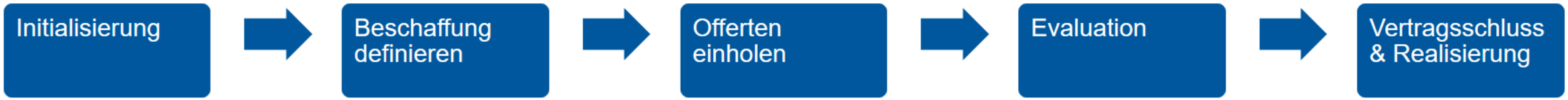
Beschaffung einer sicheren App

Herbsttagung 2017

Philipp Vontobel

Beschaffungsprozess



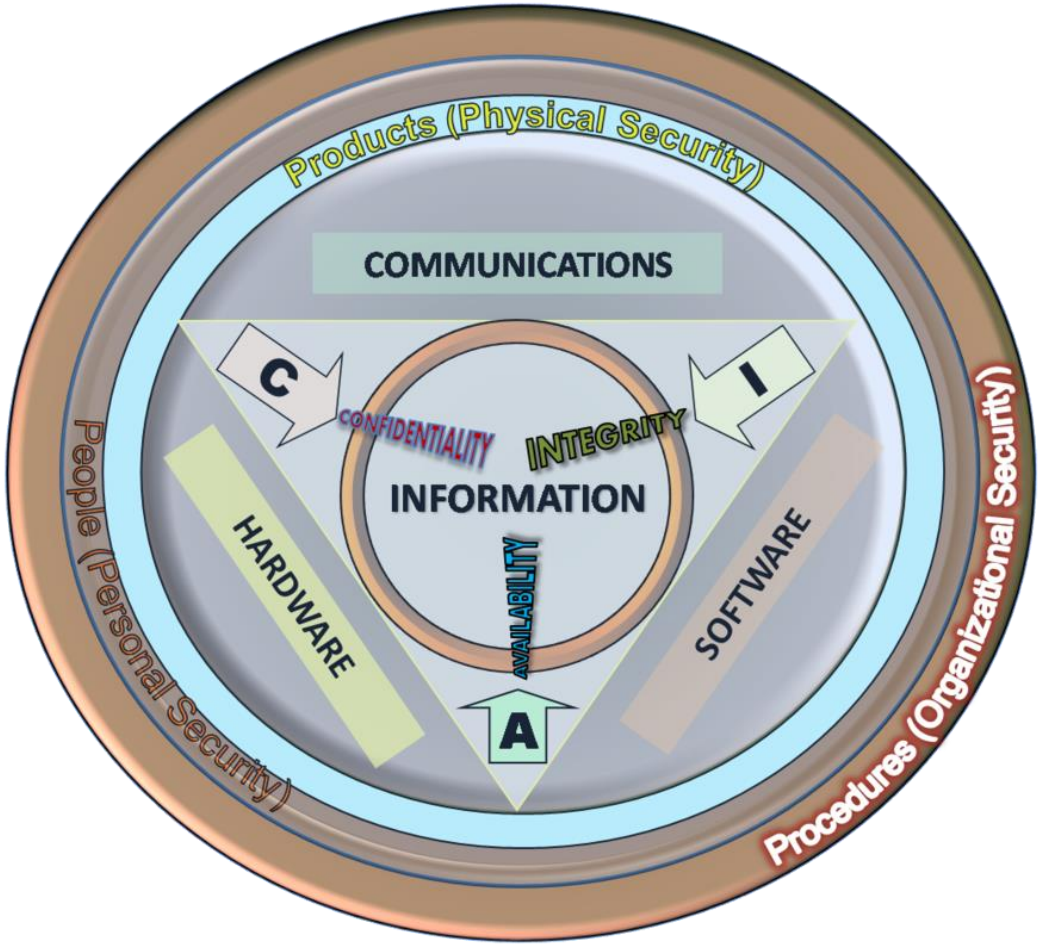
- Bedarf
  - Schutzbedarf
  - Zeit
  - Verfahren und Ablauf
- Architektur
  - Bewertungs-kriterien
- Bewertungs-kriterien
- Vertrag
  - Verfahren und Ablauf

Bedarf: Hinterfragen

- Brauchen wir wirklich eine App und wenn ja in welcher Form?
- Welche Angriffsszenarien und Risiken gibt es?
  - Vermeiden, Vermindern, Verlagern, Akzeptieren
- Quer-Vergleich zu «Altbewährtem» herstellen:
  - Würden wir dieselben Anforderungen auch an Apps auf anderen Mobilgeräte (Laptops) stellen?
  - Sind Android und iOS nicht tendenziell sogar sicherer als z.B. Desktop-Plattformen?
- Vorsicht beim Kumulieren von Anforderungen!
- Durchführen einer Schutzbedarfsanalyse zur systematischen Erhebung von InfoSec-Anforderungen.

