Cyber- und Informationssicherheit

Chance & Herausforderung in der Prüfung

Ing. Dipl.-Ing.(FH) Andreas Preslmayr MSc
Stadtrechnungshof Wien

EURORAI Seminar
18. bis 19. April 2018
Rotterdam

Programm

- **Kurzvorstellung**
  - Wien, Digitalisierung/Informations und Kommunikations Technologie (IKT)
  - Stadtrechnungshof Wien
- **Strategien** zum **Prüfungsfeld Informationssicherheit**
  - Zugang
  - Nutzen
  - Risikofelder, Kernthemen
  - Methoden
  - Organisation
  - Wirkung
- **Anwendung** des **Prüfungsfeld Informationssicherheit**
  - Praxisbeispiele
  - Erfahrungen
- **Verweise, Quellen, Rückfragen**

Wien, Digitalisierung/IKT

Turm des neuen Wiener Rathauses mit Rathausmann
Wiener Wappen:

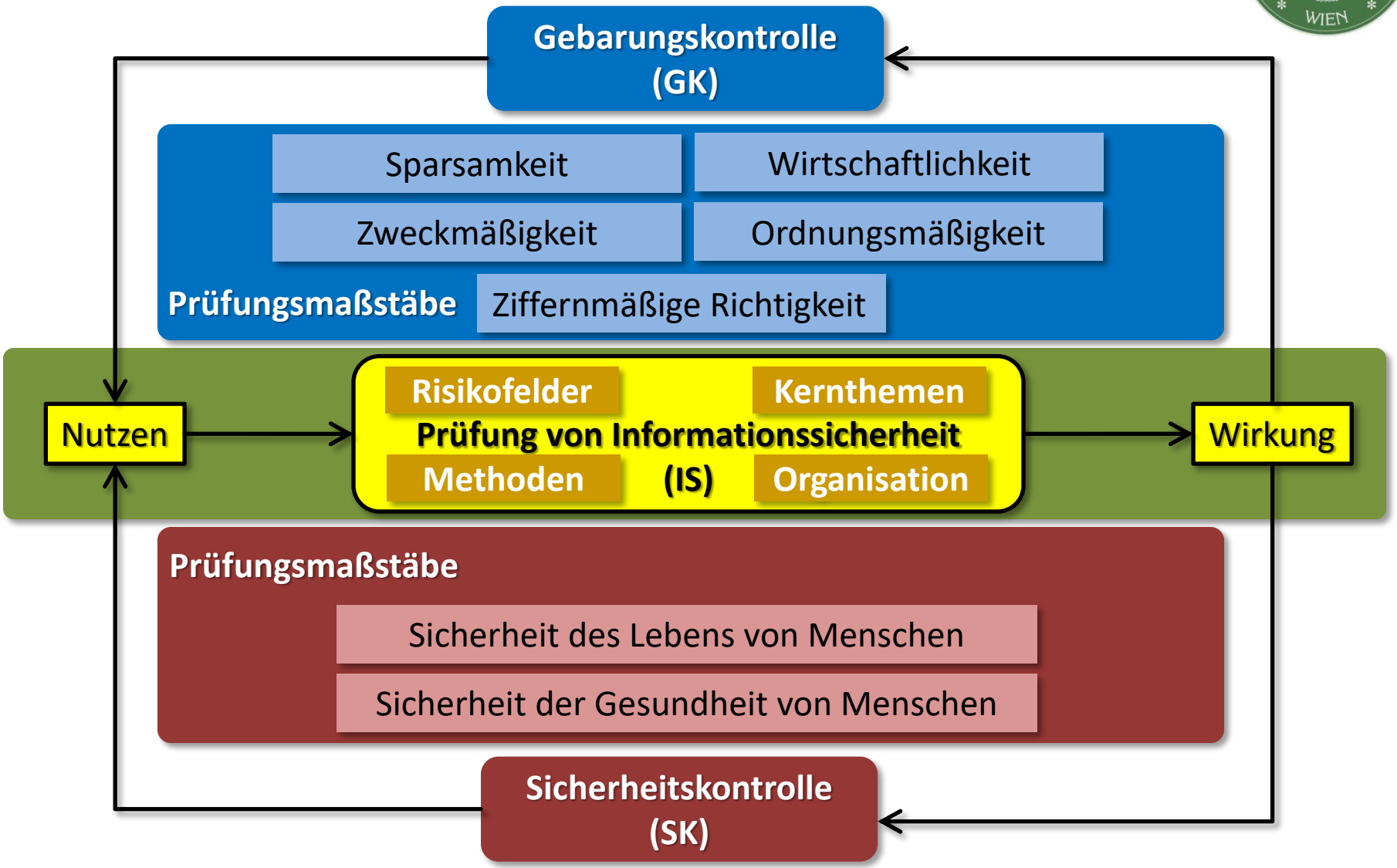
- Land Wien – Stadt Wien
  - **Bundesland** und **Bundeshauptstadt** von **Österreich**
  - Gemeinde in der Rechtsform „**Statutarstadt**“
  - **23 Gemeindebezirke** (Stadtbezirke)
  - **Einwohner**: **~1,87 Mio.** (Stand: 1.1.2017)
  - **Fläche**: **~415 km²**
  - **BIP** (2015): **~86,5 Mrd. €**
  - 2016: **Einnahmen ~22,4 Mrd. €** - **Ausgaben ~21,4 Mrd. €**
- Digitalisierung
  - seit **März 2011** Initiative der **Smart City Wien**
  - seit **September 2014** Positionierung der **DigitalCity.Wien** (Digitale IKT Metropole/Digitalkompetenzen Smart City Wien)
  - **seit 2016 Innovationschub** von **IKT** in der Verwaltung (Blockchain Open Government Data, „Sag‘s Wien“ App, usw.)
- Informations- und Kommunikationstechnologie (IKT)
  - **3** zentrale **IKT Dienstleister** mit **ISO/IEC 27001 Zertifizierungen**
  - **IKT** Infrastruktur **Konsolidierungsprojekt** bis **2019**
  - ~85.000 User, ~5.000 Server, ~5.380 Datenbanken, ~114.000 Arbeitsplatz-Endgeräte, ~1.000 MitarbeiterInnen

