Cyber- and information security

STADTRECHNUNGSHOF WIEN

Chance & challenge in the audit

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

City of Vienna Court of Audit

EURORAI conference

18th – 19th April 2018

Rotterdam

EURORAI

European Organization of Regional Audit Institutions

Rekenkamer ROTTERDAM

Agenda

- **Overview**
  - Vienna, digitization/information and communication technology (ICT)
  - City of Vienna Court of Audit
- **Strategy** of the **audit domain information security**
  - Approach
  - Value
  - Areas of risk, core subjects
  - Methods
  - Organization
  - Impact
- **Practice** of the **audit domain information security**
  - Examples
  - Experience
- **References, resources, inquiries**

Vienna, Digitization/ICT

Tower of the New City Hall with City Hall Man, Crest of Vienna

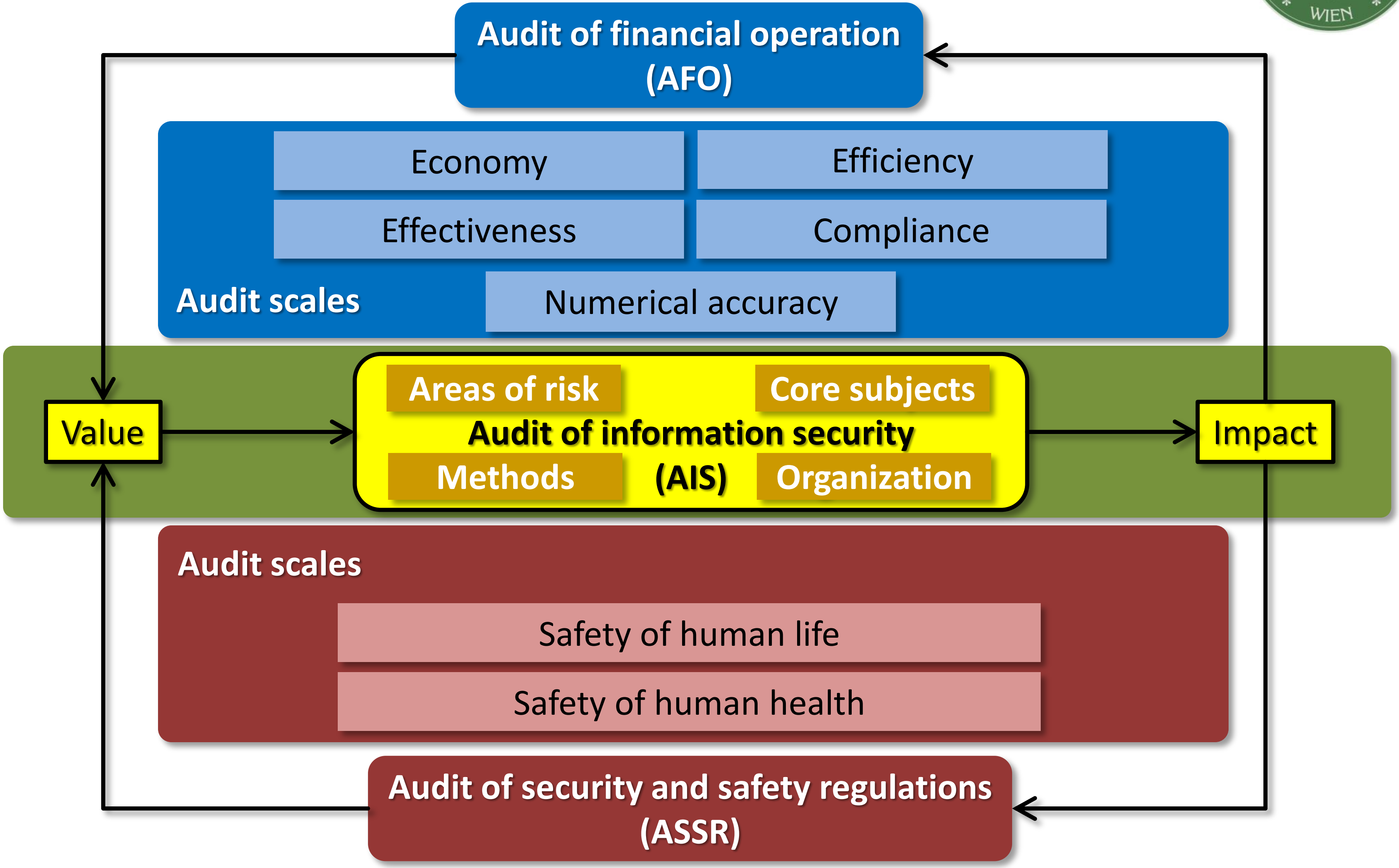
- City of Vienna – Province of Vienna
  - **Capital city** and **province of Austria** at the **same time**
  - Municipality in the legal form „**City Statut**“
  - **23 districts** (municipalitities)
  - **Population**: ~**1,87 Mio.** (as at 1.1.2017)
  - **Area**: ~**415 km²**
  - **GDP** (2015): ~**86,5 Bn. €**
  - 2016: **Revenue ~22,4 Bn. €** - **Spending ~21,4 Bn. €**
- Digitization
  - since **March 2011 Smart City Wien** initiative
  - since **September 2014** positioning **DigitalCity.Wien** (Digital ICT Metropolis/Digital Expertise of Smart City Wien)
  - **since 2016 innovation boost** of **ICT** in administration (Blockchain Open Government Data, „Sag‘s Wien“ App, etc.)
- Information- and communication technologie (ICT)
  - **3** key **ICT service providers** with **ISO/IEC 27001 certifications**
  - **ICT** infrastructure **consolidiation project** until **2019**
  - ~85.000 users, ~5.000 servers, ~5.380 databases, ~114.000 workstation devices, ~1.000 employees

