

IT Security am Airport Nürnberg

Jörg Ziegler

IT Security

Agenda	→ Sicherheit am Airport Nürnberg
	→ Prozess "IT-Sicherheit" nach BSI
	→ IT-Sicherheitsmanagement – Einführung und laufender Betrieb
	→ Schutzbedarf / Bedrohungen
	→ Maßnahmen zur IT-Sicherheit
	→ Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security
	→ IT Security Report
	→ Aktuelle Entwicklungen in der IT-Sicherheit

IT Security

Sicherheit am Airport Nürnberg	→ Risk-Management
Prozess „IT-Sicherheit“ nach BSI	→ Sicherheit im Luftverkehr
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	→ Baulicher Brandschutz
Schutzbedarf / Bedrohungen	→ Baustellensicherheit
Maßnahmen zur IT-Sicherheit	→ Vorbeugender Brandschutz Brandschutzbeauftragter
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	→ Arbeitssicherheit
IT Security Report	→ Datenschutz - Datenschutzbeauftragter
Aktuelle Entwicklungen in der IT-Sicherheit	→ Rechtssicherheit
	→ Versicherungsschutz
	→ IT-Sicherheit
	→ ...

IT Security

Sicherheit von Geschäftsprozessen durch IT-Unterstützungsprozesse (IT-Infrastruktur und Daten)

Sicherheit am Airport Nürnberg
Prozess „IT-Sicherheit“ nach BSI
IT-Sicherheitsmanagement-Einführung und laufender Betrieb
Schutzbedarf / Bedrohungen
Maßnahmen zur IT-Sicherheit
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security
IT Security Report
Aktuelle Entwicklungen in der IT-Sicherheit



IT Security

Sicherheit am Airport Nürnberg	→ Erstellung IT-Security Policy (IT Sicherheitsleitlinie)
Prozess „IT-Sicherheit“ nach BSI	→ Benennung IT-Sicherheitsmanager
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	→ Erstellen einer vollständigen Übersicht über vorhandene IT-Systeme
Schutzbedarf / Bedrohungen	→ Entwicklung IT-Sicherheitskonzept
Maßnahmen zur IT-Sicherheit	→ Einweisung / Mitarbeiter Sensibilisierung
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	→ Durchführung von unterschiedlichen Schulungsmaßnahmen
IT Security Report	→ Umsetzung und Überwachung der IT-Sicherheitsmaßnahmen
Aktuelle Entwicklungen in der IT-Sicherheit	→ Aufrechterhalten des sicheren Betriebs
	→ Erstellung eines IT Security Management Reports

IT-Sicherheitsmanagement – Einführung und laufender Betrieb

IT Security Policy (IT Sicherheitsleitlinie)	→ Zielsetzung der IT-Sicherheitsziele, Bedeutung der Security
Rolle des IT Security Manager	<i>„Die Kernkompetenz des Konzerns besteht in der schnellen, sicheren und reibungslosen Abwicklung des Luftverkehrs am Boden. Unsere IT-Systeme und die dafür erforderlichen Schutzmaßnahmen müssen deshalb so ausgelegt sein, dass eine hohe Verfügbarkeit garantiert werden kann. Dies gilt in besonderem Maße für jene Systeme, welche die operativen Prozesse unterstützen.“</i>
Gliederung für IT-Sicherheitskonzept	
Mitarbeitereinweisung	
	→ Verantwortung aller Mitarbeiter zur Einhaltung
	→ Anforderungen an das Unternehmen (externe Anforderungen der Gesetze u. Kunden, interne Anforderungen z. B. Qualitätsaspekte)
	→ Organisationsauftrag (Benennung des IT Security Managers, Ressourcen)
	→ Festlegen der Zielgrößen
	→ Vorgaben zum Reporting

IT-Sicherheitsmanagement – Einführung und laufender Betrieb

IT Security Policy (IT Sicherheitsleitlinie)	→ „IT Security Manager etabliert, koordiniert und überwacht die IT-Sicherheit“
Rolle des IT Security Manager	→ IT-Sicherheitskonzept erstellen → Abstimmung im Unternehmen
Gliederung für IT-Sicherheitskonzept	→ Freigabe bei GF und IT-Leitung einholen → Umsetzung initiieren
Mitarbeitereinweisung	→ Umsetzung für LAN selbst vornehmen → Einhaltung überwachen
	→ Schnittstellenfunktionen einbinden (z.B. Risk-Management)
	→ Reports an GF und IT-Leitung
	→ Permanente Anpassung des Sicherheitskonzeptes → Schulung und Sensibilisierung aller Beteiligten

