter durch Festlegung der Verantwortung, Rechte und Pflichten. Personalauswahl und -schulung
- Daten und Dokumente lenken

- Durchführen interner Audits
- Einschätzen und ggf. messen der Sicherheitslage anhand der Vorgaben
- Auswerten von Sicherheitsvorfällen
- Berichterstattung an das Management zwecks Bewertung

- Ergreifen von Korrektur- und Vorbeugungsmaßnahmen, basierend auf den Ergebnissen der Überprüfung von Sicherheitsvorfällen
- Ableitung von Maßnahmen zur kontinuierlichen Verbesserung des ISMS
- Management-Reviews

Überwachung und Ziele

A.5 Sicherheits-Politik

A.6 Organisation der Sicherheit

A.7 Management von Werten

A.8 Personelle Sicherheit

A.9 Physische und umgebungsbezogene Sicherheit

A.10 Management der Kommunikation und des Betriebs

A.11 Zugangskontrolle

A.12 Beschaffung, Entwicklung und Wartung von Systemen

A.13 Management von Informationssicherheitsvorfällen

A.14 Management des kontinuierlichen Geschäftsbetriebes

A.15 Einhaltung der Verpflichtungen

Überwachung und Ziele

A.5 Sicherheits-Politik

A.6 Organisation der Sicherheit

A.7 Management von Werten

A.8 Personelle Sicherheit

A.9 Physische und umgebungsbezogene Sicherheit

A.10 Management der Kommunikation und des Betriebs

A.11 Zugangskontrolle

A.12 Beschaffung, Entwicklung und Wartung von Systemen

A.13 Management von Informationssicherheitsvorfällen

A.14 Management des kontinuierlichen Geschäftsbetriebes

A.15 Einhaltung der Verpflichtungen

Ziel:

SICHERHEITSBEREICHE

→ Verhinderung von unberechtigten Zutritt

→ Schutz gegen externe Bedrohung

SICHERHEIT VON BETRIEBSMITTEL

→ Verhindern von Verlust, Schaden, Diebstahl und Kompromittierung von Werten

Festlegung von Sicherheitsbereichen
Sicherheit der Einrichtungen
Allgemeine Anweisungen
Regelung über örtliche Standortverwaltung (SRE)
Personenkontrolle, Schleuse, Ausweis, Chipkarte, SIPORT

✓ Zutrittslogbuch
✓ Büros, Fenster, Schreibtische, Schränke der MA verschlossen
✓ Überwachung der Umgebungsbedingungen
✓ Regelung zur ordnungsgemässen Entsorgung
✓ Dokumente / Laptops etc. in verschliessbaren Schränken aufbewahren
✓ Mitverträge, Infrastrukturen → Abhängigkeiten

- Informationsverarbeitende Geräte befinden sich in Sicherheitszonen und sind mit entsprechenden Sicherheitsschranken und Zutrittskontrollen versehen
- Geräte werden physisch vor Sicherheitsbedrohungen u. umgebungsbedingten Gefahren geschützt
- Die erforderliche Infrastruktur zum Betrieb der Geräte (Stromversorgung, Telekommunikationsleitg.) wurde bei der Kalkulation der Risiken berücksichtigt
- Es wurden Wartungspläne erstellt und diese werden befolgt
- Es existieren allgemeine Sicherheitsanweisungen, z.B. hinsichtlich dem Aufräumen von Schreibtischen, Umgang mit Firmenequipment

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen	Sicherheitszonen (Hindernisse wie Wände, über Zutrittskarten kontrollierte Zugänge oder mit Pförtnern besetzte Empfangsbereiche) müssen die Abschnitte schützen, die informationsverarbeitende Einrichtungen beherbergen.
Zutrittskontrolle	Sicherheitsbereiche müssen durch angemessene Zutrittskontrollen geschützt sein, um sicherzustellen, dass nur autorisierten Mitarbeitern Zutritt gewährt wird.
Sicherungen von Büros, Räumen u. Einrichtungen	Physischer Schutz für Büros, Räume und Einrichtungen muss geplant und umgesetzt werden
Schutz vor Bedrohungen von Außen und aus der Umgebung	Physischer Schutz gegen Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen und anderen Formen natürlicher und von Menschen verursachter Katastrophen muss vorgesehen und umgesetzt sein
Arbeit in Sicherheitszonen	Physischer Schutz und Richtlinien für die Arbeit in Sicherheitszonen muss entwickelt und umgesetzt werden
Öffentlicher Zugang, Anlieferung- u. Ladezonen	Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Zugangspunkte, an denen unbefugte Personen den Standort betreten können, müssen kontrolliert und, *sofern möglich*, von informationsverarbeitenden Einrichtungen getrennt werden, um unerlaubten Zutritt zu verhindern