City of Vienna Court of Audit

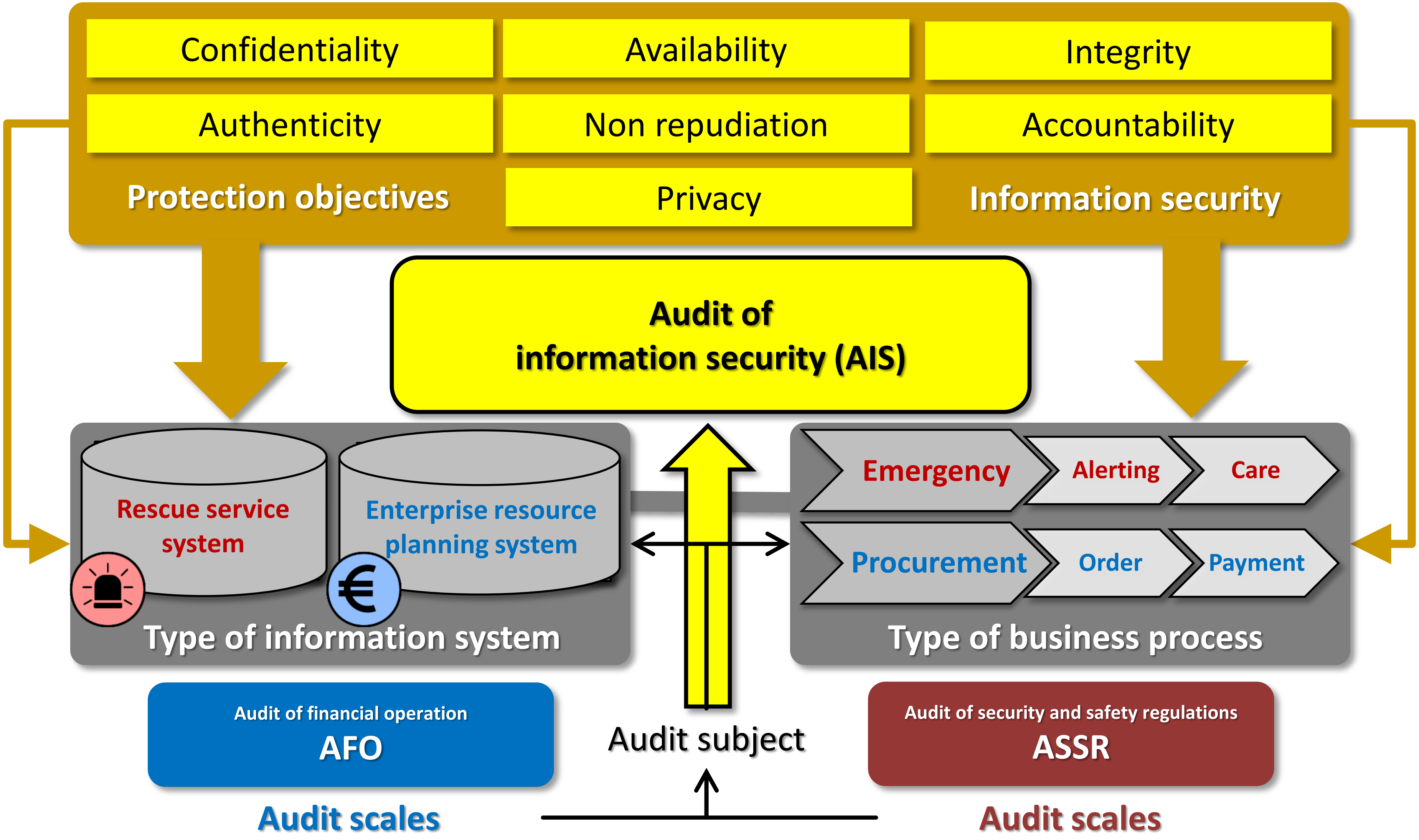
Palais Obentraut, Building City of Vienna Court of Audit.
Logo City of Vienna Audit Department

