Joint Security Management:
Ein organisationsübergreifendes Konzept für Anwender und Anbieter

Dr. Eberhard von Faber ▪ GI Fachgruppe SECMGT ▪ 13.04.2018

T · · Systems ·

Die Kette ist nur so stark, wie ihr schwächstes Glied.

3. Arbeitsteilung in der IT-Industrie

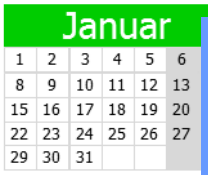
4. Flexibilität: Katalog-Bausteine

unterschiedliche Hersteller (Quellen)

Austausch und Neukombination

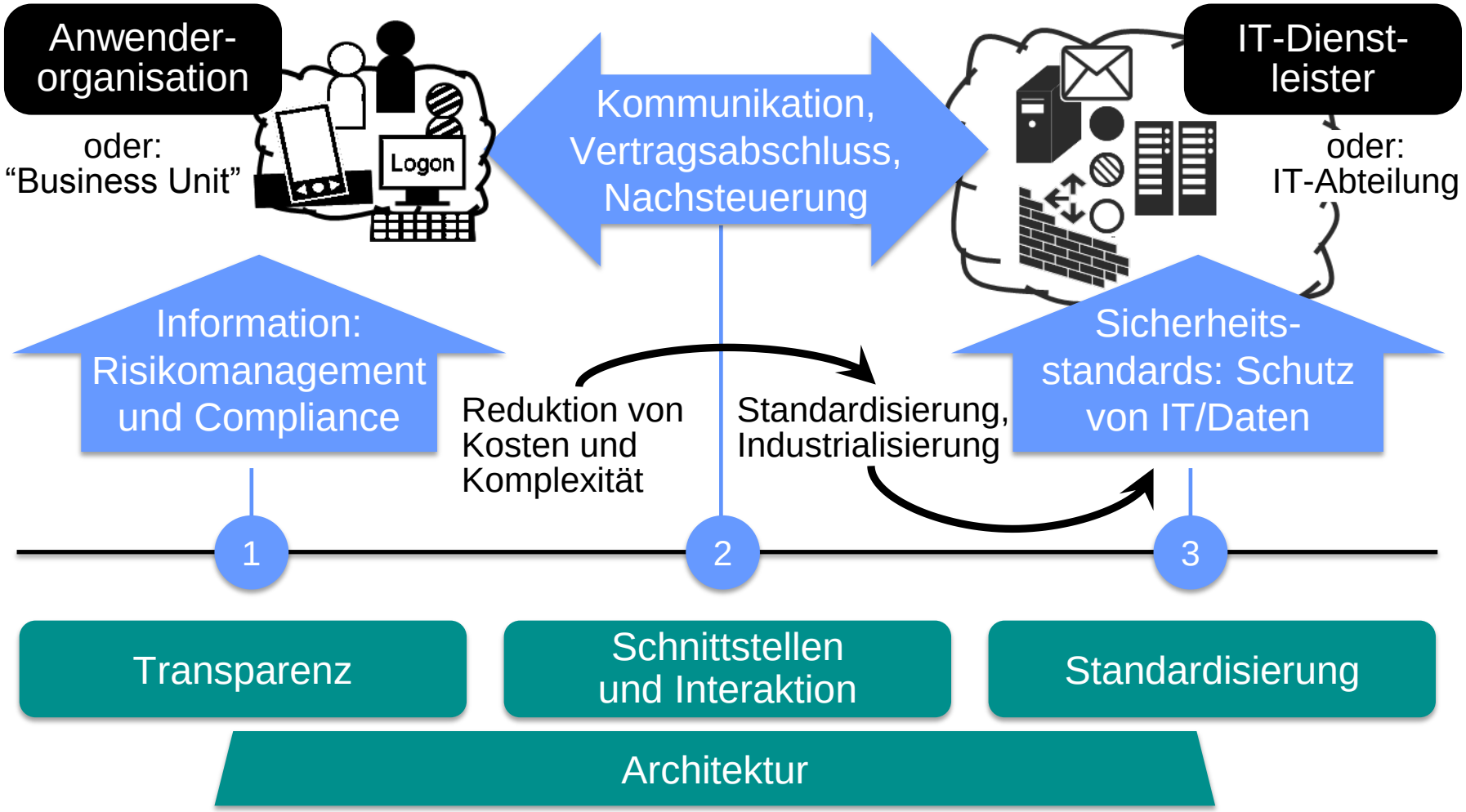
mehrseitige Beanspruchung

1. organisationsübergreifend: Anwender u. Dienstleister

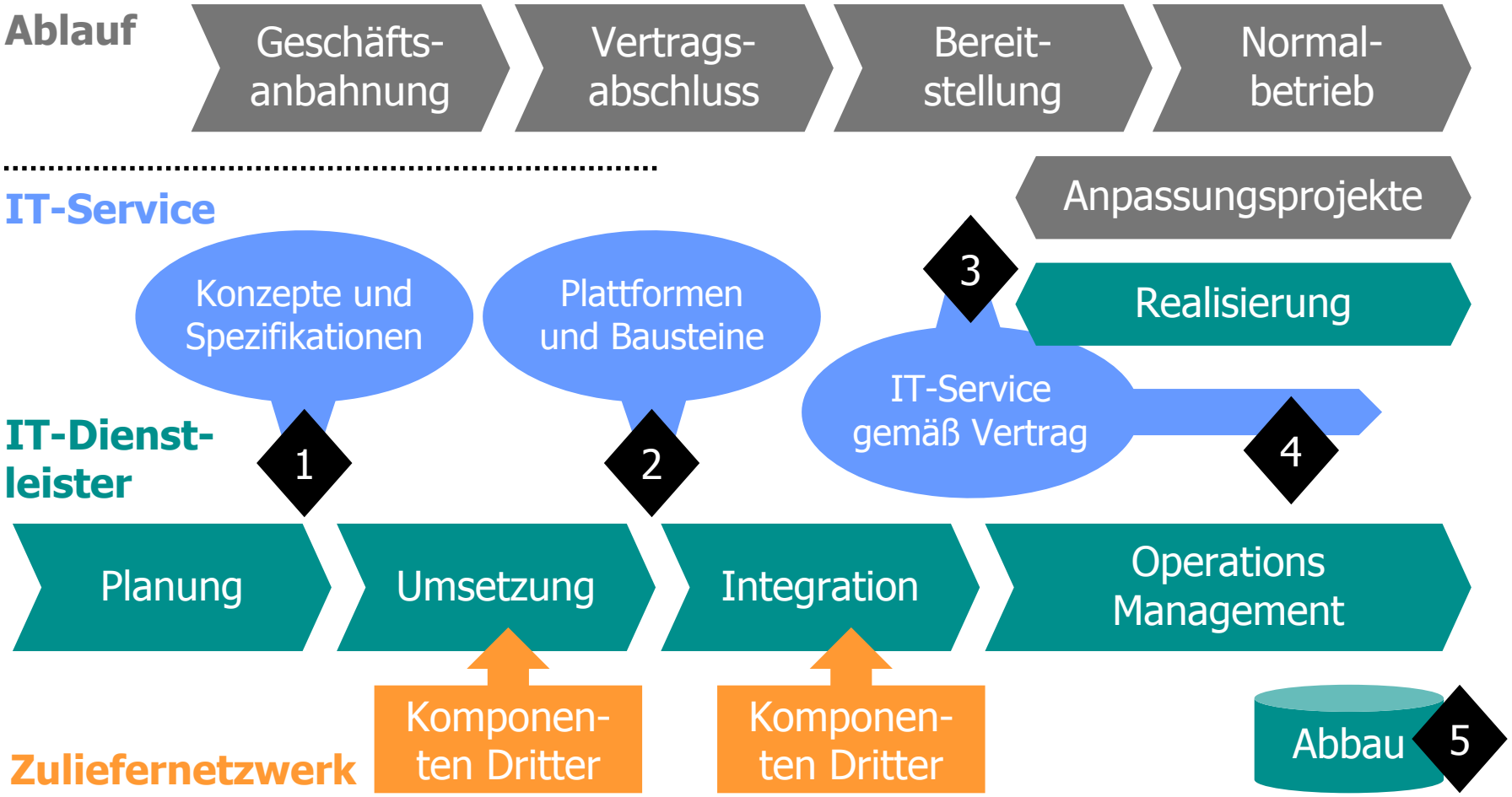


2. Geschäftsablauf und Markt

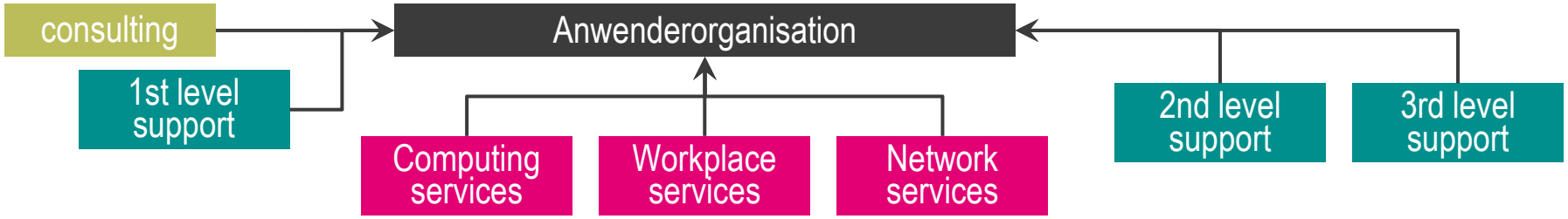
1. Organisationsübergreifend handeln: Das ESARIS-Steuerungsmodell.



