Joint Security Management: wie Anwenderunternehmen und Anbieter im Cloudzeitalter adäquat zusammenwirken

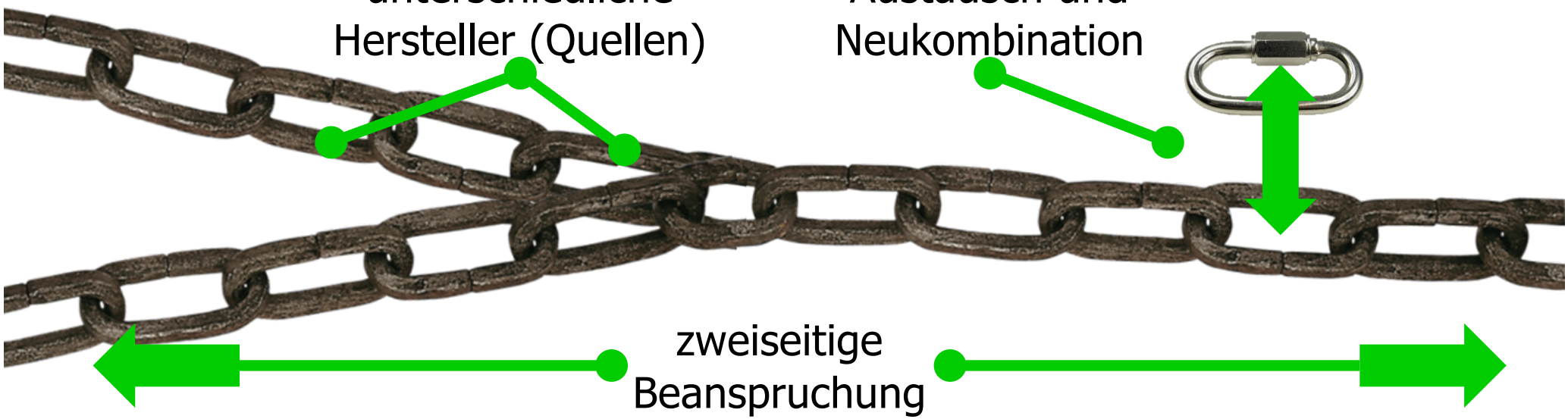
Prof. Dr. Eberhard von Faber ▪ Security Forum ▪ 18.01.2018