- History
  - Founded **1st of June 1920**, **City of Vienna Audit Department**
  - Between 1939-1945, Audit Office
  - Since **1st of January 2014**, **City of Vienna Court of Audit**
- Legal basis
  - **Vienna city constitution**, **audit of financial operation (AFO)**
  - In the year **1977** the regional assembly passed an **annex** to the **Vienna City constitution** which covered the **audit of security and safety regulations (ASSR)** (uniqueness of the court of audits and audit departments of Austria)**.** This was due to the collapse of a major bridge crossing the danube river „Reichsbrücke“.
- Mission
  - **Autonomous** and **independent audit institution** with a total of 92 staff members (69 employees in the audit services)
  - **Audit of financial operation (AFO)** of the underlying financial volume of the municipal departments, enterprises and the investments as well as the institutions which receive financial provisions from the City of Vienna
  - **Audit of security and safety regulations (ASSR)** at the municipality in question to the safety of human life or the safety of human health in accordance to the authority assignements, infrastructure and facilities

Approach audit domain information security



Value audit domain information security



Confidentiality

Availability

Integrity

Authenticity

Non repudiation

Accountability

Protection objectives

Privacy

Information security

Audit of information security (AIS)

Rescue service system

Enterprise resource planning system

Type of information system

Emergency

Alerting

Care

Procurement

Order

Payment

Type of business process

Audit of financial operation

AFO

Audit subject

Audit of security and safety regulations

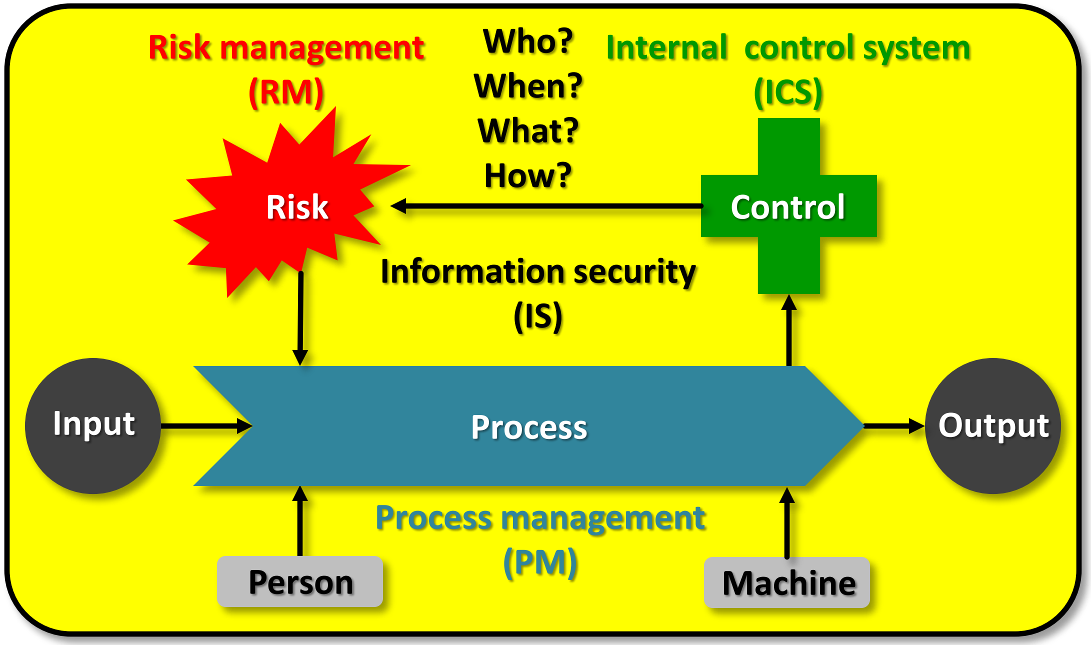
ASSR

Audit scales

Audit scales

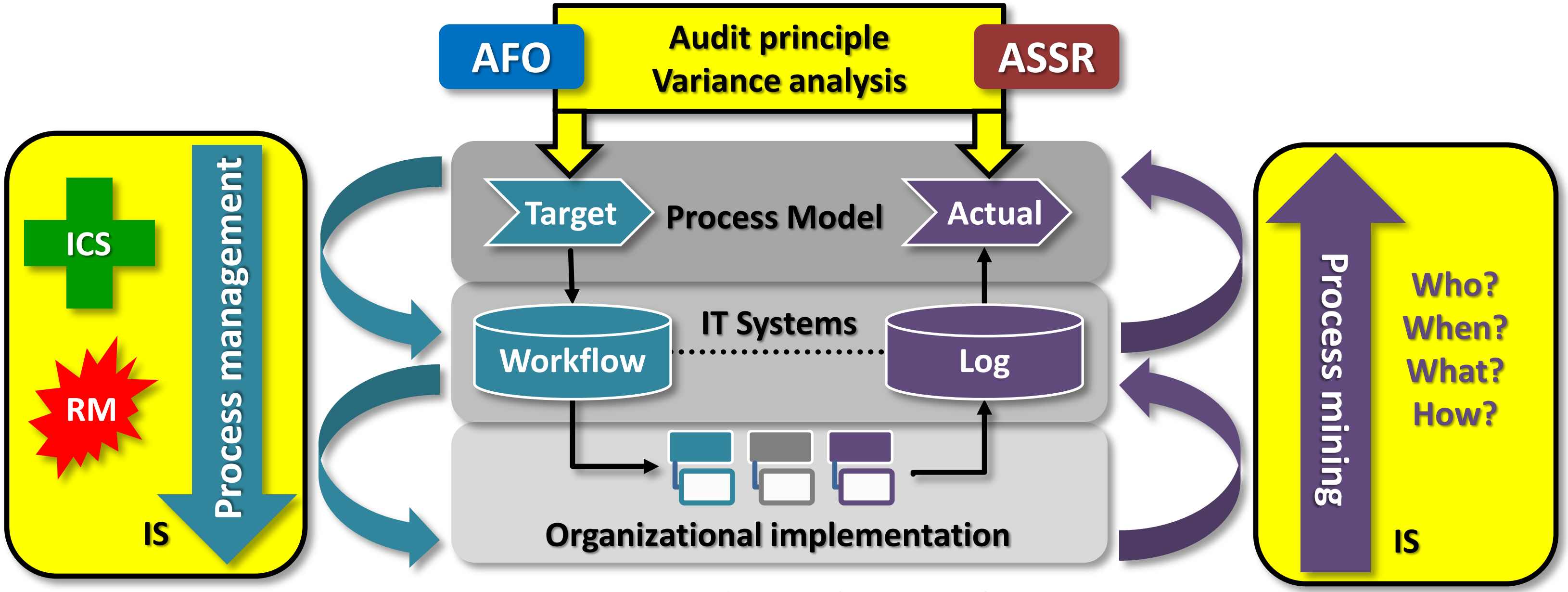
Areas of risk, core subjects audit domain information security