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen
Zutrittskontrolle
Sicherungen von Büros, Räumen u. Einrichtungen
Schutz vor Bedrohungen von Außen und aus der Umgang
Arbeit in Sicherheitszonen
Öffentlicher Zugang, Anlieferung- u. Ladezonen

- Lage und Stärke der Sicherheitszonen durch Risikobetrachtung ermitteln (entsprechend der Assets)
- Physisch solide Begrenzung. Stabile Konstruktion der Wände.
- Türen sollen angemessenen Schutz gegen unautorisierten Zutritt bieten (Gitter, Alarmierung, Schlösser)
- Fenster im Erdgeschoss vergittern
- Zutritt soll sich auf autorisierte Mitarbeiter beschränken. → Pförtner oder andere Einrichtungen zu Kontrolle
- Physische Barrieren sollen, wo angemessen, unautorisierten Zutritt und Verschmutzung durch die Umgebung verhindern
- Notwendiges Maß des Brandschutzes identifizieren. Alle Brandschutztüren sollten alarmgesichert, überwacht und in Verbindung mir den anschließenden Wänden getestet werde. → BKO hinzuziehen
- Einbruchmeldesysteme (Außentüren und Fenster) installieren und regelmäßig testen
- Durch die Organisation verwaltete, informationsverarbeitende Einrichtungen sollten physisch von informationsverarbeitende Einrichtungen getrennt sein, die durch Externe administriert oder betrieben werden

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen	
Zutrittskontrolle	➢ Datum/Uhrzeit des Zutritts/Verlassens eines Bereichs durch einen Besucher sollten aufgezeichnet werden ➢ Alle Besucher sollten permanent überwacht/begleitet werden (Es sein denn Zutritt ist autorisiert worden) ➢ Zutritt sollte Zweckgebunden sein. Über Sicherheitsanforderungen und Verhalten im Notfall in Kenntnis setzen ➢ Zutritt zu Bereichen in den sensitive Informationen verarbeitet oder gespeichert werden sollten kontrolliert werden und nur autorisierten Personen gewährt werden. (Authentisierung über Chip, PIN, etc. ..) Die Nachvollziehbarkeit aller Zutrittsvorgänge muß sichergestellt sein ➢ Alle Mitarbeiter, Vertragspartner und Dritte sowie alle Besucher sollten eine sichtbare Identifikation tragen ➢ Dienstleister und Dritte sollten nur Zutritt zu Sicherheitszonen erhalten, wenn dies erforderlich ist ➢ Zutrittsrechte zu Sicherheitszonen sollten regelmäßig überprüft, aktualisiert und wenn notwendig entzogen werden
Sicherungen von Büros, Räumen u. Einrichtungen	
Schutz vor Bedrohungen von Außen und aus der Umgang	
Arbeit in Sicherheitszonen	
Öffentlicher Zugang, Anlieferung- u. Ladezonen	

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen
Zutrittskontrolle
Sicherungen von Büros, Räumen u. Einrichtungen
Schutz vor Bedrohungen von Außen und aus der Umgang
Arbeit in Sicherheitszonen
Öffentlicher Zugang, Anlieferung- u. Ladezonen

- Einhaltung relevanter Gesundheits- und Sicherheitsvorschriften soll sichergestellt werden
- wichtige Einrichtungen sollten so gelegen sein, dass sie der Allgemeinheit nicht zugänglich sind
- Gebäude sollten so unauffällig wie möglich sein und möglichst keine Hinweise auf ihren Zweck bereitstellen
- Es sollten keine Zeichen und Schilder, werde außen noch innen, einen Hinweis auf informationsverarbeitende Aktivitäten geben
- Verzeichnisse und interne Telefonbücher, die einen Hinweis auf die Lage von informationsverarbeitenden Einrichtungen mit sensitiven Informationen geben, sollten nicht öffentlich zugänglich sein

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen
Zutrittskontrolle
Sicherungen von Büros, Räumen u. Einrichtungen
Schutz vor Bedrohungen von Außen und aus der Umgang
Arbeit in Sicherheitszonen
Öffentlicher Zugang, Anlieferung- u. Ladezonen