Nach systematischer Erhebung dürfen Risiken auch mal akzeptiert werden.

Informationssicherheit InfoSec (international)



"Preservation of **confidentiality**, **integrity** and **availability** of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)

Informationssicherheit:

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

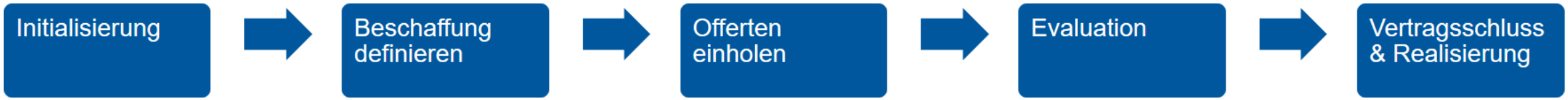
- Authentizität (Verbindlichkeit)
- Nicht-Abstreitbarkeit
- Anonymität?

Informationssicherheit (national)

- Bundesgesetz über den Datenschutz (DSG):
  - Deckt grundsätzlich «nur» Personendaten ab.
  - Verlangt angemessene technische und organisatorische Massnahmen um die Daten gegen unbefugtes Bearbeiten zu schützen (Art. 7 Abs. 2)
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
  - Pflicht zur Sicherstellung von **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** der Daten sowie Schutz vor Vernichtung, Verlust, technische Fehler, Fälschung, Diebstahl oder widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen etc. (Art. 8 Abs. 1)

- Oft haben öffentliche Verwaltungen Templates verfügbar, die beispielsweise IT-Grundschutzkataloge (abgeleitet vom deutschen BSI) unter anderem zur Risikoabwägung enthalten.
- Oder: https://www.it-sicher.kaufen/

Beschaffungsprozess



- Bedarf
- Schutzbedarf
- Zeit
- Verfahren und Ablauf

- Architektur
- Bewertungs-kriterien

- Bewertungs-kriterien

- Vertrag
- Verfahren und Ablauf

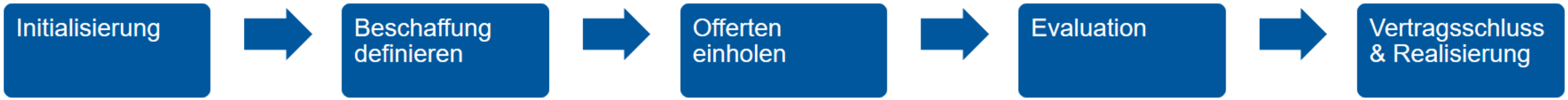
Schutzbedarfsanalyse (u.a. HERMES-Initialisierung)

- Schutzbedarfsanalysen/ISDS-Vorabklärungen (mit Template/Toolunterstützung) helfen dabei, die wichtigsten Ansatzpunkte zu identifizieren.

- Beispiel Suisse ePOLICE:
  - Schutzbedarfsanalyse und Vorabklärung ISDS (Prüfung Lastenheft) wurde vor Publikation durchführt.
  - Gegenseitiges Verständnis und Vertrauen aufgebaut.
  - Kein Einfluss auf Zeitachse! Sämtliche Arbeiten waren parallel möglich.
  - Es ergaben sich konkrete InfoSec-Anforderungen.

Schutzbedarfsanalysen mit Tool/Template-Unterstützung lohnen sich; nach der Beschaffung sind Massnahmen schwerer umzusetzen.