Stadtrechnungshof Wien

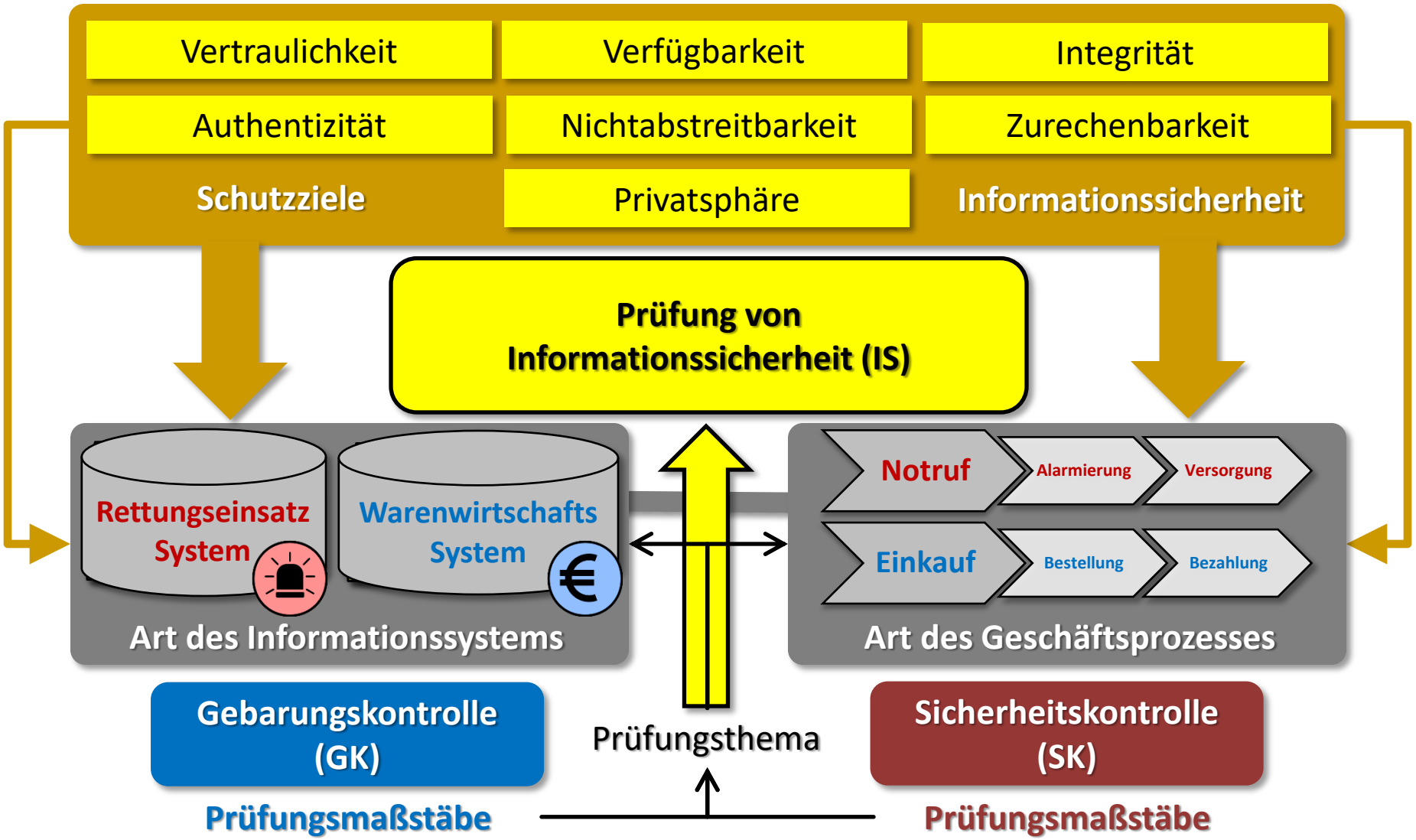
Palais Obentraut, Gebäude des Stadtrechnungshof Wien
Wappen Kontrollamt

- Geschichte
  - gegründet **1. Juni 1920**, **Kontrollamt der Stadt Wien**
  - zwischen 1939-1945, Rechnungsprüfungsamt
  - seit **1. Jänner 2014**, **Stadtrechnungshof Wien**
- Rechtsgrundlage
  - **Wiener Stadtverfassung**, **Gebarungskontrolle (GK)**
  - im Jahr **1977**, **zusätzlich** Verankerung der **Sicherheitskontrolle (SK)** in der **Wiener Stadtverfassung** aufgrund des Einsturzes der Wiener Reichsbrücke (Einzigartigkeit unter den Rechnungshöfen bzw. Kontrollämtern von Österreich)
- Aufgaben
  - **weisungsfreie** und **unabhängige Kontrolleinrichtung** mit insgesamt 92 Bedienstete (69 Bedienstete im Prüfungsdienst)
  - **Gebarungskontrolle (GK)** des unterliegenden Finanzvolumens des Magistrats, der Unternehmungen und der Beteiligungen der Stadt Wien sowie der Einrichtungen die Förderungen der Stadt Wien erhalten
  - **Sicherheitskontrolle (SK)** der Gemeinde betreffend der sich auf die Sicherheit des Lebens oder der Gesundheit von Menschen beziehenden behördlichen Aufgaben, Einrichtungen und Anlagen