T · · Systems ·

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

1. Arbeitsteilung in der IT-Industrie

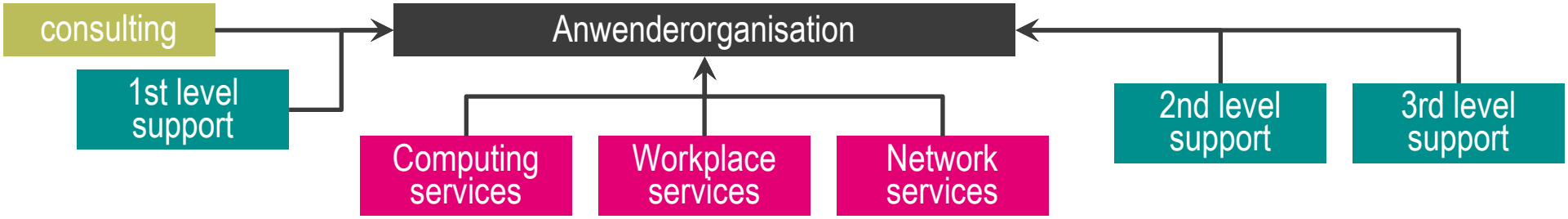
2. Flexibilität: Katalog-Bausteine



3. organisationsübergreifend: Anwender u. Dienstleister

4. Geschäftsablauf und Markt

1. 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

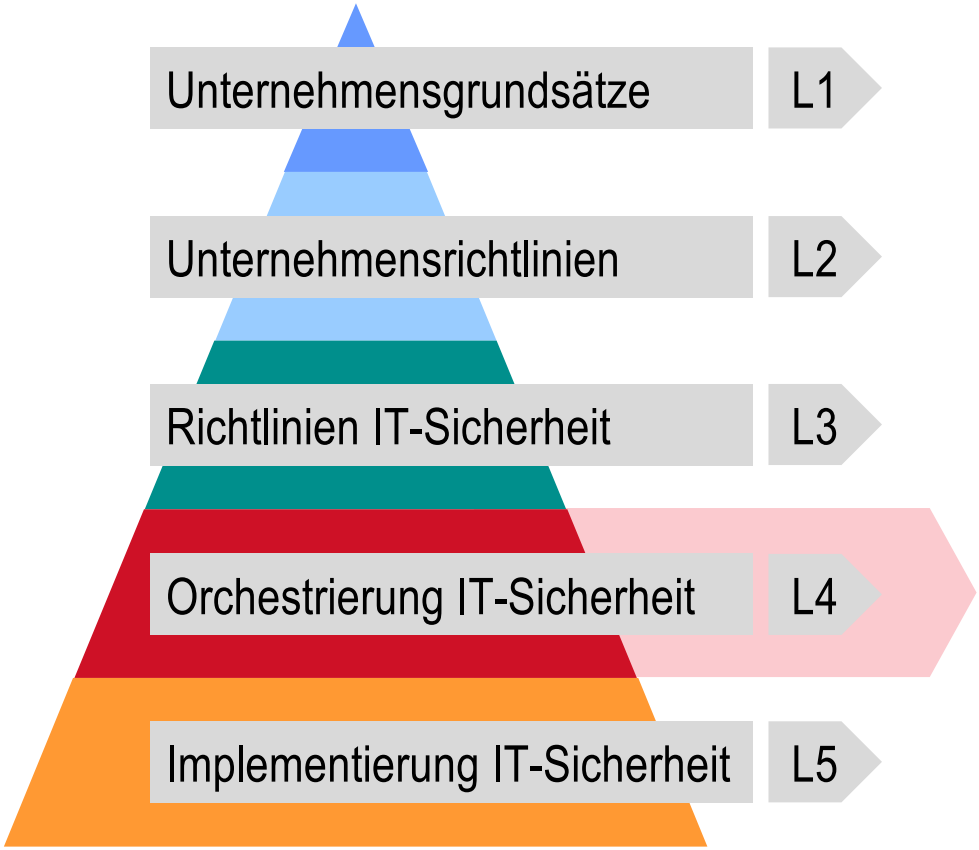
Gateways | Router, switches etc. | Firewalls, IDS/IPS etc. | Proxy, load balancer etc. | Network services