Beschaffungsprozess



- Bedarf
- Schutzbedarf
- Zeit
- Verfahren und Ablauf

- Architektur
- Bewertungs-kriterien

- Bewertungs-kriterien

- Vertrag
- Verfahren und Ablauf

Faktor Zeit

Royal Navy fleet being depleted by long procurement process

Quelle: http://www.itv.com/news/2016-11-29/royal-navy-fleet-being-depleted-by-long-procurement-process/

Software 137

HMS Windows XP: Britain's newest warship running Swiss Cheese OS

Spotted on carrier control room screens - reports

By Gareth Corfield 27 Jun 2017 at 13:52 SHARE ▼

HMS Queen Elizabeth just after leaving her Rosyth dockyard for the first time yesterday. Crown copyright

Quelle: The register

Faktor Zeit: Ansatzpunkte

- Technologische Entwicklung als Tatsache in Vertrag verankern:
  - «state-of-the-art» zu jedem Zeitpunkt: Geräte, OS, Firmware, Dev.-Tools und -Frameworks, Standards, Security-Empfehlungen und Good Practices etc.
  - Weiterentwicklung und Aufrechterhaltung der vollen Funktionalität und Sicherheitsstufe mindestens für jeden Major-Release der zugrundeliegenden Plattform fordern.

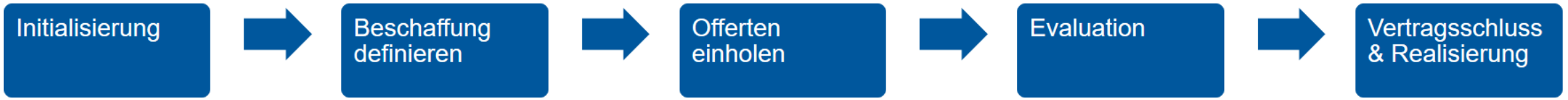
- Institutionalisierte Endgeräte-Labors beim Lieferanten fordern und ev. besichtigen und/oder auditieren.

Faktor Zeit: Hinweise für öffentliche Beschaffungen

- Öffentliche Beschaffungen haben gesetzliche Fristen von max. 50-60 Tagen, dauern aber oft 6-12 Monate, selbst ohne Einsprachen
- Das «Dialogverfahren» (künftig wohl auch in Kantonen zulässig) wird kaum genutzt, soll aber mehr gefördert werdne künftig.
- Können künftig auch «Agile Beschaffungen» durchgeführt werden?
- Ist ein Freihänder möglich? («geistiges Eigentum», «technische Besonderheiten», ev. «Unvorhersehbarkeit», «Ersetzung / Ergänzung /Erweiterung» etc.)

Mehr Mut zeigen bei Beschaffungen um den Zeitraum zu verkürzen.

Beschaffungsprozess



- Bedarf
- Schutzbedarf
- Zeit
- Verfahren und Ablauf

- Architektur
- Bewertungs-kriterien

- Bewertungs-kriterien

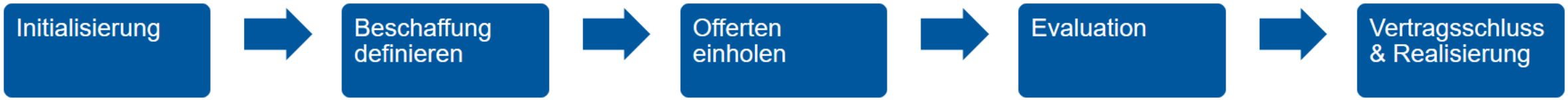
- Vertrag
- Verfahren und Ablauf

Verfahren und Ablauf

- Involvierung InfoSec Spezialisten bei der Vorbereitung des Verfahren (Erstellung Lastenheft)
- ISDS/DSA von Beginn weg berücksichtigen («Gratis InfoSec Audit»)
- Externe Prüfung/Bewertung der Angebote bei unabhängigen InfoSec Spezialisten
- Qualitäts-Meilensteine mit vertraglichen Folgen im Realisierungsprojekt:
  - Konventionalstrafen
  - Vertragsauflösung
  - Kostenpflichtiges Hinzuziehen einer Konkurrenzfirma etc.

InfoSec-Meilensteine in Verfahren einbauen und KnowHow bei Bedarf einkaufen.