Zugang Prüfung Informationssicherheit



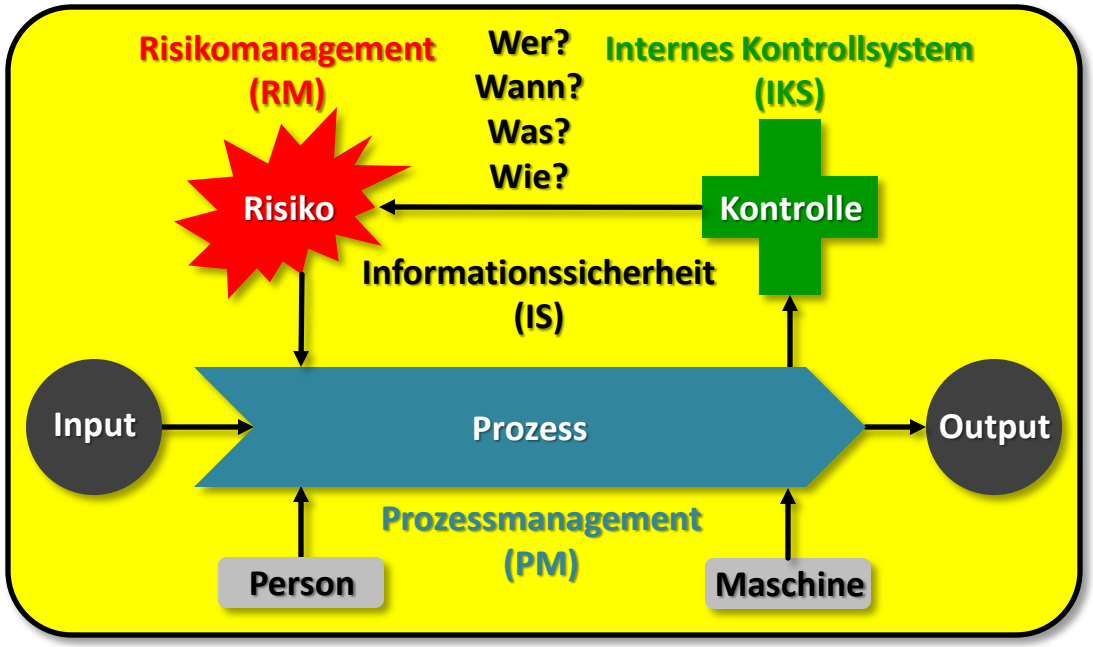
Nutzen Prüfung Informationssicherheit



Risikofelder, Kernthemen

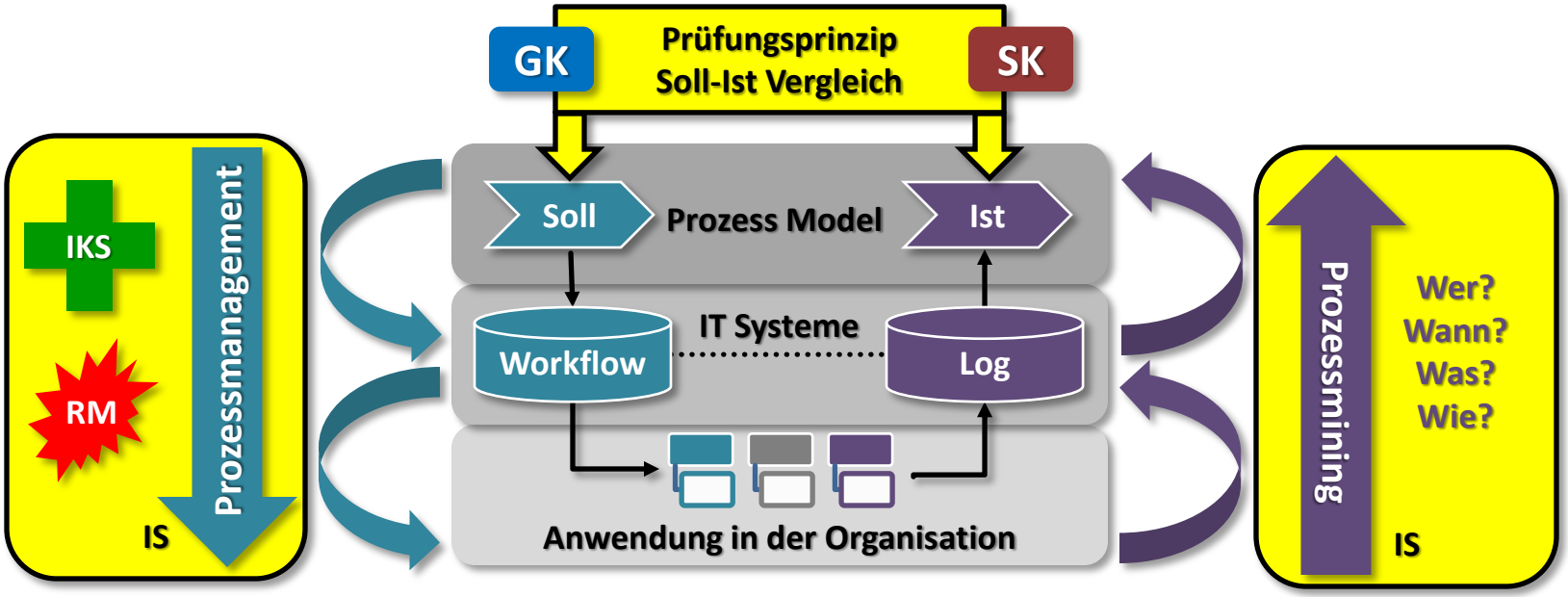
Prüfung Informationssicherheit

- **Risikofelder** entsprechend den Fragestellungen der Prüfungsthemen mit den relevanten **Fachthematiken** aus den bekannten **Regelungen der IKT Branche** (ISO/IEC 2700x Serie, BSI-Standard, IT-Grundschutz, ITIL, COBIT, usw.)
- gezielter **Fokus** auf folgende **Kernthemen/Zusammenhänge**:



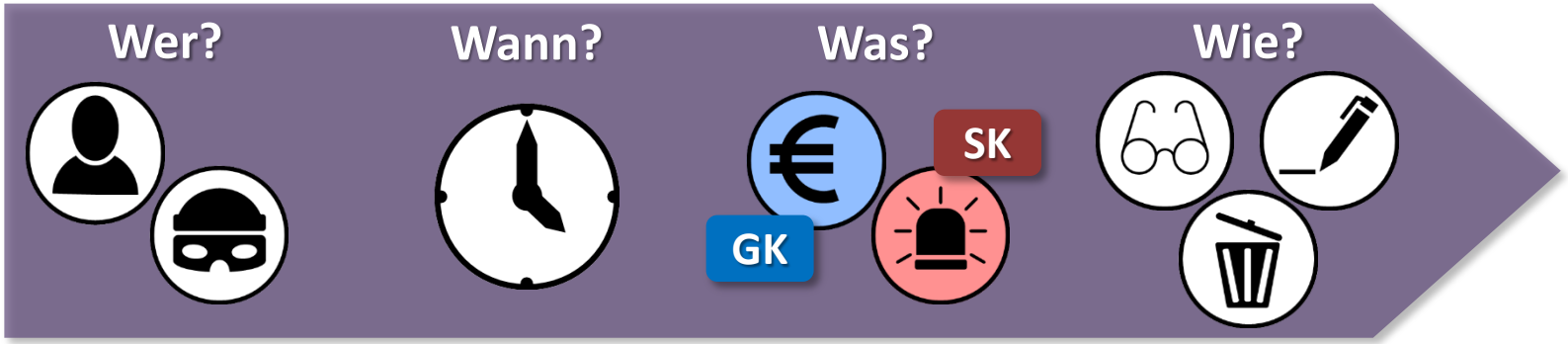
Methoden Prüfung Informationssicherheit

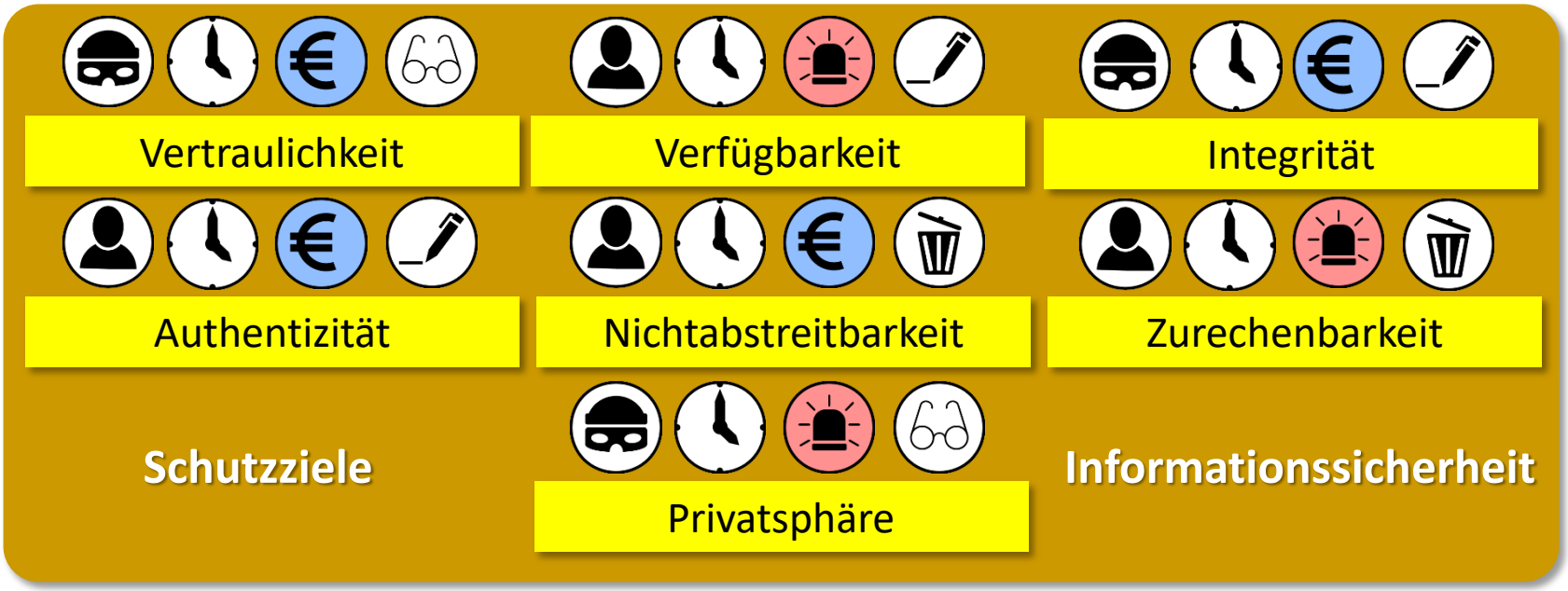
- Grundsätzlich **Verwendung** von **Audit Berechtigungen/Rollen** und **Audit Funktionen** des zu prüfenden **Informationssystems**
- Grundsätzlich **Extraktion/Auswertung** der jeweiligen **Rohdaten** direkt aus den zugrundeliegenden **IT Systemen** durch den **IKT Dienstleister**, nicht durch den Anwender (meistens der Geprüfte)
- **Anwendung/Entwicklung** Datenanalysemethode **Prozessmining**



Methoden Prüfung Informationssicherheit

Prozessmining





Organisation Prüfung Informationssicherheit

- **Fachbereich IT Prüfungen** mit **Expertenwissen** von 3 Personen (nicht ausschließlich eigenständiger Organisationseinheit sondern gebündelte Wissenskompetenz)
  - **Beiziehung** im Rahmen **bestimmter Fragestellungen** zu den jeweiligen Prüfungsthemen
  - **Auswahl** und **Durchführung** von **eigenständigen IT Prüfungen**
  - **Beobachtung/Entwicklung/Bereitstellung** entsprechender **Methoden** und **Werkzeuge** (z.B. MS Excel® mit entsprechenden PlugIns, Befragungssoftware, usw.)
  - **Bereitstellung** von **IT Wissen** im **Intranet** des Stadtrechnungshof Wien
- **Herausforderungen**
  - **Digitale Grundkompetenzen** und **Erfahrungen** von **PrüferInnen**
  - **Expertise Datenmanagement**t (Auswahl, Datenstruktur, Extraktion/Export, Analyse, Auswertung, Interpretation, Darstellung)
  - **Permanente Anwendung** und **Weiterentwicklung** des Können und Wissens in Verbindung zu den raschen technologischen Entwicklungen
  - **Problematik der Expertise** und **Rekrutierung** von **IT Personal** mit den **Berufsbildern „Wirtschaftsinformatiker“**, **„Informationssicherheitsexperte“** und **„Daten Analyst“** in **Kontrolleinrichtungen**