2. Ablauf der Geschäftsbeziehung und Lebenszyklus der IT-Services.



3. Arbeitsteilung in der IT-Industrie.
Services und Komponenten.



Primary management services

Service management services (active)	Service monitoring services	Service continuity	Diagnostics and repair	Incident response

Additional services

Broker, reseller	Systems integration	Application management	Archiving and content management	Vulnerability services	Threat intelligence, incident response

Computing components

Application software	Operating systems	Virtualization (computing)	Storage systems	DC and DC infrastructure	Management systems

Workplace components

Workplace computer	Mobile devices

Network components

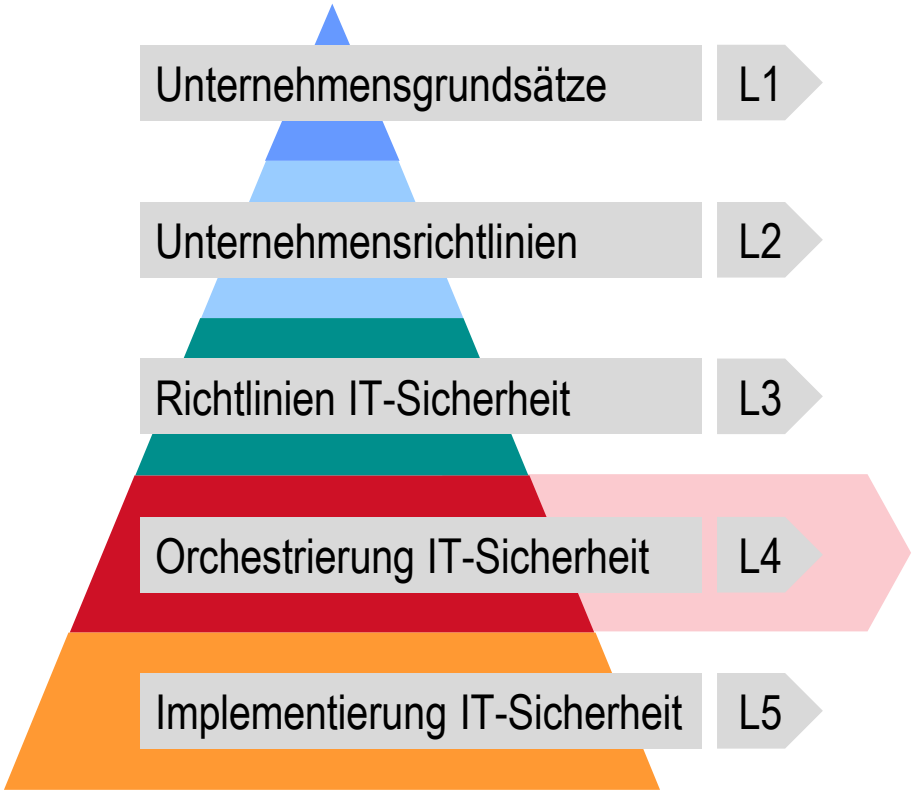
Gateways	Router, switches etc.	Firewalls, IDS/IPS etc.	Proxy, load balancer etc.	Network services

General components

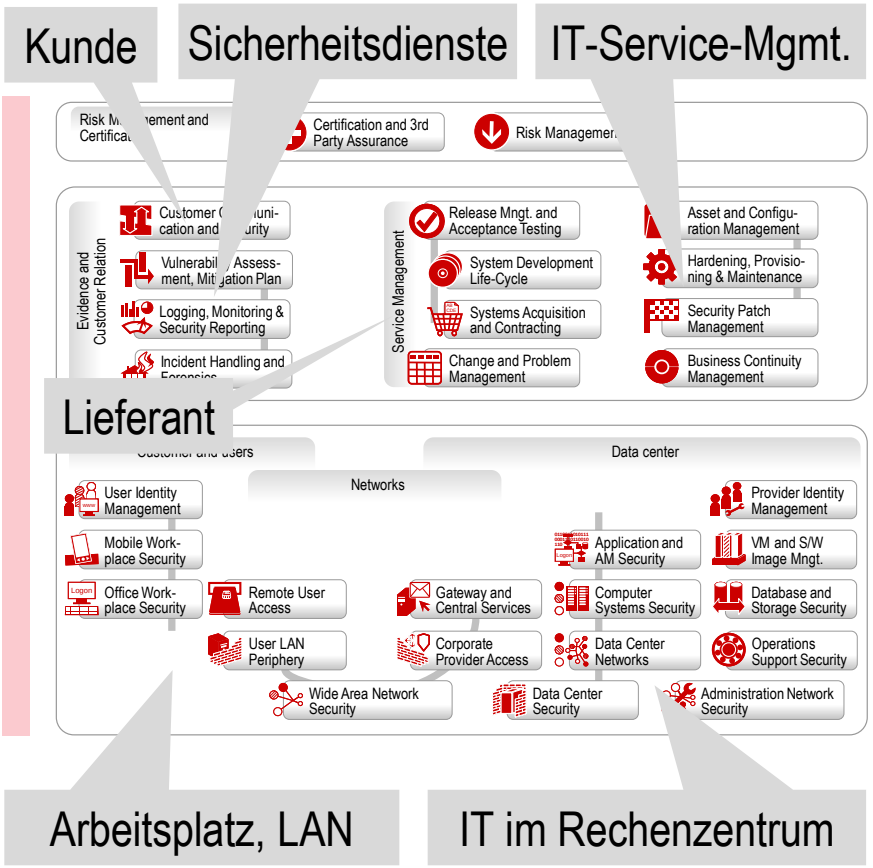
Middle-ware	Databases, directories	Server hardware	Encryption software etc.	Authenti-cation	Identity management	Key manage-ment