- **Areas of risk** corresponding to the questions of the audit themes with the relevant **case topics** from the known **regulations of the ICT branch** (ISO/IEC 2700x Serie, BSI-Standard, IT-Basic Protection, ITIL, COBIT, etc.)
- targeted **focus** to the following **core subjects/context**:



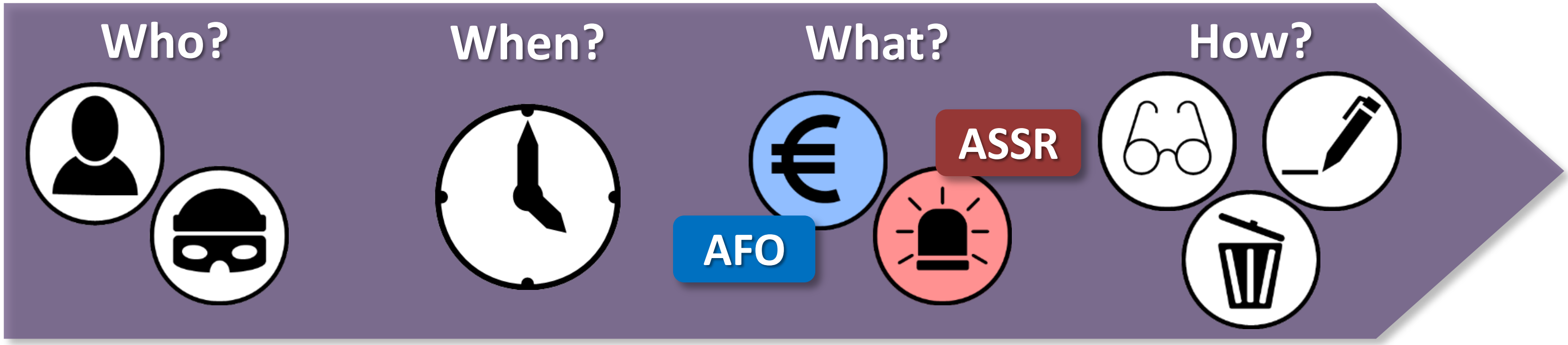
Methods audit domain information security