General components

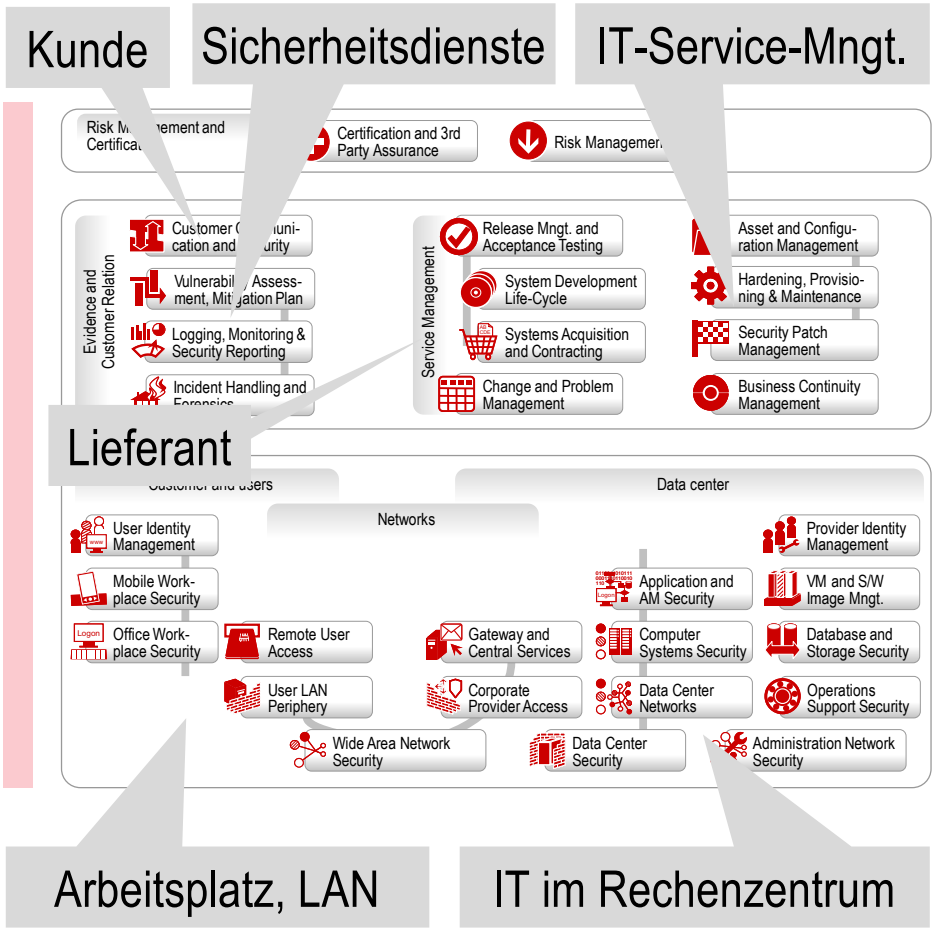
Middle-ware | Databases, directories | Server hardware | Encryption software etc. | Authenti-cation | Identity management | Key manage-ment

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

schrittweise Verfeinerung



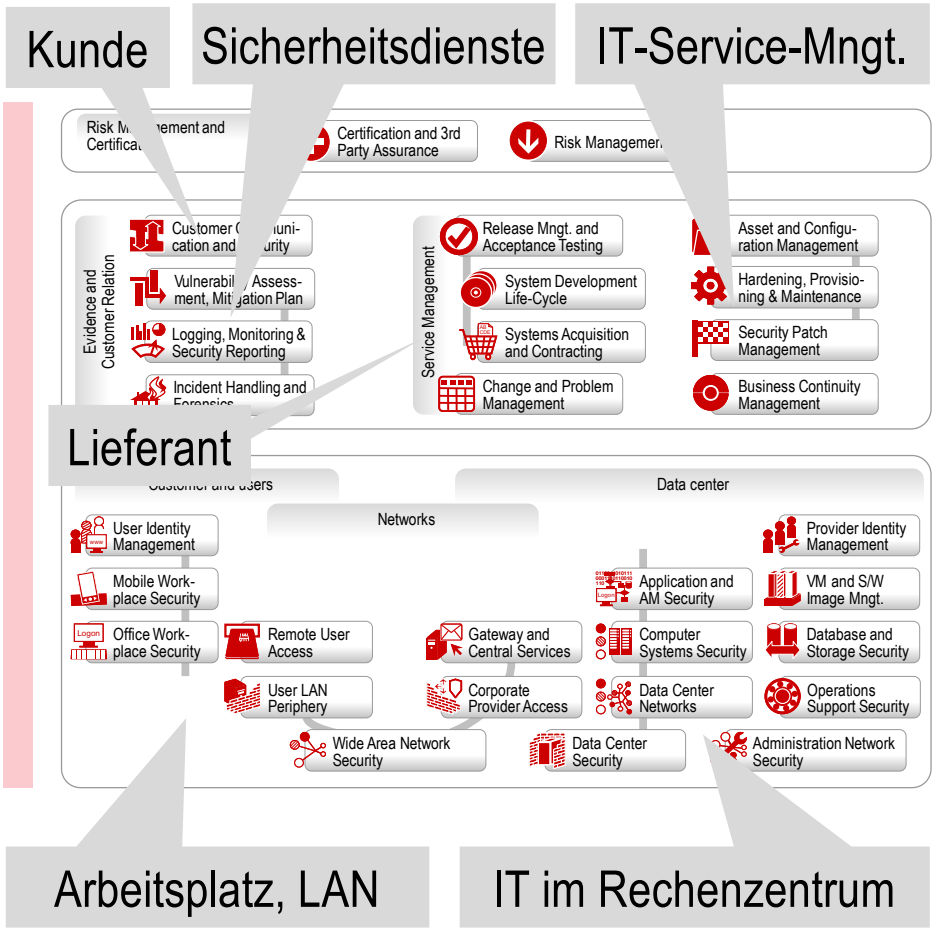
Aufteilung gemäß Organisation der IT-Produktion