Beschaffungsprozess



- Bedarf
- Schutzbedarf
- Zeit
- Verfahren und Ablauf

- Architektur
- Bewertungs-kriterien

- Bewertungs-kriterien

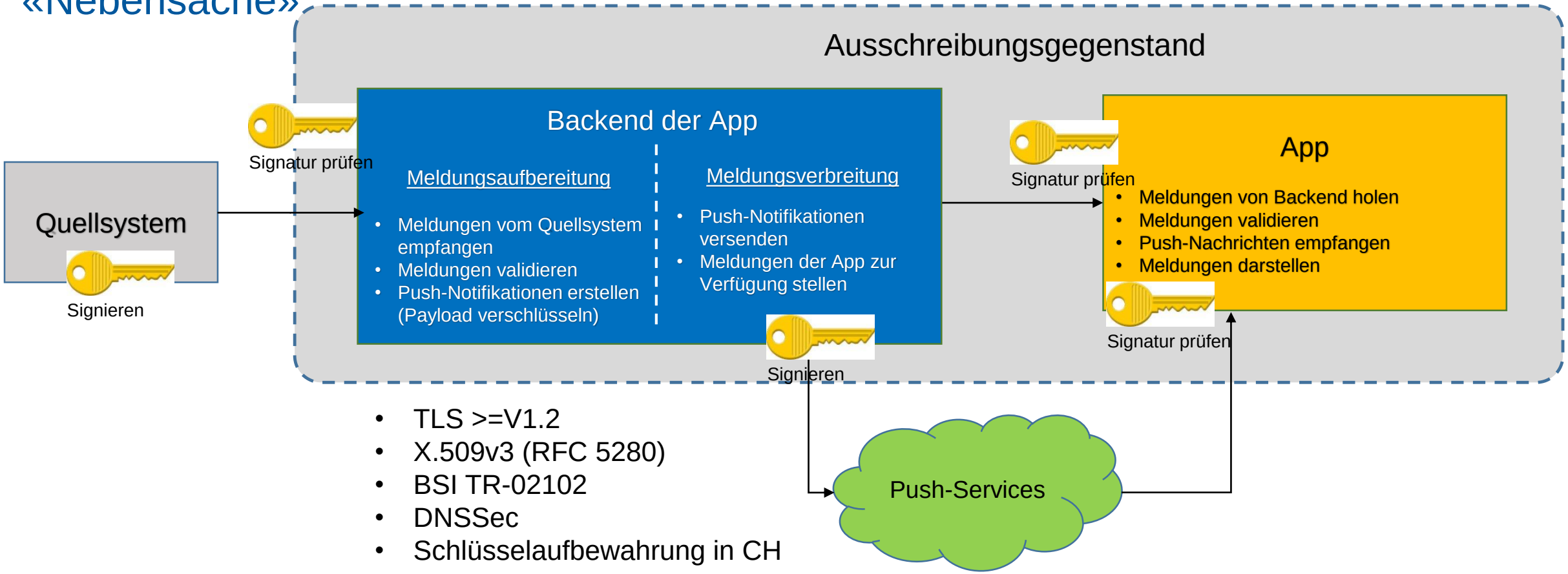
- Vertrag
- Verfahren und Ablauf

Architektur: Komponentenwahl

- Unbekannte Komponenten bergen teils unbekannte Risiken:
  - Third-party-tools
  - Frameworks
  - Gerätekomponenten (Chips etc.)
  - Plugins
  - Webservices
  - …
- Minimum: Offenlegung und Mitspracherecht («Veto») erzwingen.
- Idealerweise: Zusätzlich bestimmte Komponenten antizipieren und ausschliessen (z.B. Google Analytics).