IT-Sicherheitsmanagement – Einführung und laufender Betrieb

IT Security Policy (IT Sicherheitsleitlinie)	<ul style="list-style-type: none"> → Management-Summary → Glossar
Rolle des IT Security Manager	<ul style="list-style-type: none"> → Szenariobeschreibung → Definition Objekte, Subjekte (Personen) und Sicherheitsziele → Festlegung des Schutzbedarfes
Gliederung für IT-Sicherheitskonzept	<ul style="list-style-type: none"> → Wert des Sicherheitsziels und Schaden bei Nichteinhaltung (monetär, Image, Qualität, Geschäftsforderung, gesetzlich) → Angriffspotential
Mitarbeitereinweisung	<ul style="list-style-type: none"> → Gefährdung, Bedrohung (Subjekt versucht unzulässiges Objekt mit best. Angriffspotential anzugreifen), Schaden → Schwachstellenanalyse der Objekte
	<ul style="list-style-type: none"> → Sicherheitsanforderungen
	<ul style="list-style-type: none"> → Auswahl von Sicherheitsmaßnahmen (Vertraglich beim Outsourcing, organisatorisch, Infrastruktur wie Türen, Verkabelung, RZ, Abstrahlschutz, Sicherheitsfunktionen bei HW und SW)
	<ul style="list-style-type: none"> → Begründung der Wirtschaftlichkeit, Praktikabilität, Angemessenheit, Akzeptanz
	<ul style="list-style-type: none"> → Bestimmung und weitere Behandlung des Restrisikos (bestimmen, akzeptieren, versichern, weiter reduzieren) → Verweise auf weitere Dokumente → Organisationsstruktur

IT-Sicherheitsmanagement – Einführung und laufender Betrieb

IT Security Policy (IT Sicherheitsleitlinie)	<ul style="list-style-type: none"> → Verhalten am Arbeitsplatz → Informationen bei Einstellung neuer Mitarbeiter → Vereinbarungen mit Externen → Regelungen für IT-Mitarbeiter (in- und extern) → Checklisten (z. B. für Backup, Archiv, Operating)
Rolle des IT Security Manager	
Gliederung für IT-Sicherheitskonzept	
Mitarbeitereinweisung	

IT Security

Sicherheit am Airport Nürnberg	<ul style="list-style-type: none">→ Schutzbedarf→ Potentielle Bedrohungen durch→ Gefahrenbereich
Prozess „IT-Sicherheit“ nach BSI	
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	
Schutzbedarf / Bedrohungen	
Maßnahmen zur IT-Sicherheit	
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	
IT Security Report	
Aktuelle Entwicklungen in der IT-Sicherheit	

Schutzbedarf / Bedrohungen

Schutzbedarf	<p>→ Daten</p> <ul style="list-style-type: none"> • unbefugte Kenntnisnahme (Verlust der Vertraulichkeit) • unbefugte Änderung (Verlust der Integrität) • Vorenthaltung (Unbefugte Vorenthaltung, technischer Defekt) • Missbrauch <p>→ Personen</p> <ul style="list-style-type: none"> • Verlust der Anonymität (Spionage, Internet-Überwachung..) • Unberechtigte Zuordnung (z.B. Zusendung von Pornowerbung..) <p>→ Geräten</p> <ul style="list-style-type: none"> • Entwendung • Manipulation • Zerstörung
Potentielle Bedrohungen durch	
Gefahrenbereich	

Schutzbedarf / Bedrohungen

Schutzbedarf	→ Hacker
Potentielle Bedrohungen durch	→ Autorisierte Mitarbeiter / Nutzer
Gefahrenbereich	→ Nicht autorisierte Mitarbeiter / Nutzer
	→ Ehemalige Mitarbeiter
	→ Kunden
	→ Wettbewerber
	→ Lieferanten
	→ Politisch Motivierte
	→ + höhere Gewalt