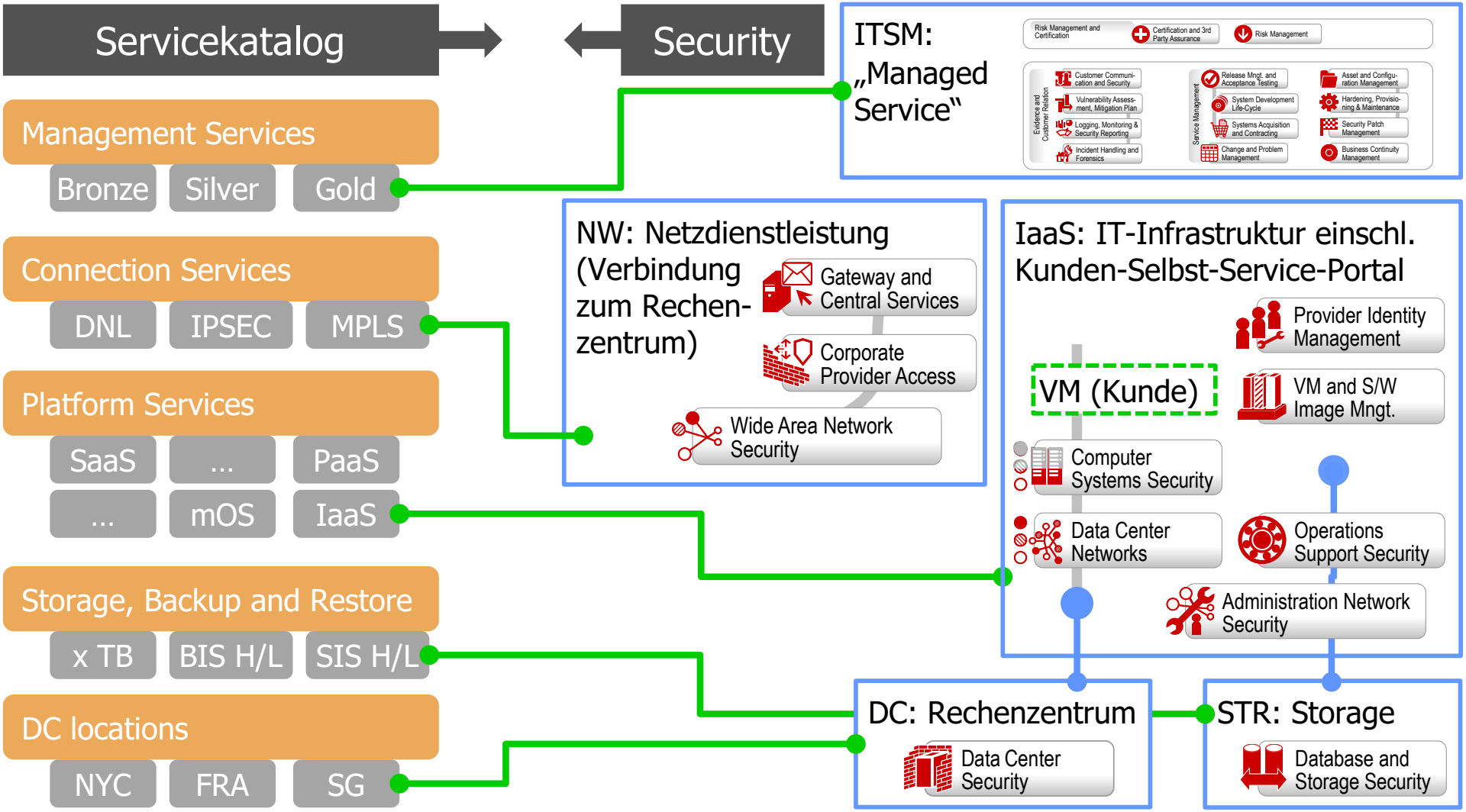
2. Flexibilität: Katalog-Bausteine (links) und Sicherheitsstandards (rechts).