Architektur: Beispiel einer Meldungs-App

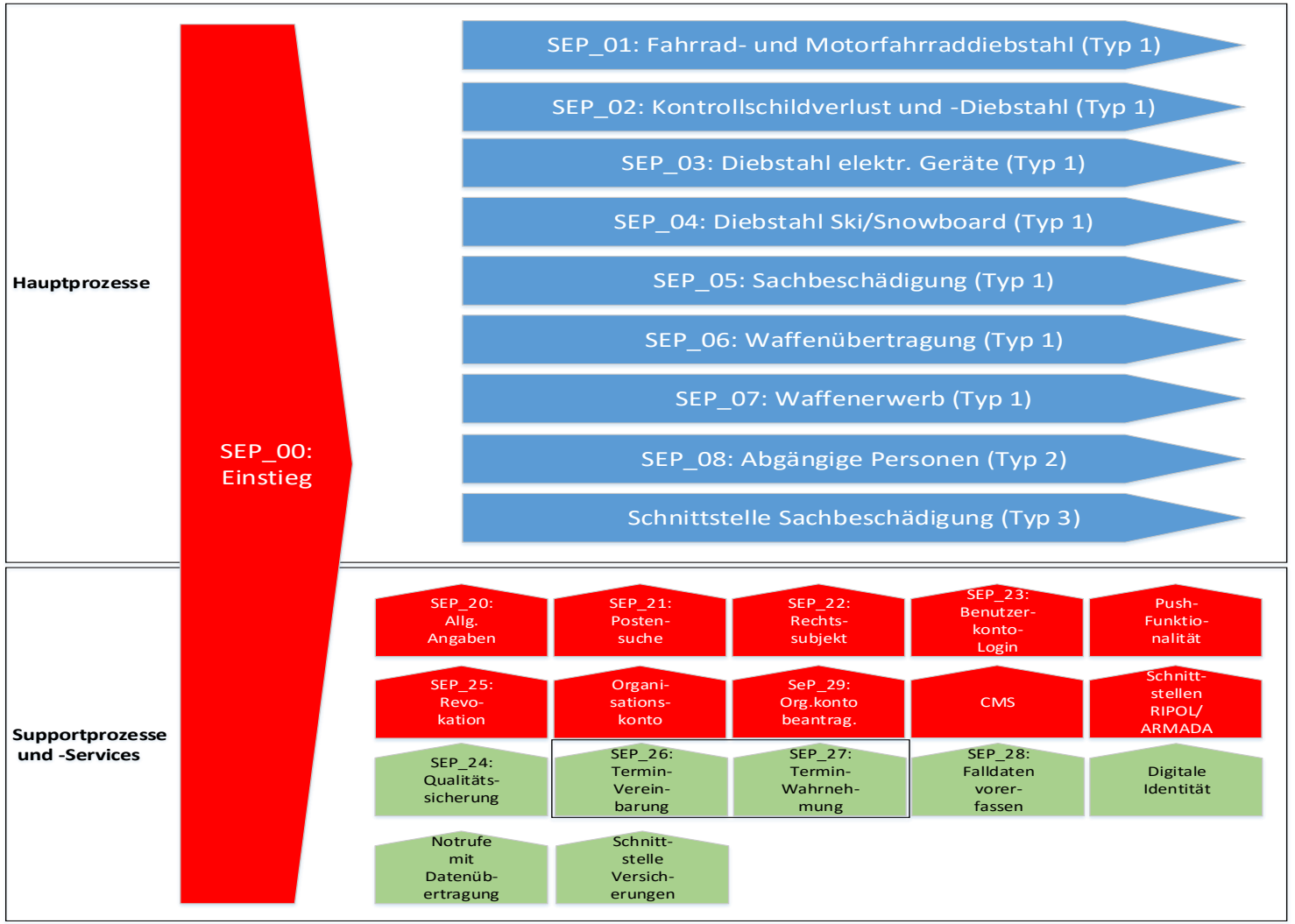
InfoSec Ziele: Integrität, Nachvollziehbarkeit und Authentizität; Vertraulichkeit eher «Nebensache»



- TLS >=V1.2
- X.509v3 (RFC 5280)
- BSI TR-02102
- DNSSec
- Schlüsselaufbewahrung in CH
- …

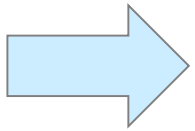
Architektur: Beispiel Suisse ePOLICE

- Ziele: Effektive und Effiziente Prozesse, Modernität, Usability, Kosten
- Prozess- bzw. Servicearchitektur, keine eigentliche Systemarchitektur
- InfoSec zwar umfassend betrachtet, aber eher generisch gefordert.



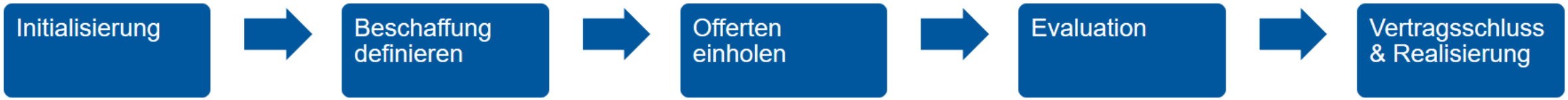
Architektur: Übersicht

- Die Architektur kann bei Beschaffungen vorgegeben oder zumindest skizziert werden.
- Der Detailgrad der Architekturvorgaben kann beliebig hoch ausfallen.
- Den Anbietern sollten so viele Freiheiten wie möglich gewährt werden.
- Funktionale Beschreibungen sparen wertvolle Zeit.



Nach Risiko- und Zeitabwägung sowie verfügbarem KnowHow die nötigsten Architekturvorgaben definieren.