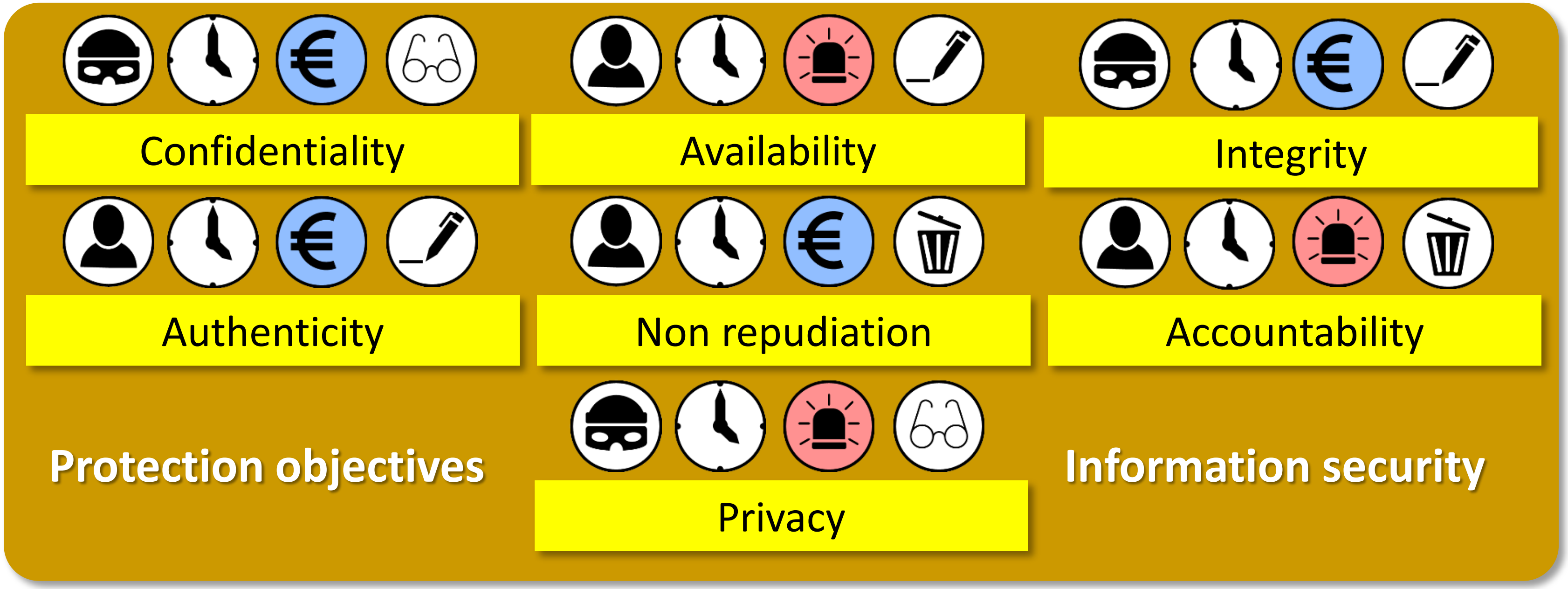
- Generally the **use** of **audit permission/roles** and **audit features** of the related **information systems** to be audited
- Generally the **extraction/evaluation** of the particular **raw data** directly from the underlying **IT systems** by the **ICT service provider**, not by the user (mostly the audited one)
- **Application/development** data analysis method **process mining**



Methods audit domain information security

Process mining





Organization
audit domain information security

- **Specialist division IT audits** with **expert knowledge** of 3 persons (not exclusively discrete unit of organization but clustered knowledge competence)
  - **Participation** in the case of **certain questions** to the respective audit subjects
  - **Selection** and **execution** of **independent IT audits**
  - **Observation/development/allocation** of appropiate **methods** and **tools** (e.g. MS Excel® with relevant plug-ins, survey software, etc.)
  - **Allocation** of **IT knowledge** in the **intranet** of the City of Vienna Court of Audit
- **Challenges**
  - **Basic digital skill** and **know-how** of **the audit staff**
  - **Expertise of data managemen**t (selection, data structure, (extract/export, analysis, evaluation, interpretation, presentation)
  - **Continuous practice** and **enhancement** of the ability and the knowledge in association to the rapid technological evolution
  - **Problem of expertise** and **recruitment** of **IT staff** with the **job profiles „business informatics“**, **„expert in information security“** and **„data analyst“** in **audit institutions**

Impact audit domain information Security

- **Effectiveness** of the **protection objectives** in **information systems**
- About the **audit** of **process** increase of the **practical relevance** and thus of the **awareness** and the **effect** in particular
  - of **permissions/roles (who?)**
  - of **efficiency** and **effectiveness** (**throughput times, RM, ICS** and **process steps** – **when?**, **what?** and **how?**)
  - on **data structuring required for verification** in the respective **information systems**
    (e.g. ***.XES event data format** in **process mining**)