Schutzbedarf / Bedrohungen

Schutzbedarf	<ul style="list-style-type: none"> → Malware (Viren, Würmer, Trojanische Pferde,..) → Irrtum und Nachlässigkeit eigener Mitarbeiter
Potentielle Bedrohungen durch	<ul style="list-style-type: none"> → Software-Mängel/-Defekte → Hardware-Mängel/-Defekte
Gefahrenbereich	<ul style="list-style-type: none"> → Mängel der Dokumentation → Unbeabsichtigte Fehler von Externen
	<ul style="list-style-type: none"> → Hacking (Vandalismus, Missbrauch, ...)
	<ul style="list-style-type: none"> → Unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage
	<ul style="list-style-type: none"> → Höhere Gewalt (Feuer, Wasser,)
	<ul style="list-style-type: none"> → Manipulation zum Zweck der Bereicherung → Sabotage
	<ul style="list-style-type: none"> → Sonstiges

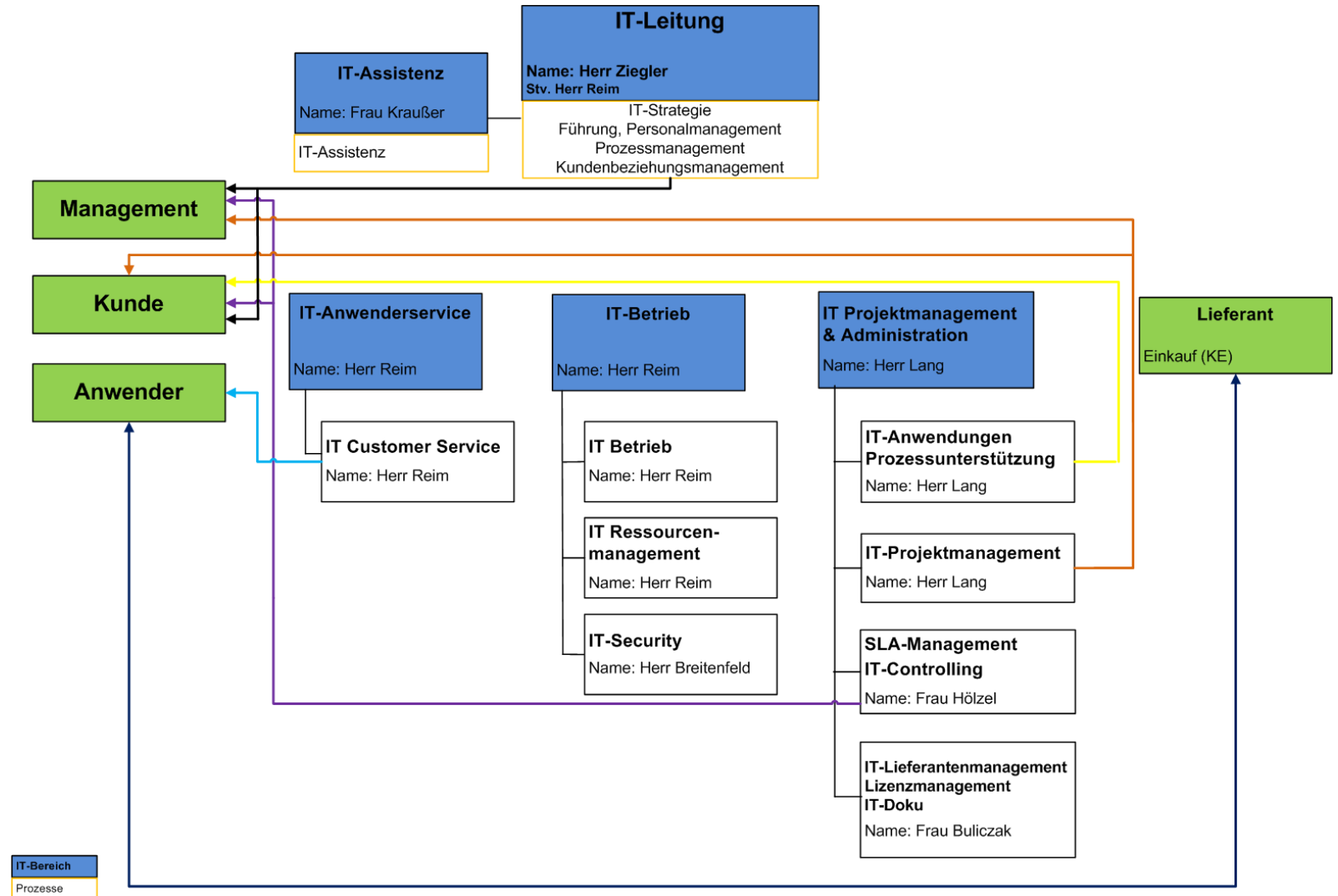
IT Security

Sicherheit am Airport Nürnberg	<ul style="list-style-type: none"> → Physikalischer Zugangsschutz (z.B. Rechnerraum) → Schreibschutz / Zugriffsschutz / Passwörter → Betriebskonzepte / Redundanz von Systemen und Schnittstellen → Service Level Agreements → IT-Prozessmanagement (z.B. IT-Betrieb, Projekte..) → Eskalationsprozesse → Firewall (Dienstefilter) → Gateway Security (Viren, Spam, Url-Filter) → Betriebssystemsisicherheit (Patch.-M., Client-Virenschutz) → VPN (Tunneling)
Prozess „IT-Sicherheit“ nach BSI	
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	
Schutzbedarf / Bedrohungen	
Maßnahmen zur IT-Sicherheit	
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	
IT Security Report	
Aktuelle Entwicklungen in der IT-Sicherheit	

IT Security

Sicherheit am Airport Nürnberg	<ul style="list-style-type: none"> → IT-Prozesslandkarte → Einsatz Systemmanagement → IT-Toolübersicht → IT-Tool-Integration → Availability-Management- Verfügbarkeitsauswertung → IT-ServiceCenter Tool – Abbildung wichtiger ITIL Service Delivery Prozesse
Prozess „IT-Sicherheit“ nach BSI	
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	
Schutzbedarf / Bedrohungen	
Maßnahmen zur IT-Sicherheit	
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	
IT Security Report	
Aktuelle Entwicklungen in der IT-Sicherheit	