Servicekatalog → ← **Security**

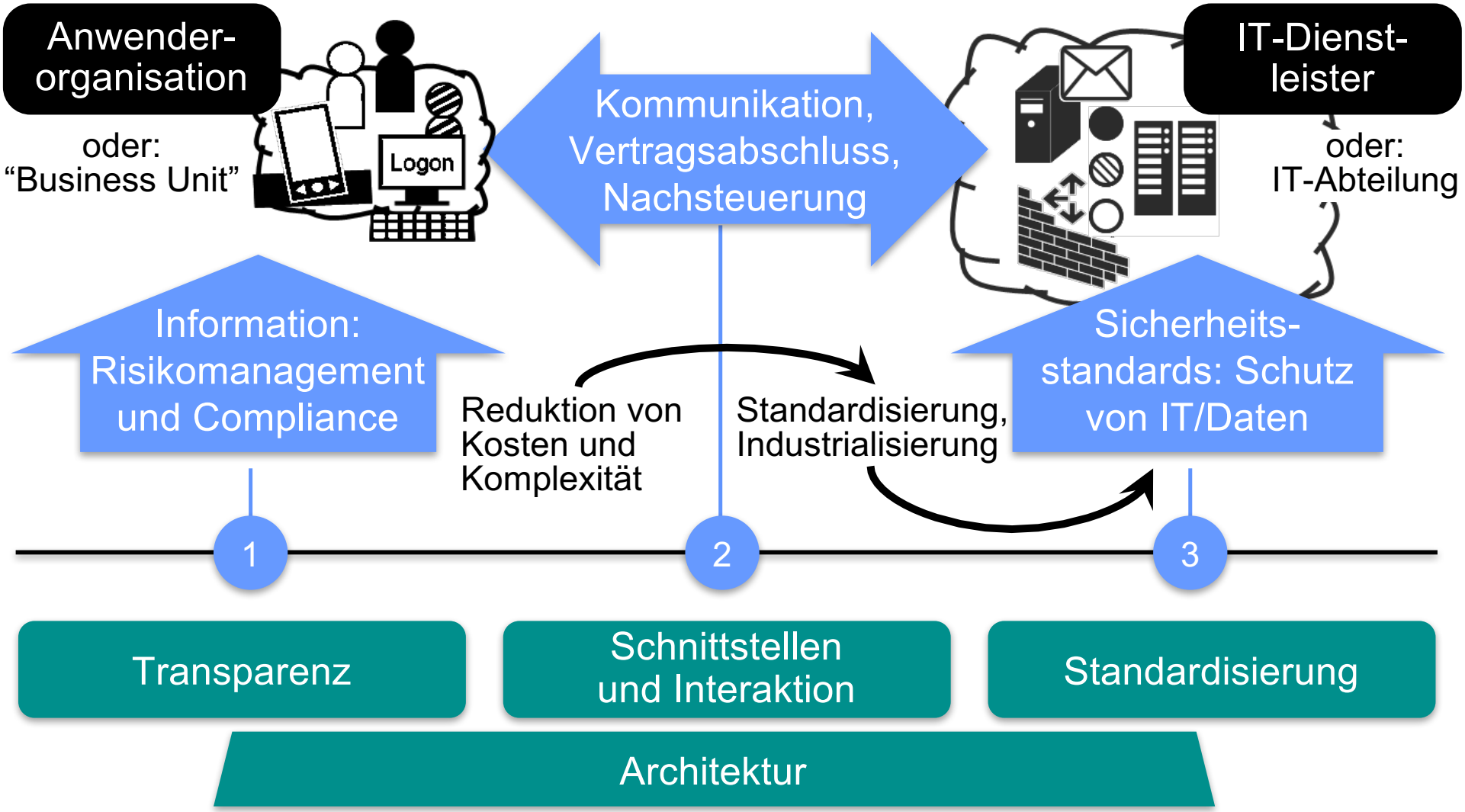
- **Management Services**
  - Bronze
  - Silver
  - Gold
- **Connection Services**
  - DNL
  - IPSEC
  - MPLS
- **Platform Services**
  - SaaS
  - …
  - PaaS
  - …
  - mOS
  - IaaS
- **Storage, Backup and Restore**
  - x TB
  - BIS H/L
  - SIS H/L
- **DC locations**
  - NYC
  - FRA
  - SG