- gefährliche und leicht entzündliche Materialien sollten in sicherer Entfernung von Sicherheitszonen gelagert werden
- Materialien mit hoher Brandlast, wie Schreibmaterial und Papier, sollten generell nicht in einer Sicherheitszone gelagert werden
- Ersatzgeräte und Backup-Medien sollten in sicherer Entfernung von der Sicherheitszone untergebracht sein um zu verhindern, dass dies bei einem Schaden am primären Standort auch betroffen sind
- angemessene Ausstattung zur Brandbekämpfung sollte bereitgestellt und adäquat platziert sein

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen
Zutrittskontrolle
Sicherungen von Büros, Räumen u. Einrichtungen
Schutz vor Bedrohungen von Außen und aus der Umgang
Arbeit in Sicherheitszonen
Öffentlicher Zugang, Anlieferung- u. Ladezonen

- das Personal sollte nur bei Bedarf (Need-to-know-Basis) von der Existenz einer Sicherheitszone und den Aktivitäten innerhalb der Zone Kenntnis haben
- nichtüberwachtes Arbeiten in Sicherheitszonen sollte, aus Gründen der Sicherheit und um Gelegenheiten für schädliche Aktivitäten (Sabotage) zur verringern, vermieden werden
- nichtbesetzte Sicherheitszonen sollten verschlossen und regelmäßig kontrolliert werden
- das Mitführen von Aufnahmegeräten gleich welcher Art sollte, sofern nicht explizit gestattet, verboten sein

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Schutz vor unerlaubten Zutritt zu und Beschädigung und Störung von Organisationsinfrastrukturen und der Organisation gehörenden Informationen

Sicherheitszonen	
Zutrittskontrolle	
Sicherungen von Büros, Räumen u. Einrichtungen	
Schutz vor Bedrohungen von Außen und aus der Umgang	
Arbeit in Sicherheitszonen	
Öffentlicher Zugang, Anlieferung- u. Ladezonen	➢ Zugang zu Anlieferungs- und Ladezonen eines Gebäudes von außerhalb sollte nur identifiziertem und berechtigtem Personal erlaubt sein ➢ die Anlieferungs- und Ladezone sollte so gestaltet sein, dass Lieferungen ausgeladen werden können, ohne dass das Lieferpersonal Zutritt zu anderen Bereichen des Gebäudes erhält ➢ die Außentüren einer Anlieferungs- und Ladezone sollten gesichert sein, wenn die Türen zum inneren Bereich geöffnet sind ➢ eingehendes Material sollte auf potentielle Bedrohungen hin untersucht werden bevor dieses Material aus der Anlieferungs- und Ladezone zu seinem Bestimmungsort gebracht wird ➢ eingehendes Material sollte bei Anlieferung laut Vorgaben inventarisiert werden ➢ eingehende und ausgehende Lieferungen sollten, wo es möglich ist, physikalisch getrennt aufbewahrt werden

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

Platzierung und Schutz von Betriebsmitteln	Betriebsmittel müssen so platziert und geschützt werden, dass das Risiko durch Bedrohungen aus der Umgebungen, durch Katastrophen als auch die Gelegenheit für unerlaubten Zugriff reduziert wird
Unterstützende Versorgungseinrichtungen	Betriebsmittel müssen vor Stromausfällen und Ausfällen anderer Versorgungseinrichtungen geschützt werden
Sicherheit der Verkabelung	Versorgerleitungen für Strom und Telekommunikation, welche Daten transportieren oder die Informationssysteme versorgen, müssen vor Abhören und Beschädigung geschützt sein
Instandhaltung von Gerätschaften	Gerätschaften müssen korrekt instand gehalten und gepflegt werden, um ihre Verfügbarkeit und Vollständigkeit sicherzustellen
Sicherheit von außerhalb des Standorts befindlicher Ausrüstung	Betriebmittel, die sich außerhalb des Standorts befinden, müssen unter Beachtung der unterschiedlichen Risiken, die durch den Einsatz außerhalb eines Standorts entstehen, geschützt werden
Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	Bei jeglicher Gerätschaft, welche Speichermedien enthält, muss vor der Entsorgung überprüft werden, ob alle sensiblen Daten und die lizenzierte Software entfernt oder sicher überschrieben wurden
Entfernung des Eigentum	Betriebsmittel, Informationen oder Software dürfen nicht unberechtigt aus dem Standort entfernt werden