3. Arbeitsteilung, Architektur: Dokumentation gliedern, Sicherheit in Kerngeschäft integrieren.

schrittweise Verfeinerung



Aufteilung gemäß Organisation der IT-Produktion



4. Flexibilität: Katalog-Bausteine (links) und Sicherheitsstandards (rechts).

Servicekatalog → ← **Security**

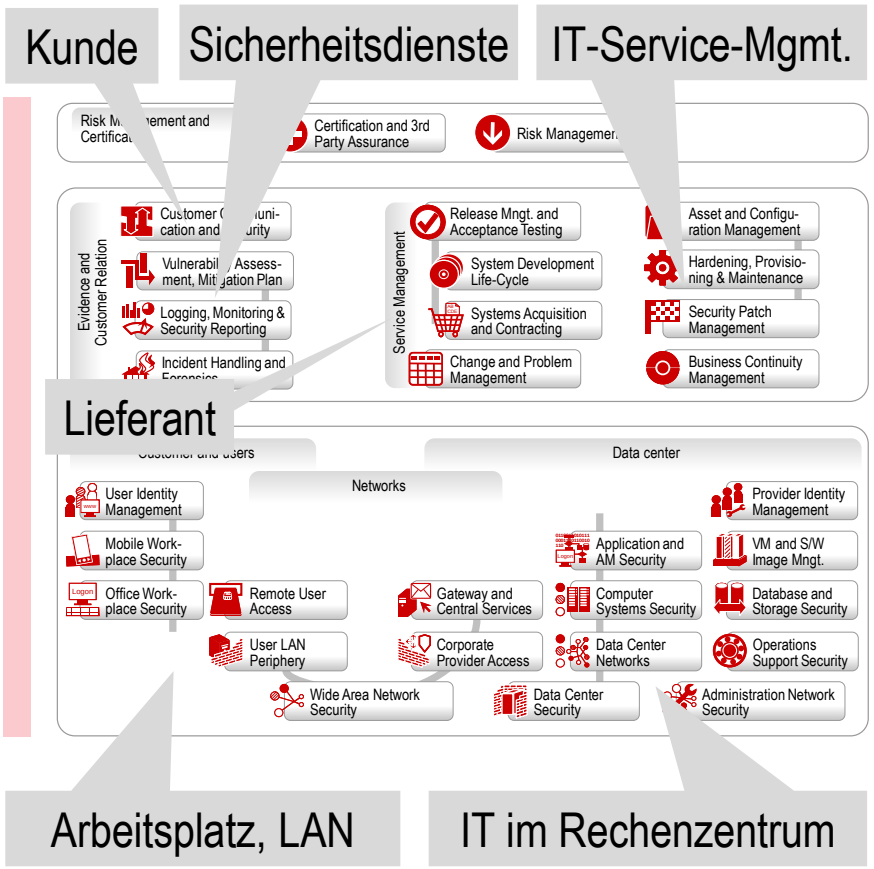
Management Services
- Bronze
- Silver
- Gold