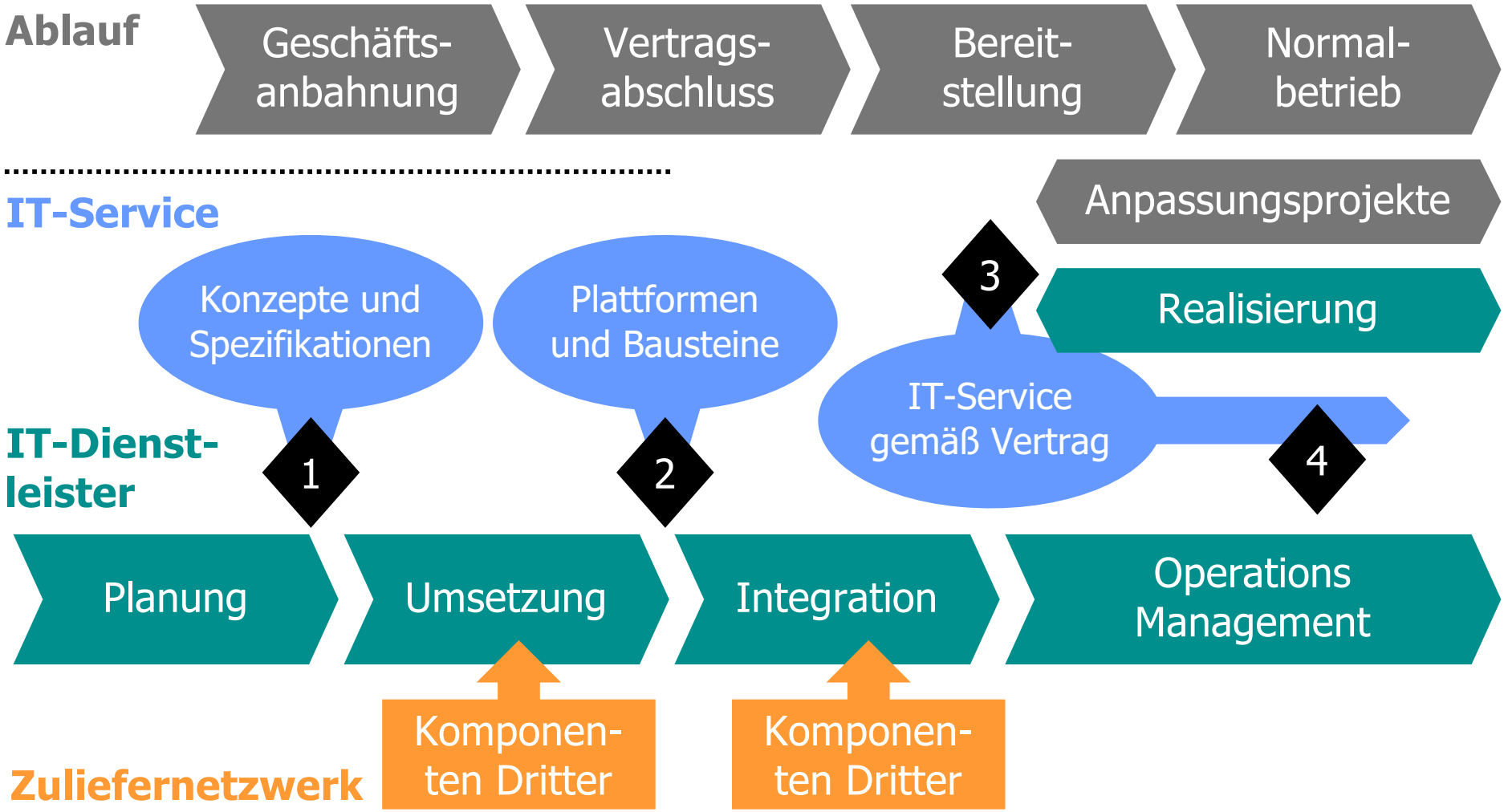
2. Flexibilität: Katalog-Bausteine (links) und Sicherheitsstandards (rechts).