IT-Centerbereichs-/Prozessmatrix Airport Nürnberg



Maßnahmen zur IT-Sicherheit

Einsatz Systemmanagement

IT- Toolübersicht

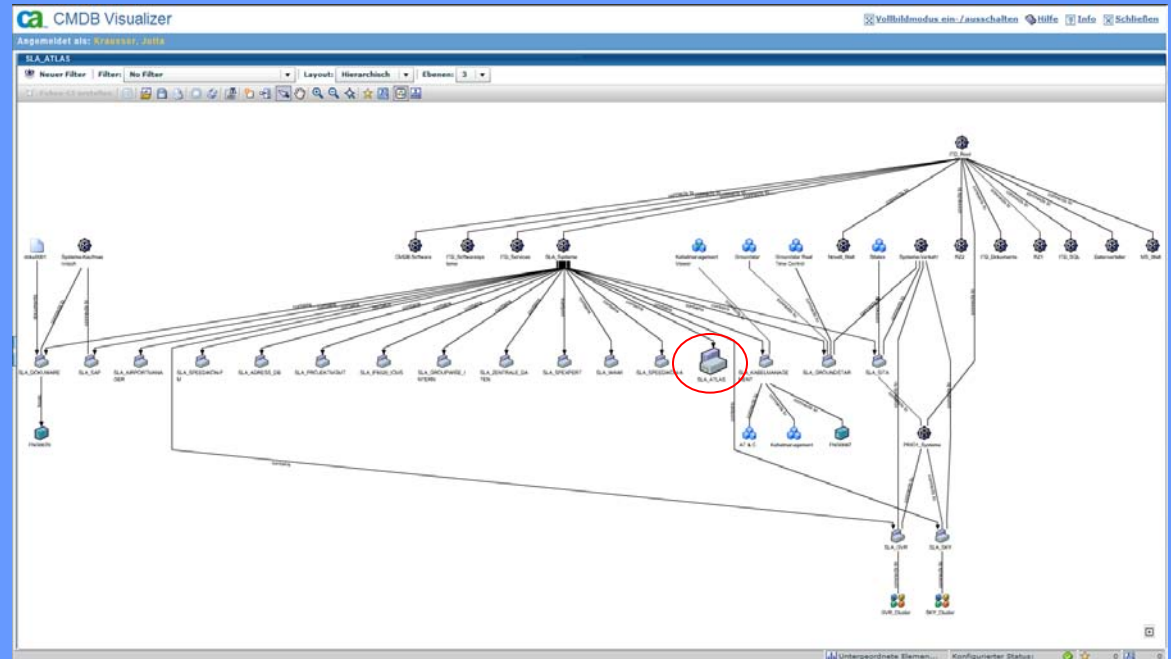