Connection Services
- DNL
- IPSEC
- MPLS

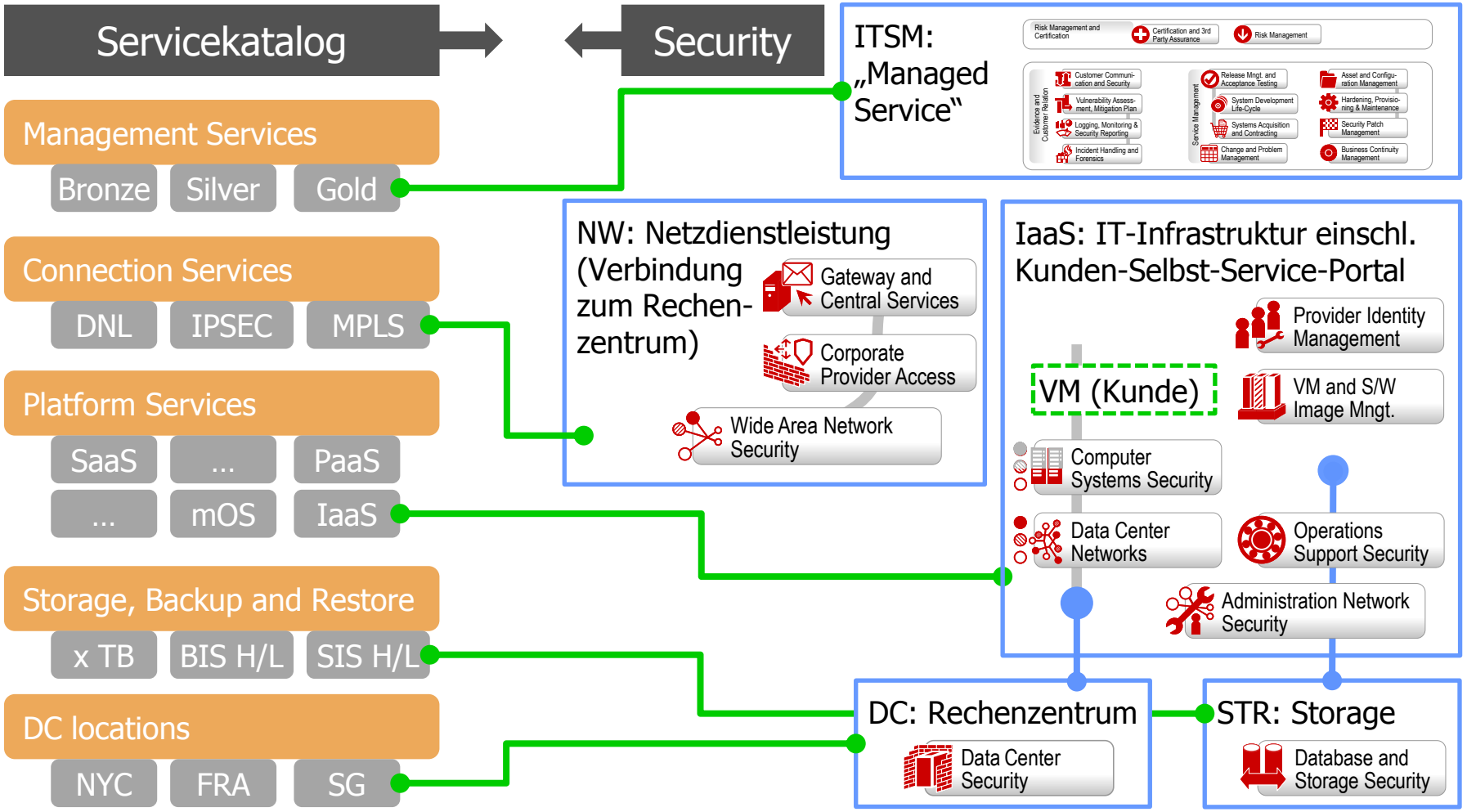
Platform Services
- SaaS
- ...
- PaaS
- ...
- mOS
- IaaS

Storage, Backup and Restore
- x TB
- BIS H/L
- SIS H/L

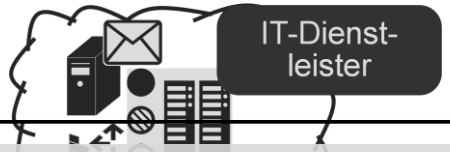
DC locations
- NYC
- FRA
- SG



4. Flexibilität: Katalog-Bausteine (links) und Sicherheitsstandards (rechts).



Joint Security Management (JSM)



- Sicherheit in alle Kernprozesse integrieren
- Industrielle Arbeitsteilung berücksichtigen
- Sicherheitsmanagement auf IT-Services und Kunden ausrichten

[sondieren]		[anbieten]
▪ Bedarf definieren (Strategie, Anforderungen) ▪ Beschaffung vorbereiten (Marktsondierung, Planung		▪ Service- und Security-Spezifikation für Kunden bereithalten ▪ Marketing, Vertrieb und Deal-Management ausrichten
▪ Beschaffen (verhandeln, Vertrag abschließen)	[entscheiden]	▪ Verkaufen (verhandeln, Vertrag abschließen)
▪ Vertragsbeendigung vertraglich fixieren	[migrieren]	▪ Migration durchführen (gemäß Plan und vertrag)
▪ Anforderungen und Richtlinien definieren ▪ Sicherheitsorganisation/–prozesse pflegen; Ressourcen anpassen ▪ IT-Dienste sicher integrieren und nutzen	[schützen]	▪ Sicherheitsstandards nach Marktanforderungen ▪ Für Umsetzung sorgen und kontrollieren ▪ Sicherheitsorganisation/–prozesse pflegen; Ressourcen anpassen
▪ Sicherheitsberichte analysieren und nutzen ▪ Audits und Tests gemäß Vertrag durchführen ▪ Risiken bewerten und behandeln	[erkennen]	▪ Transparenz schaffen bzgl. der IT-Sicherheit ▪ Sicherheitsberichte gemäß Vertrag liefern ▪ Audits und sonstige Tests gemäß Vertrag unterstützen
▪ Schnittstellen pflegen und den Betrieb unterstützen (falls nötig) ▪ Bei Sicherheitsvorfällen aktiv werden ▪ Die Erfüllung des Vertrages durchsetzen	[nachsteuern]	▪ Schnittstellen im Service Delivery Management für Kunden anbieten und mit den notwendigen ITSM-Prozessen verbinden ▪ Mitwirkung des Kunden einfordern
▪ Anforderungen an den IT-Dienstleister prüfen und aktualisieren ▪ Die Arbeitsteilung überprüfen und optimieren ▪ Vertrag überprüfen und anpassen	[verständigen]	▪ Sicherheit bei Zulieferern und Zulieferleistungen ▪ Kunden über Weiterentwicklungen informieren ▪ Verträge und Vereinbarungen verhandeln und ändern (falls nötig)
▪ Verbesserungen und Innovationen initiieren ▪ Projekte aufsetzen und unterstützen ▪ Knowhow auf dem aktuellen Stand halten	[verbessern]	▪ Standardisieren; Kosten; Qualität ▪ Verbesserungen und Innovationen implementieren ▪ Den Kunden in solche Projekte ggf. einbeziehen