Beschaffungsprozess



- Bedarf
- Schutzbedarf
- Zeit
- Verfahren und Ablauf

- Architektur
- Bewertungs-kriterien

- Bewertungs-kriterien

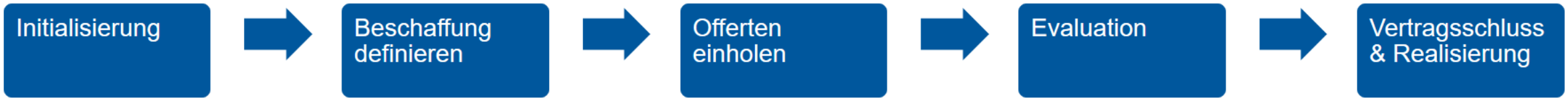
- Vertrag
- Verfahren und Ablauf

Bewertungskriterien

Eignungskriterium (Firma)	• Wirtschaftliche Elemente • Nachhaltigkeit • Zertifikat ISO 27001 (ISMS) • Referenzen (Reputation Lieferant)
Technische Spezifikation (MUSS Produkt/Dienstleistung)	• Best/Good-Practices: OWASP Richtlinien-Einhaltung erzwingen • Security-Audits von Dritten akzeptieren • Offenlegung/Ausschluss von Komponenten • Zwingende InfoSec-Anforderungen: z.B. TLS >=V1.2
Zuschlagskriterium (SOLL Produkt/Dienstleistung)	• InfoSec-Konzept • Architektur-Konzept: Progressive/Hybrid/Native, Micro-Services • Konzept für Patching und Updates

Bewertungsspielraum durch qualitative Kriterien sicherstellen.

Beschaffungsprozess



- Bedarf
- Schutzbedarf
- Zeit
- Verfahren und Ablauf

- Architektur
- Bewertungs-kriterien

- Bewertungs-kriterien

- Vertrag
- Verfahren und Ablauf

Vertrag

- SLA inklusive InfoSec Messpunkte:
  - Reaktionszeit auf Incidents
  - Zeitnahes Nachziehen von Patches und Security Updates
  - Business Continuity / Desaster Recovery
  - Aktuelle Dokumentation
  - Etc.
- Gewährleistung/Garantie auch bezüglich InfoSec regeln:
  - Recht auf Security-Audit durch externen Partner verankern
- Change Management klar regeln
- Konventionalstrafen und Klauseln bezüglich Vertragsänderung und Vertragsauflösung

Vertrag vor Anbieterentscheid ausarbeiten.

Zusammenfassung der wichtigsten Punkte

- ✓ Nach systematischer Erhebung dürfen **Risiken auch mal akzeptiert werden**.
- ✓ **Schutzbedarfsanalysen** mit Tool/Template-Unterstützung **lohnen sich**; nach der Beschaffung sind Massnahmen schwerer umzusetzen.
- ✓ **Mehr Mut zeigen bei Beschaffungen** um den Zeitraum zu verkürzen.
- ✓ **InfoSec-Meilensteine** in Verfahren **einbauen** und **KnowHow** bei Bedarf **einkaufen**.
- ✓ Nach Risiko- und Zeitabwägung sowie verfügbarem KnowHow **die nötigsten Architekturvorgaben definieren**.
- ✓ **Bewertungsspielraum** durch qualitative Kriterien **sicherstellen**.
- ✓ **Vertrag vor Anbieterentscheid ausarbeiten.**

InfoSec von Anfang an berücksichtigen!

Quellen, weiterführende Links

- https://www.it-sicher.kaufen
- Buch: *«Beschaffung unter Berücksichtigung der IT-Sicherheit»* (Piller 2017), ISBN 3658185988
- ISO 27001 (ISMS)
- ISO 27002 (Leitfaden ISMS, nicht zertifizierbar)
- «IT Security made in Germany» (https://www.teletrust.de/itsmig/)
- https://www.pmi.org/learning/library/importance-of-security-requirements-elicitation-9634 (Basis: CLASP von OWASP)
- Lean procurement canvas (https://www.lean-agile-procurement.com/)
- Internationaler Standard für IT-Sec-Zertifizierungen : Common criteria (http://www.commoncriteriaportal.org/)
- https://www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit/
- OWASP Contract Annex (https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)

CSI CONSULTING

INFORMATION AND COMMUNICATION