IT Tool Integration

Qualitätsvereinbarung

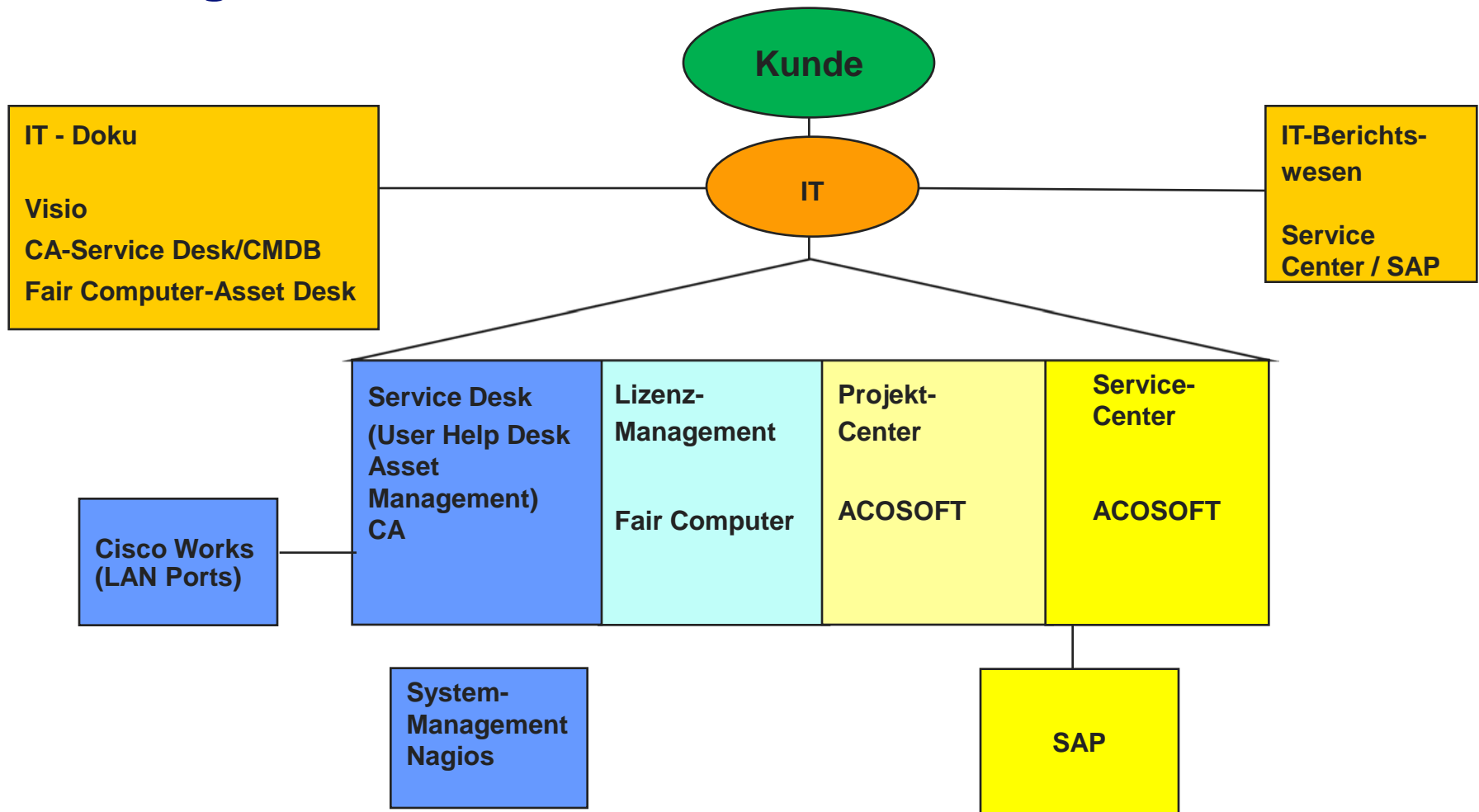
Availability Management – Verfügbarkeitsauswertung