wozu?

- Datenschutz
- Compliance
- Vertrauen (Wirtschaft)
- Widerstandsfähigkeit (Wirtschaft)

wo?

Beispielunternehmen
- Umsatz: 10 Mrd. €

Branchendurchschnitt
- IT-Kosten: 350 Mio. €/Jahr
- IT-Sicherheit: ≈ 26 Mio. €/J

T · · Systems ·

[nachsteuern] Interaktion ermöglichen und unterstützen.

Anwenderorganisation:

Unterstützen und Mitwirken [nachsteuern]

- Schnittstellen pflegen und den Betrieb unterstützen (falls nötig)
- Im Falle von Sicherheitsvorfällen aktiv werden
- Die Erfüllung des Vertrages durchsetzen

IT-Dienstleister:

- Schnittstellen im Service Delivery Management für Kunden anbieten und mit den notwendigen ITSM-Prozessen verbinden
- Mitwirkung des Kunden einfordern

Interaktion ermöglichen [nachsteuern]

IT und IT-Sicherheit bleiben nicht stehen. Obwohl die Durchführung der Änderungen dem IT-Dienstleister obliegt, ist bei vielen Änderungen die Mitwirkung der Anwenderorganisation angezeigt. Größere Änderungen werden häufig von der Anwenderorganisation angestoßen.

Damit beide Partner interagieren können, ist es nicht ausreichend, Rollen zu definieren und Personen zu benennen. Sie müssen in die prozessualen Abläufe integriert werden. Das genaue Verständnis der Aufgaben und Schnittstellen ist die Grundlage dafür.

[nachsteuern] Aufgaben und Rollen im Normalbetrieb.

