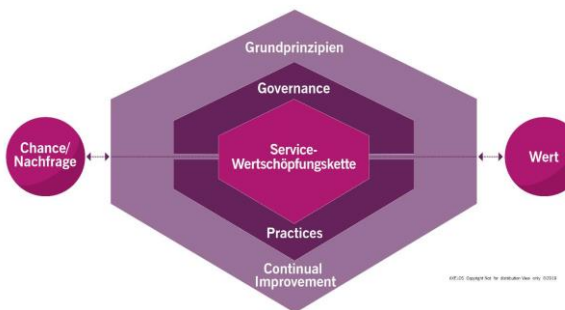
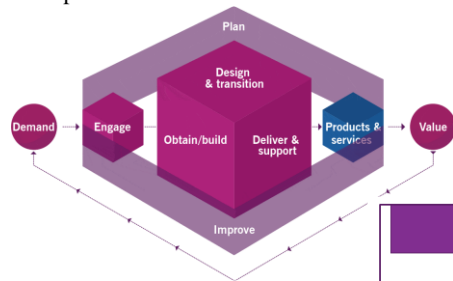


- 1 Focus on value
- 2 Start where you are
- 3 Progress iteratively with feedback
- 4 Collaborate and promote visibility
- 5 Think and work holistically
- 6 Keep it simple and practical
- 7 Optimize and automate



ITIL Service Value System
 Chance/Opportunity/Demand
 Guiding principles
 Governance
 Service Value Chain
 Practices
 Continual improvement
 Value => der Output des Systems
 (Zusammenarbeit)

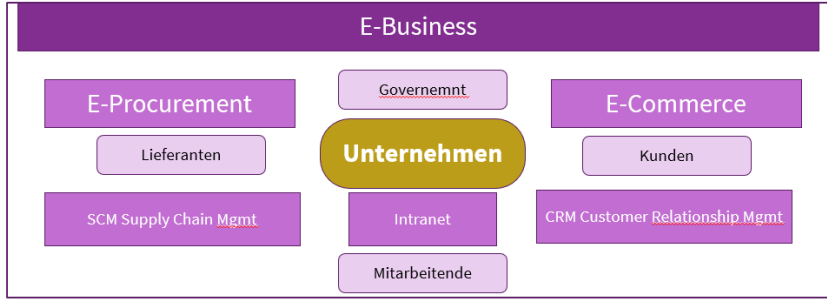
diesen Mechanismus handeln wir. Es baut aufeinander auf. **Guiding Principles** sind universell und dauerhaft gültig und leitet die Unternehmung durch den Prozess. **Governance** stellt zusätzliche Regeln auf und achtet auf die Einhaltung der Regeln und Principles. **Service value Chain** Operationsmodell. Gliedert Aktivitäten. Bringt den Input zum Output. **Practices** sind Ressourcen für die Durchführung wie andere Services oder Applikationen. **Continual improvement** Feedback für Verbesserungen. denn aussehen? Wie ist das Ressourcen von aussen verwendet werden und wie sie wurde stattfin-den. **& Support** Hier wird das



Enterprise Architektur

- Geschäftsarchitektur
- Prozessarchitektur (Organisationsarchitektur)
- Datenarchitektur
- Anwendungsarchitektur
- Technologie- oder Infrastrukturarchitektur

E-Business Application Map



DoD(Departement of Defense)

Web Services?

UDDI Universal Description, Discovery and Integration. Standardisierter Verzeichnisdienst.

REST Representational State Transfer ist eine Softwarearchitektur.

Arten von Changes nach ITIL 4: Normal change, Standard Change und Emergency Change

OSI (Open Source Interconnection) 7 Layer Model						
Layer	Application/Example		Central Device/ Protocols	G A T E W A Y	DOD4 Model	
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		User Applications SMTP		Process	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		Logical Ports RPC/SQL/NFS NetBIOS names			Host to Host
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R I N G	TCP/SPX/UDP		Internet	
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting					
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		Switch Bridge WAP PPP/SLIP		Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		Hub			

Informationssicherheit

der Vertraulichkeit von Informationen
 welchen Personen Informationen einsehen oder verändern dürfen.
 der Integrität von Informationen
 Sicherung, dass Informationen nicht unerkannt bzw. unbemerkt verändert werden.
 der Verfügbarkeit von Informationen
 Zeit in denen Informationen verfügbar sind.
 der Verbindlichkeit von Informationen
 zweifelsfreie und gegebenenfalls gerichtsverwertbare Zuordnung (Log, Signaturen).
 der Authentizität von Informationen
 Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Information.