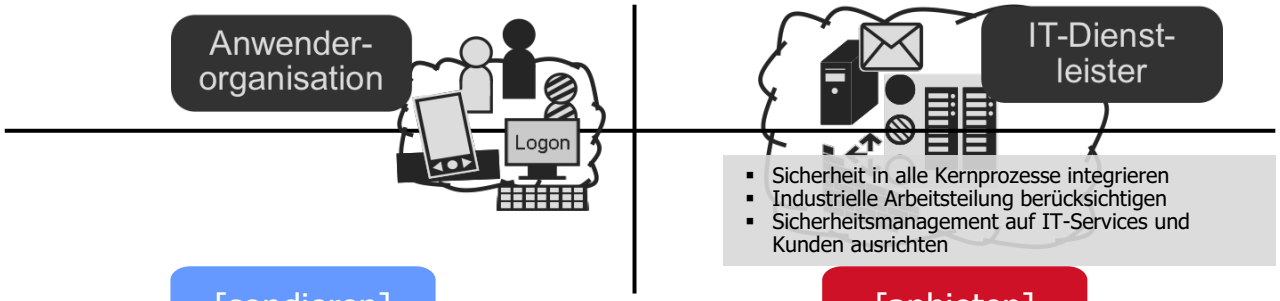
3. Organisationsübergreifend handeln: Das ESARIS-Steuerungsmodell.



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



Joint Security Management (JSM)



Anwender-organisation		IT-Dienst-leister
		▪ 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)

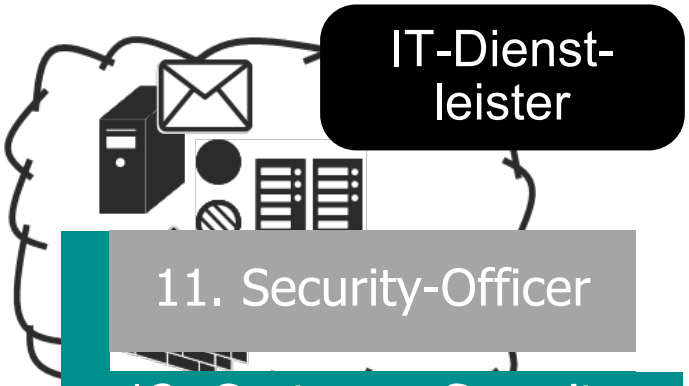
wo?

Beispielunternehmen
- Umsatz: 10 Mrd. €

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

[nachsteuern] Aufgaben und Rollen im Normalbetrieb.

Aufgaben und Schnittstellen im Normalbetrieb



1. Governance: Rollen, Ressourcen, Prozesse

2. Risikomanagement, Lagebild, Compliance

3. Nutzung Security-Reports, Audits etc.

4. Maintenance, Change-Advisory

5. Help-Desk- und Vorfallmeldung

6. Vorfall- und Notfall-Management

7. sichere Integration

8. Anforderungs-management

9. Projekt-Management

10. Service-Orchestrierung Vertragsmanagement

11. Security-Officer

12. Customer Security Manager

13. Service-Delivery-Management

14. Help-Desk, Vorfallmngt.

15. Account-/Service-Delivery-Manager

16. Service-Delivery-Management, Projects

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

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

T · · Systems ·