Anwender-organisation

Aufgaben und Schnittstellen im Normalbetrieb

IT-Dienst-leister

1. Governance: Rollen, Ressourcen, Prozesse

11. Security-Officer

2. Risikomanagement, Lagebild, Compliance

3. Nutzung Security-Reports, Audits etc.

12. Customer Security Manager

4. Maintenance, Change-Advisory

13. Service-Delivery-Management

6. Vorfall- und Notfall-Management

5. Help-Desk- und Vorfallmeldung

14. Help-Desk, Vorfallmngt.

7. sichere Integration

8. Anforderungs-management

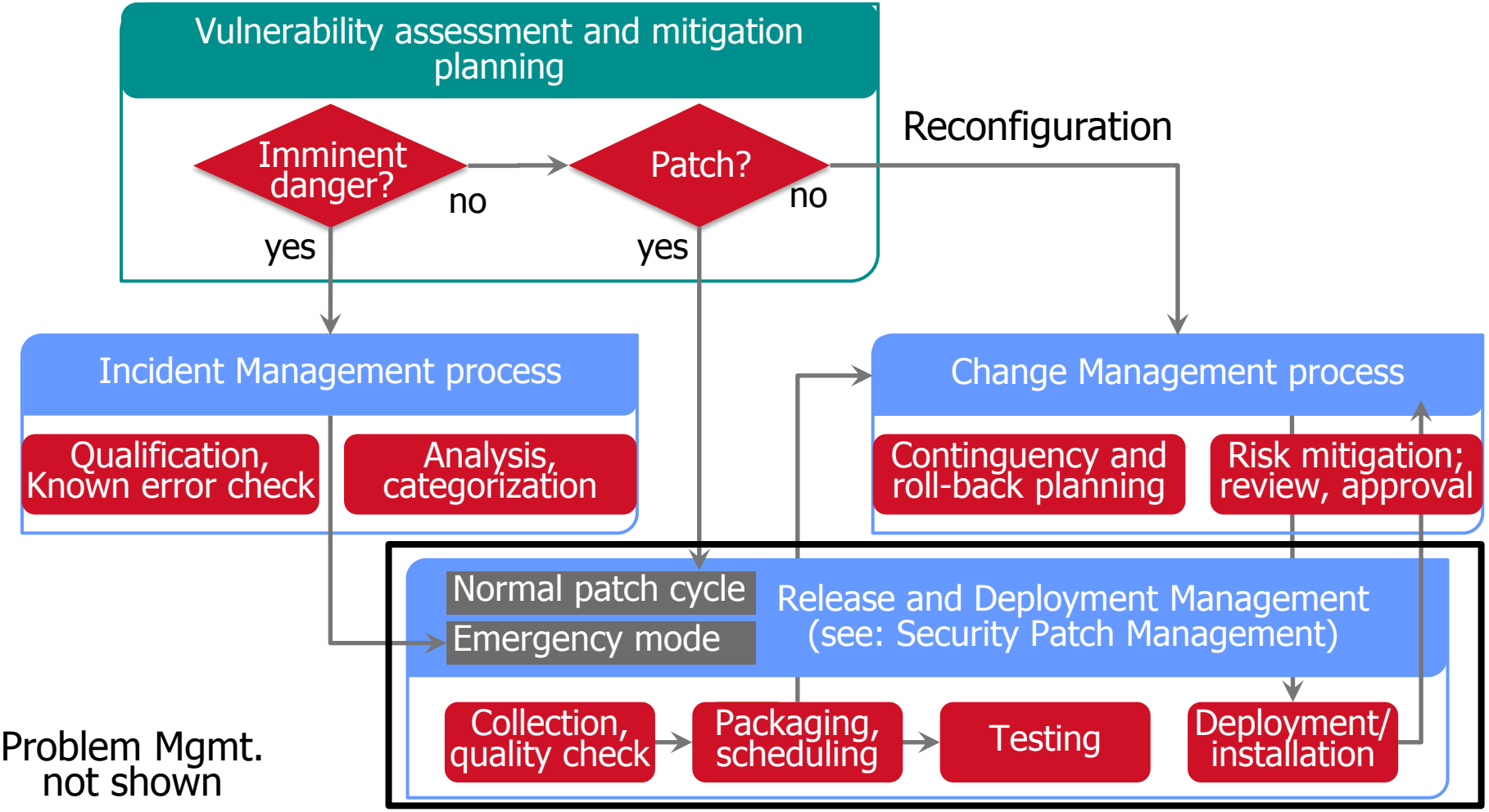
15. Account-/Service-Delivery-Manager

10. Service-Orchestrierung Vertragsmanagement

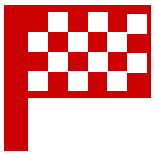
9. Projekt-Management

16. Service-Delivery-Management, Projects

Von der Schwachstellenerkennung bis zur Beseitigung...



Softwareaktualisierung (Patch Management, SPM).



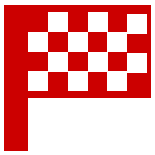
Herausforderungen („Was muss erreicht werden?"):

- Verringerung der Wahrscheinlichkeit, dass Schwachstellen ausgenutzt werden, durch „unverzügliche" Anwendung von Patches oder durch Implementierung anderer Maßnahmen,
- Integration der Softwareaktualisierung in die Standardproduktionsprozesse (z.B. Verbindung mit dem „Change-Management"-Prozess, bei dem, falls nötig, auch der Kunde einbezogen wird),
- Minimierung der Down-Time und des Aufwandes,
- Verifikation des Erfolgs und Weiterverfolgung (tracking) von Reparaturen, die aus bestimmten Gründen nicht oder nicht in der geplanten Zeit durchgeführt werden konnten.

Maßnahmen („Was muss getan werden?"):