- SQL-Injection
- Cross-Site-Scripting
- Session Hijacking
- Cross-Site-Request-Forgery
- Directory Traversal
- E-Mail-Injection
- Man-in-The-Middle-Angriff
- Man-in-the-Browser
- Denial of Service

Change schedule Verschiedene Änderungen werden zu einem Release zusammengeführt. Dabei wird sichergestellt, dass Änderungen nicht mit anderen Änderungen oder anderen Aufgaben in Konflikt geraten.

Verschlüsselung • gemeinsam genutzten Computer, Daten eines Benutzers sind für die Mitbenutzer unlesbar
 • unberechtigt Zugang zu einem Computer resp. den Daten ist nicht möglich
 • Informationen auf mobilen Geräten wie Notebooks und USB-Speichermedien
 • eMail werden über unsichere Pfade verteilt
 • Nutzung von unsicheren WLAN in öffentlichen Bereichen -> Verschlüsselt kommunizieren **Digitale Signatur** verbindet mit anerkannten Zertifikaten, wer tat wann was verbindet die Identität des Unterzeichnenden (WER) unveränderbar. **OATH Open Authentication Initiative** hat zum Ziel eine Strong Authentication Technology bei Web und normalen Anwendungen umzusetzen. Um auf geschützte Services/Daten auf dem Resource Server zuzugreifen, muss ein «Access Token» vom Client als Repräsentation der Autorisierung übermittelt werden. Mittels

des Parameters scope können die mit dem Access Token verbundenen Berechtigungen festgelegt werden. Zum einen kann der Client gewünschte Berechtigungen beim Authorization Server anfragen, zum anderen teilt dieser die gewährten Berechtigungen mit. Das Access Token hat eine zeitlich begrenzte Gültigkeit. **QPC Zertifikat** Qualified Personal Certificate und Qualified Commercial Certificate erfüllt die höchsten Anforderungen des schweizerischen Signaturgesetzes (ZertES) und des europäischen Standards (ETSI). Es dient der Erstellung von rechtlich verbindlichen digitalen Signaturen (gemäss schweizerischem Obligationenrecht OR der Handunterschrift gleichgestellt) und wird zum elektronischen Unterzeichnen von Dokumenten verwendet. **CAB** Change Advisory Board Prozessziel: Bewerten eines vorgeschlagenen Changes und Autorisieren der Change-Planungs-Phase. Falls erforderlich, werden höhere Genehmigungs-Ebenen in den Freigabe-Prozess mit einbezogen (z.B. das IT-Management). **Architektur schichten** Präsentationsschicht, Applikationsschicht, Persistenzschicht. **ACID** atomicity, consistency, isolation, durability. Sichert für Datenbanken, auch wenn errors auftauchen. Daten behalten ihre Gültigkeit. **Testkonzept** • Herkunft der Testdaten • Definition von Struktur, Umfang, Qualität und Lebensdauer der Daten • Abklärung der Verfremdung oder der künstlichen Erzeugung der Daten • Definition der Verantwortlichkeiten im Testdatenprozess • Erläuterungen zum Einsatz entsprechender Werkzeuge • Berücksichtigung von Standards, Normen, Compliance- sowie Datenschutzrichtlinien • Auswirkungen auf nachgelagerte Prozesse bei verfremdeten oder synthetisch erzeugten Daten • Löschen beziehungsweise Rückgabe und Archivierung der Testdaten

Verfremdung. Testdaten werden verfremdet, bezieht sich nur auf Textdaten. Olivier Düggelin -> O.D **Pseudonym** Anstelle der richtigen Namen werden Namen und deren Verknüpfungen durch ein Pseudonym ersetzt wie Donald Duck. **Synthetisieren** Daten werden generiert mit all ihren Verknüpfungen.