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

Platzierung und Schutz von Betriebsmitteln
Unterstützende Versorgungseinrichtungen
Sicherheit der Verkabelung
Instandhaltung von Gerätschaften
Sicherheit von außerhalb des Standorts befindlicher Ausrüstung
Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
Entfernung des Eigentum

- Betriebsmittel sollten so platziert werden, dass unnötiger Zugang in den Arbeitsbereich minimiert wird
- informationsverarbeitende Einrichtungen, die sensitive Daten verarbeiten, sollten so platziert werden, dass das Risiko einer Einsicht durch Unbefugte während der Nutzung minimiert wird. Lagerstätten sollten gegen unerlaubten Zugriff geschützt werden
- Betriebsmittel, die einen speziellen Schutz benötigen, sollten isoliert untergebracht sein, um den allgemeinen Schutzbedarf der Umgebung zu reduzieren
- es sollten Maßnahmen getroffen werden, um die potentiellen Risiken durch physische Bedrohungen wie z.B. Diebstahl, Feuer, Explosivstoffe, Rauch, Wasser, Staub, Vibration, chemische Effekte, Störungen der elektrischen Versorgung, Störung der Kommunikation, elektromechanische Abstrahlung und Vandalismus zu reduzieren
- Regelungen zum Essen, Trinken und Rauchen in der unmittelbaren Nähe informationsverarbeitender Einrichtungen sollten getroffen werden
- Umweltbedingungen wie Temperatur und Luftfeuchtigkeit sollten überwacht werden, damit kein Fall eintritt der den Betrieb informationsverarbeitender Einrichtungen negativ beeinflusst
- alle Gebäude sollten mit einem Blitzschutz versehen sein. Alle Versorgungsleitungen für Strom und Kommunikation sollten mit Überspannungsschutz ausgestattet sein
- Betriebsmittel, die sensitive Informationen verarbeiten, sollten gegen Abstrahlung geschützt sein, um den derartigen Abfluss von Informationen zu verhindern

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

- Platzierung und Schutz von Betriebsmitteln
- **Unterstützende Versorgungseinrichtg.**
- Sicherheit der Verkabelung
- Instandhaltung von Gerätschaften
- Sicherheit von außerhalb des Standorts befindlicher Ausrüstung
- Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
- Entfernung des Eigentum

- Alle unterstützenden Versorgungseinrichtungen, z.B. Strom, Wasser, Abwasser, Heizung/Lüftung und Klima sollten entsprechend den Anforderungen ausgelegt sein
- Um einen unterbrechungsfreien Betrieb bzw. ordnungsgemäßes Herunterfahren von geschäftskritischen Anwendungen sicherzustellen, wird der Einsatz einer unterbrechungsfreien Stromversorgung empfohlen
  - → Maßnahmenpläne, Notstromaggregat, ausreichende Menge Treibstoff, USV, redundante Stromversorgung
- Not-Aus-Schalter, Notbeleuchtung
- Wasserversorgung zuverlässig und angemessen dimensionieren, um Klima-, Befeuchtungsgeräte und Brandschutzeinrichtungen zu versorgen. Im Bedarfsfall Alarmierungssysteme auswählen und installieren
- Telekommunikationseinrichtungen sollten redundant über zwei unterschiedliche Routen an den Telekommunikationsdienstanbieter angebunden sein, um sicherzustellen, das beim Ausfall einer Anbindung die Kommunikation noch möglich ist
- Alle Versorgungseinrichtungen sollten regelmäßig hinsichtlich ihrer Funktionstüchtigkeit geprüft und angemessen getestet werden, um so das Risiko einer Fehlfunktion oder eines Ausfalls zu minimieren

→ Kontinuierliche Sicherstellung

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

- Platzierung und Schutz von Betriebsmitteln
- Unterstützende Versorgungseinrichtungen
- **Sicherheit der Verkabelung**
- Instandhaltung von Gerätschaften
- Sicherheit von außerhalb des Standorts befindlicher Ausrüstung
- Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
- Entfernung des Eigentum