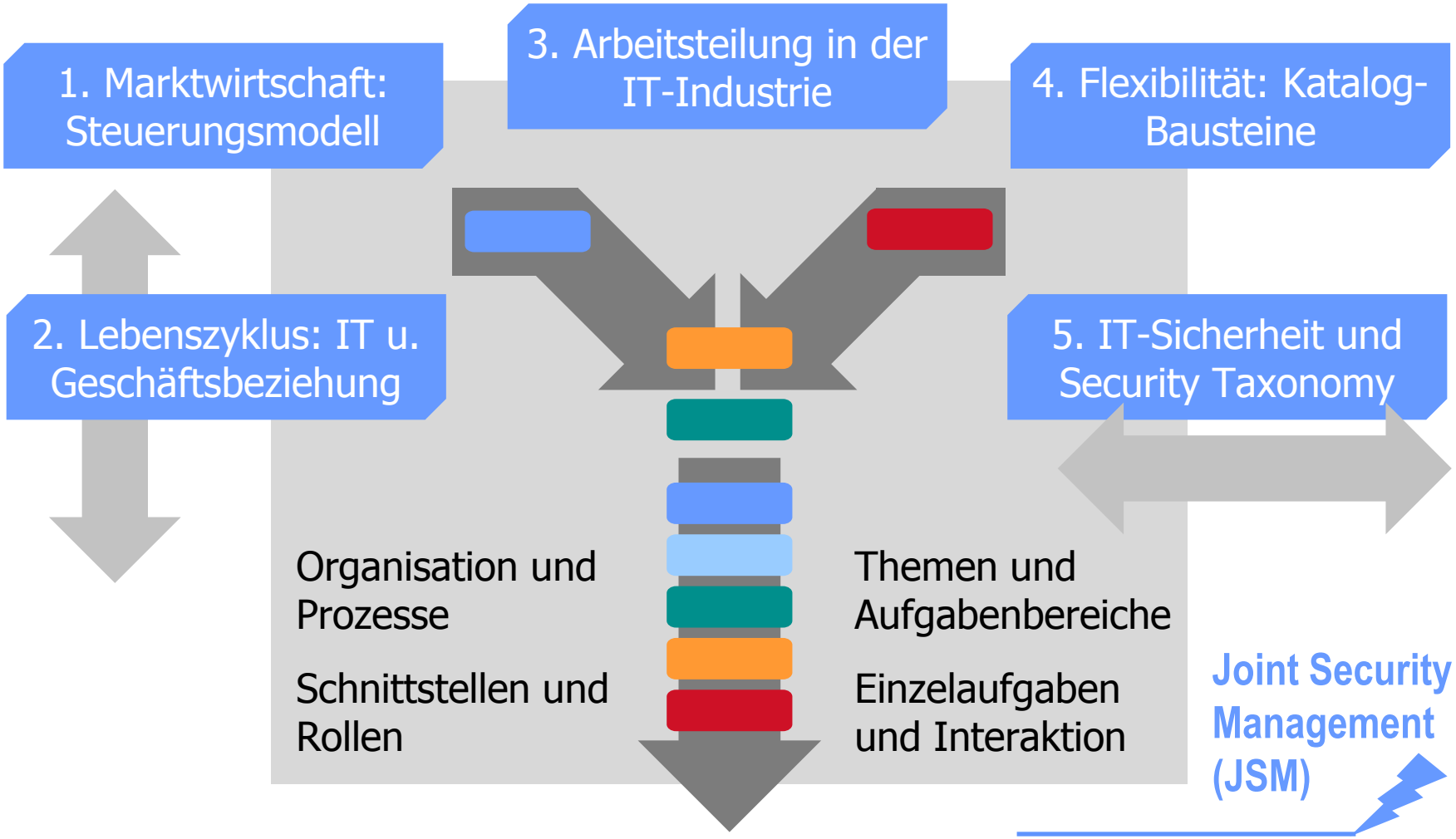
- Integration in die Standardproduktionsprozesse: Nutzung des Change-Managements zur Steuerung der Installation von Patches und anderer Reparaturmaßnahmen; Trigger erfolgt nur durch einen Change-Request; ggf. Unterstützung bei der Planung (weil Patches paketiert und in einer bestimmten Reihenfolge implementiert werden müssen),

Softwareaktualisierung (Patch Management, SPM).



- Einhaltung der Zeiten (Perioden), wie im Schwachstellenmanagement festgelegt,
- Identifikation der Patches (und Workarounds); Test und Freigabe,
- Backup und Möglichkeit eines Roll-back,
- Nutzung eines Inventars und eines Speichers für Patches,
- Führen eines Patch-Registers; Aktualisierung der CMDB,
- Zusammenarbeit mit dem Service-Delivery-Management, z.B. um die Anwenderorganisation über mögliche Down-Times zu informieren bzw. diese mit ihr abzustimmen,
- Möglichkeit für Emergency-Patches (und Workarounds) mit modifiziertem Change-Management und möglicherweise unter Umgehung des Change Advisory Boards und des Service-Delivery-Managements,
- Nutzung einer technischen Infrastruktur für die teilautomatische Anwendung von Patches (wie z.B. die Nutzung der Windows Server Update Services (WSUS), entsprechendes für andere Komponenten bzw. Software-Typen wie Firmware).
- (Ende)

JSM auf einer Seite...



Joint Security Management (JSM).

- *Arbeitsteilung und Industrialisierung der IT:* Auswirkungen auf das Sicherheitsmanagement
- *Flexibilität:* Katalog-Bausteine und Sicherheitsstandards
- *Steuerungsmodell:* Sicherheit in Lieferketten und Lebenszyklen
- *Ablauf:* Geschäftsbeziehung und Lebenszyklus der IT-Services
- *Joint Security Management:* Aufgabenteilung für beide Partner und Zusammenarbeit

Joint Security Management: organisationsübergreifend handeln

Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion

ISBN 978-3-658-20833-2 (Hardcover) + eBook

Neuerscheinung 2018; schreiben Sie an ESARIS@t-online.de