Wirkung Prüfung Informationssicherheit

- **Wirksamkeit** der **Schutzziele** in den **Informationssystemen**
- Über die **Prüfung** von **Prozessen** Erhöhung des **Praxisbezuges** und damit des **Bewusstseins** und der **Wirkung** insbesondere
  - von **Berechtigungen/Rollen** (**Wer?**)
  - von **Effizienz** und **Effektivität** (**Durchlaufzeiten, RM, IKS** und **Prozessschritte** – **Wann?**, **Was?** und **Wie?**)
  - auf für **Prüfung erforderliche Datenstrukturierungen** in den jeweiligen **Informationssystemen** (z.B. ***.XES Ereignisdatenformat** bei **Prozessmining**)

Praxisbeispiele

Prüfung Informationssicherheit

- **Prozessanalyse (Prozessmining)** bei der Prüfung des **IT Servicemanagements** des IKT Dienstleister der Stadt Wien (2016)
- Prüfung über die **Regelungen der IKT Sicherheit von externen KundInnen** des IKT Dienstleister der Stadt Wien (2015)
- **Berechtigungen/Rollen** bei
  - der Prüfung der **elektronischen Schadenmeldungsanwendung** der Stadt Wien (2016)
  - der Prüfung der **Erstellung des Rechnungsabschlusses der Stadt Wien auf SAP Basis** (2014)
- **Aktuelle Prüfungen** (2017 - 2018)
  - **Informationssicherheit** und **Prozessanalyse (Prozessmining)** betreffend der Verwaltung/Verwendung von Zugangstoken (Berechtigungen) sowie des elektronischen Prozesses eines auszustellenden Behördendokumentes in Schulverwaltungssoftware
  - **Prozessanalyse (Prozessmining)** beim SAP Beschaffungsprozess von IKT Hardware und Software

Erfahrungen
Prüfung Informationssicherheit

Herausforderungen

- Rascher **Fortschritt** des **Standes der Technik** in der **Informationssicherheit** gegenüber den in Betrieb befindlichen Softwareapplikationen (auch aufgrund der **laufend bekannt werdenden Sicherheitsproblematiken**)
- Zugang des **„Security by Design“** im Rahmen von Softwareentwicklungen
- **Implementierung** von **Audit Berechtigungen/Rollen** und **Audit Funktionen** in der jeweiligen **Software**
- zugrundeliegende **Datenstrukturen** und **Auswertemethoden** für die Datenanalyse des **Prozessmining** sind nur **sehr gering vorhanden**
- **Aufwendungen** (Zeit und Geld) der IKT Dienstleister für die **Entwicklung** und die **Auswertung** von bestimmten **Datenstrukturen** für die Datenanalyse des **Prozessmining** für Prüfung von Kontrolleinrichtungen **nicht geplant**
- **Wachstum** des Einsatzes von **IKT Systemen** und des damit in Zusammenhang stehenden **rapiden Wachstums** der darin **generierten Datenmengen**

Verweise, Quellen, Rückfragen

- **Homepage des Stadtrechnungshof Wien**
  (http://www.stadtrechnungshof.wien.at/)
- **Wien in Zahlen**
  (https://www.wien.gv.at/statistik/pdf/wieninzahlen-2017.pdf)
- **Smart City Wien**
  (https://smartcity.wien.gv.at/)
- **DigitalCity.Wien**
  (https://digitalcity.wien/)
- **Prozess Mining Manifest**
  (http://www.win.tue.nl/ieeetfpm/lib/exe/fetch.php?media=shared:pmm-german-v1.pdf)

Herzlichen Dank für Ihre Aufmerksamkeit !