- Strom und Telekommunikationsleitungen zu informationsverarbeitenden Einrichtungen sollten, wo möglich, unterirdisch verlegt oder anders geschützt werden
- Netzkabel sollten, z.B. durch Verwendung eines Kabelkanals oder durch Vermeidung von Strecken, die über öffentliche Bereiche führen, vor unbefugtem Abhören und Beschädigung geschützt werden
- Stromkabel sollten vor Kommunikationskabeln getrennt geführt werden, um Interferenzen zu vermeiden
- Um Fehlbedienungen , z.B. falsches Patchen von Netzverbindungen, zu vermeiden, sollten klar identifizierbare Markierungen an Kabeln und Geräten vorhanden sein
- Um die Wahrscheinlichkeit von Fehlern zu reduzieren, sollte die gesamte Verkabelung (inkl. Patchfelder) ausführlich dokumentiert werden
- Für sensitive o. kritische Systeme sollten die folgenden, zusätzlichen Maßnahmen in Erwägung gezogen werden
  1. Einsatz von armierten Kabelkanälen und verschlossenen Verteilerräumen und –schränken
  2. Nutzung von alternativen Strecken oder Übertragungsmedien, welche angemessenen Schutz bieten
  3. Einsatz von Glasfaser
  4. Abschirmung der Verkabelung gegen elektromagnetische Abstrahlung
  5. technisches Abtasten (Scannen) und Inspektion der Verkabelung nach unerlaubt angeschlossenen Geräten
  6. kontrollierter Zugang zu Patch-Feldern und Verteilerräumen

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

- Platzierung und Schutz von Betriebsmitteln
- Unterstützende Versorgungseinrichtungen
- Sicherheit der Verkabelung
- **Instandhaltung von Gerätschaften**
- Sicherheit von außerhalb des Standorts befindlicher Ausrüstung
- Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
- Entfernung des Eigentum

- Geräte sollten gemäß der vom Hersteller empfohlenen Spezifikationen und Intervall gepflegt werden
- Reparaturen/Wartungsmaßnahmen sollten nur von dafür zugelassenem Wartungspersonal durchgeführt werden
- alle vermuteten und tatsächlichen Fehler sowie alle getroffenen vorbeugenden und Fehlerbehebenden Maßnahmen sollten dokumentiert werden
- angemessene Maßnahmen sollten getroffen werden, wenn für Geräte Wartung vorgesehen ist. Dabei sollte Berücksichtigt werden, ob die Wartung durch eigenes Personal oder durch Externe ausgeführt wird. Wenn notwendig sollten sensitive Informationen vorher entfernt werden oder das Wartungspersonal für diese Arbeit genügend vertrauenswürdig sein
- Alle Anforderungen, die als Auflagen von Versicherungen oder zur Sicherstellung von Gewährleistungen (Garantien) vorgegeben sind, sollten erfüllt werden

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

- Platzierung und Schutz von Betriebsmitteln
- Unterstützende Versorgungseinrichtungen
- Sicherheit der Verkabelung
- Instandhaltung von Gerätschaften
- **Sicherheit von außerhalb des Standorts befindlicher Ausrüstung**
- Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
- Entfernung des Eigentum

- Betriebsmittel und Speichermedien, die mitgeführt werden, sollten in der Öffentlichkeit nicht unbeaufsichtigt sein Laptops sollten als Handgepäck mitgeführt werden und nach Möglichkeit nicht offensichtlich getragen werden
- die Herstellerempfehlungen zum Schutz von Betriebsmitteln sollten zu jeder Zeit Beachtung finden, z.B. der Schutz vor starken magnetischen Feldern
- Maßnahmen für Heimarbeitsplätze sollten durch eine Risikobetrachtung identifiziert und entsprechend umgesetzt werde, z.B. abschließbare Schränke, eine „Clean-Desk-Policy“, Zugriffskontrolle für Computer und eine sichere Kommunikationsverbindung zum Büro (→ SNT)
- Betriebsmittel, die außerhalb der Standorte einer Organisation betrieben werden, sollten angemessen versichert sein

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

- Platzierung und Schutz von Betriebsmitteln
- Unterstützende Versorgungseinrichtungen
- Sicherheit der Verkabelung
- Instandhaltung von Gerätschaften
- Sicherheit von außerhalb des Standorts befindlicher Ausrüstung
- **Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln**
- Entfernung des Eigentum

- Geräte die sensitive Informationen enthalten, sollten physikalisch zerstört oder die enthaltene Information sollte zerstört, gelöscht und überschrieben werden. Dabei sollten, anstelle der Standard-Lösch- und Formatierfunktion, Techniken angewendet werden, die sicherstellen, dass die ursprünglichen Informationen nicht mehr zurückgewonnen werden können