IT-ServiceCenter Tool – Abdeckung wichtiger ITIL Service Delivery Prozesse

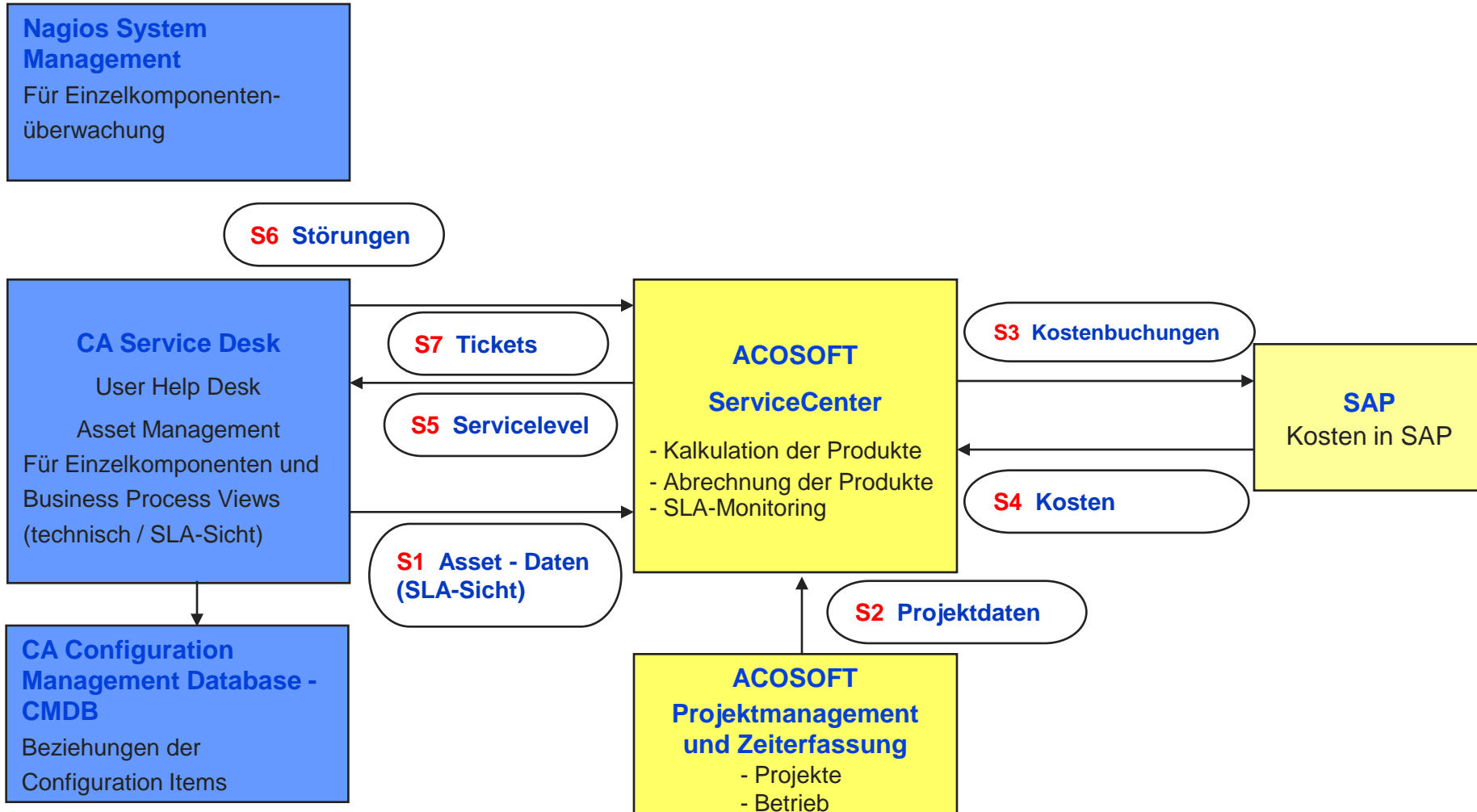
➔ Business Process View am Beispiel Frachtsystem