Examples

audit domain information security

- **Process analysis (process mining)** during the audit of the **IT service management** of the ICT service provider of the City of Vienna (2016)
- Audit of the **regulations of ICT security of external customers** of the ICT service provider of the City of Vienna (2015)
- **Permissions/roles** at
  - the audit of the **electronic claim application** of the City of Vienna (2016)
  - the audit of the **preparation of the financial account on SAP basis of the City of Vienna** (2014)
- **Current audits** (2017 - 2018)
  - **Information security** and **process analysis (process mining)** related to the management/use of access tokens (permissions) as well as the electronic process of issuing a government document in school management software
  - **Process analysis (process mining)** in the SAP procurement process of ICT hardware and software

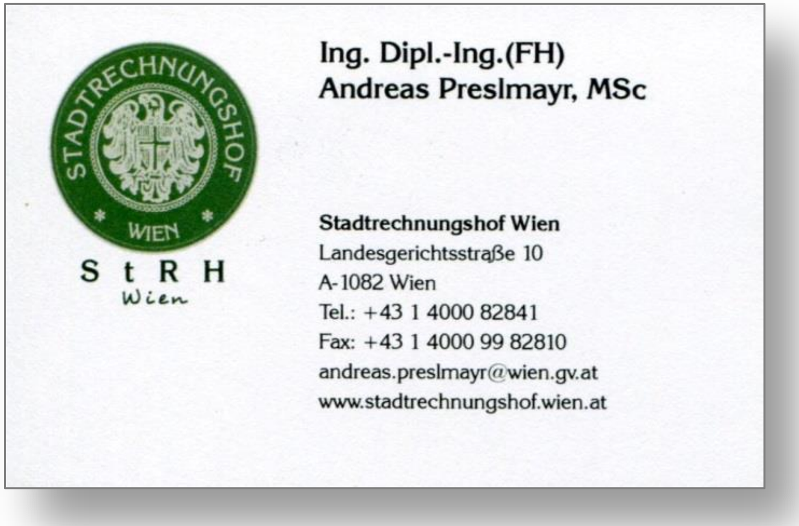
Experience
audit domain information security

Challenges

- Rapid **improvement** of the **state of art** in **information security** compared to the software applications in operation (also due to the **continuously increasing known security problems**)
- Approach of "**Security by Design**" in the context of software developments
- **Implementation** of **audit permission/roles** and **audit features** in the respective **software**
- Underlying **data structures** and **evaluation methods** for data analysis of **process mining** are only **very limited available**
- **Expenditure** (time and money) of the ICT service providers for the **development** and **evaluation** of certain **data structures** for the data analysis of the **process mining** for inspection of audit institutions are **not planned**
- **Growth** of the use of **ICT systems** and the associated **rapid growth** of the **data volumes generated therein**

References, resources, inquiries

- **Homepage City of Vienna Court of Audit**
  (http://www.stadtrechnungshof.wien.at/)
- **Vienna in figures**
  (https://www.wien.gv.at/statistik/pdf/viennainfigures-2017.pdf)
- **Smart City Wien**
  (https://smartcity.wien.gv.at/site/en/)
- **DigitalCity.Wien**
  (https://digitalcity.wien/)
- **Prozess Mining Manifest**
  (http://www.win.tue.nl/ieeetfpm/downloads/Process%20Mining%20Manifesto.pdf)



S t R H
Wien

Ing. Dipl.-Ing.(FH)
Andreas Preslmayr, MSc

Stadtrechnungshof Wien
Landesgerichtsstraße 10
A-1082 Wien
Tel.: +43 1 4000 82841
Fax: +43 1 4000 99 82810
andreas.preslmayr@wien.gv.at
www.stadtrechnungshof.wien.at

Thank you for your attention!