A.9 Physische und umgebungsbezogene Sicherheit

A.9.2 Sicherheit von Betriebsmitteln

Verhindern des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation

- Platzierung und Schutz von Betriebsmitteln
- Unterstützende Versorgungseinrichtungen
- Sicherheit der Verkabelung
- Instandhaltung von Gerätschaften
- Sicherheit von außerhalb des Standorts befindlicher Ausrüstung
- Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
- **Entfernung des Eigentum**

- Betriebsmittel, Informationen oder Software sollten nicht unberechtigt aus dem Standort entfernt werden
- Mitarbeiter, Vertragspartner und Externe, die die Mitnahme von Betriebsmittel genehmigen dürfen, sollten eindeutig bekannt sein
- die Mitnahme/Entfernung von Betriebsmitteln sollte zeitgleich begrenzt sein. Bei Rückgabe sollte die Einhaltung dieser Zeiträume überprüft werden
- dort, wo es notwendig und angebracht ist, sollte die Entnahme und die Rückgabe von Betriebsmitteln aufgezeichnet werden

Agenda

1 Situation / Szenarien / Anforderungen

2 Managementsysteme
→ Ziele, Maßnahmen, Anleitung zur Umsetzung

3 **DCSA (Datacenter Star Audit)**

4 Sicherheit am Arbeitsplatz

5 Fazit / Zusammenfassung

Agenda

1 Situation / Szenarien / Anforderungen

2 Managementsysteme
→ Ziele, Maßnahmen, Anleitung zur Umsetzung

3 DCSA (Datacenter Star Audit)

4 **Sicherheit am Arbeitsplatz**

5 Fazit / Zusammenfassung

Agenda

1 Situation / Szenarien / Anforderungen

2 Managementsysteme
→ Ziele, Maßnahmen, Anleitung zur Umsetzung

3 DCSA (Datacenter Star Audit)

4 Sicherheit am Arbeitsplatz

5 Fazit / Zusammenfassung

Service Continuity and Availability Management

- **ZIEL**
  Sicherzustellen das unter allen Umständen der mit dem Kunden vereinbarte Service verpflichtend bzgl. Kontinuität und Verfügbarkeit erbracht wird.

- **FORDERUNG**
  - ✓ Verfügbarkeits- und Service Kontinuitäts- Anforderungen müssen an Hand eines Business Plans, SLA´s und einer Risikobewertung identifiziert werden. Anforderungen sollen Zugriffsrechte und Antwortzeiten als auch die „End to End“ Verfügbarkeit von System Komponenten enthalten.
  - ✓ Der Verfügbarkeits- und Kontinuitäts- Plan soll mindestens jährlich erstellt und überprüft werden, um sicherzustellen, dass unter allen Umständen die vereinbarten Anforderungen vom „normal“ Ausfall bis hin zum „Major“ Ausfall abgedeckt sind. Dieser Plan soll sicherstellen das die vom Geschäft geforderten vereinbarten Änderungen widergespiegelt werden.
  - ✓ Der Verfügbarkeits- und Kontinuitäts-Plan soll bei jeder größeren Änderung im Geschäftsumfeld „re-tested“ werden.
  - ✓ Der Change Management Prozess soll die Auswirkung einer jeden Änderung auf den Verfügbarkeits- und Kontinuitäts-Plan überprüfen.
  - ✓ Verfügbarkeit soll gemessen und aufgezeichnet werden. Ungeplante nicht Verfügbarkeit soll untersucht und entsprechende Maßnahmen auslösen.

    Notiz Wo möglich, sollten für potentielle Angelegenheiten Präventivmaßnahmen ergriffen werden.

  - ✓ Der Service Kontinuitäts-Plan, die Kontakt Listen und die „Configuration Management Database“ (CMDB) soll auch verfügbar sein, wenn der normale Büro Zugriff verhindert ist. Der Service Kontinuitäts-Plan soll die Rückkehr zum normalen arbeiten enthalten.
  - ✓ Der Service Kontinuitäts-Plan soll in Übereinstimmung mit den Geschäftsanforderungen getestet sein.
  - ✓ Alle Kontinuitätstests müssen aufgezeichnet werden und Testausfälle in einem Aktionsplan beschrieben sein