IT Management Tools - Übersicht



IT Management Tools - Schnittstellen



Qualitätsvereinbarung

- Zielvereinbarungen für LAN und Server (z.B.99,5% Verfügbarkeit)

- Vertragsvereinbarung zu qualitätsfördernden Maßnahmen bei Minderleistung (99,5 % - 99,0 % Verfügbarkeit → 5 %, < 99,0 % Verfügbarkeit → 10 %)

- Aufzeichnung der Supportqualität (Reaktionszeit, Bearbeitungsdauer, Qualität, Verhalten)

- Aufzeichnung der Projekt- und Auftragsqualität (fachl./techn. Ausführung, Dauer, Kosten)

- Auswertung der Qualitätskennzahlen und Analyse/Optimierung zusammen mit Kunden

- Unterschiedliche Supportstufen auf Wunsch des Kunden anbieten (derzeit Support Level Advanced = Reaktionszeit max. 2 Stunden)

- EDV-Rufbereitschaft mit Reaktionszeit max. 2 Stunden für definierte Prio 1 Systeme als Ziel

- Beratung des Kunden zu neuen Technologien

IT Security

Sicherheit am Airport Nürnberg	Kapitel: <ul style="list-style-type: none">→ Einleitung→ Serverräume→ Datenträgerarchiv→ Räume für technische Infrastruktur→ Microsoft Patchmanagement→ Netware Patchmanagement→ Unix/Linux Patchmanagement→ Mailfilter→ Firewall→ Virenschutz→ Datensicherung→ Systemmanagementsystem→ Netzwerkinfrastruktur
Prozess „IT-Sicherheit“ nach BSI	
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	
Schutzbedarf / Bedrohungen	
Maßnahmen zur IT-Sicherheit	
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	
IT Security Report	
Aktuelle Entwicklungen in der IT-Sicherheit	

IT Security

Sicherheit am Airport Nürnberg	<ul style="list-style-type: none"> ➔ Verstärkung von Wirtschaftsspionage ➔ Zielgruppen sind neben Wirtschaft, Forschung und Verwaltung immer mehr auch private Anwender ➔ Vermehrtes Ausspähen von Kreditkarteninformationen und Finanzdaten ➔ Social Engineering nutzt „die Schwachstelle Mensch“ aus ➔ Trend vom „sportlichen Ehrgeiz“ zur Professionalisierung und Kommerzialisierung der Internetkriminalität
Prozess „IT-Sicherheit“ nach BSI	
IT-Sicherheitsmanagement-Einführung und laufender Betrieb	
Schutzbedarf / Bedrohungen	
Maßnahmen zur IT-Sicherheit	
Ganzheitliche Prozess- und Toolintegration als Basis für IT-Security	
IT Security Report	
Aktuelle Entwicklungen in der IT-Sicherheit	

Zusammenfassung

- IT Security ist Teil der Gesamtsicherheit am Airport
- Prozess IT Security Management ist eingeführt und die Rolle des IT Security Managers ist besetzt
- Gefahrenbereiche für IT nehmen weiter zu
- Abteilung Informationstechnologie (KI) trifft permanent entsprechende Maßnahmen zur Gefahrenreduzierung
- Report zu IT Security ist erstellt, erfolgt jedes Quartal
- Sensibilisierung aller Mitarbeiter zum Thema IT-Sicherheit ist wichtige Aufgabe
- Ganzheitliche Prozessabbildung mit starker ITIL-Ausrichtung
- Integrierter Tooleinsatz zur Überwachung und Steuerung aller IT-Produkte in technischer, organisatorischer und kaufmännischer Hinsicht
- Umfangreiche Abdeckung von ITIL Service Delivery durch das Tool ServiceCenter
- Alle Mitarbeiter tragen Mitverantwortung für IT-Sicherheit