



R
H



**Rechnungshof
Österreich**

Unabhängig und objektiv für Sie.

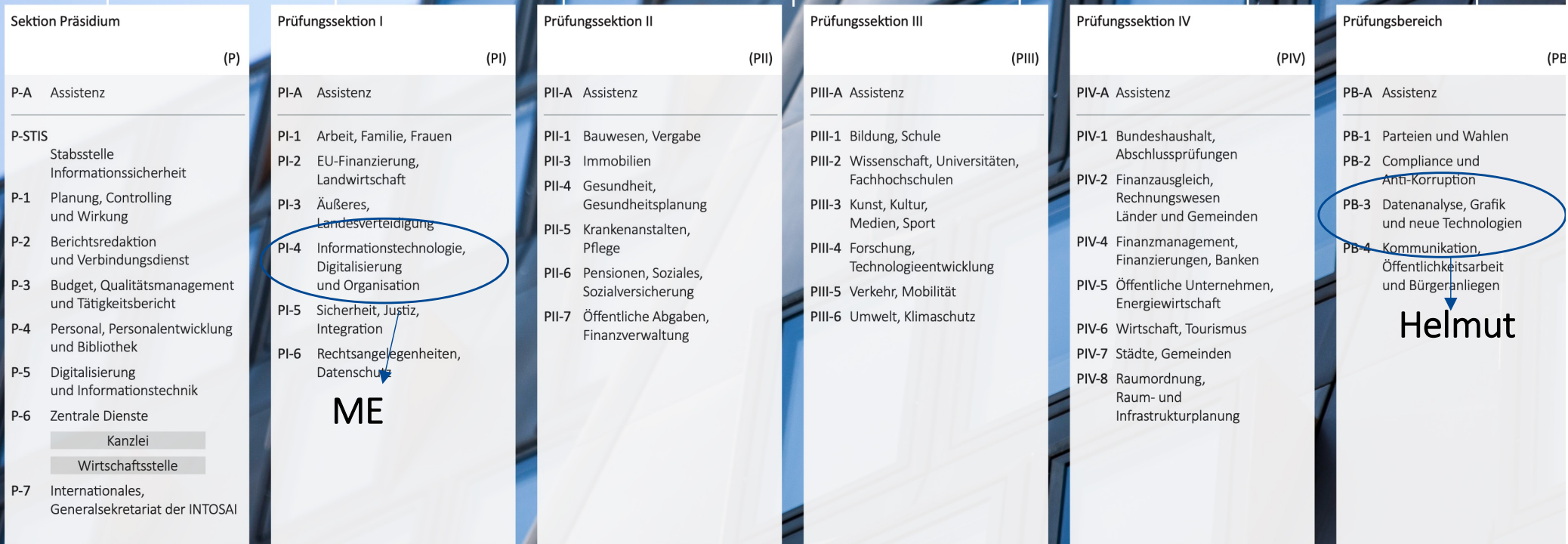
Recent IT-Audits of the Austrian Court of Audit

Andreas Mayrbäurl

PRÄSIDENTIN

Büro der Präsidentin BP

Stabsstelle Interne Revision ST-IR



ME

Helmut

We audit

more than 5,700 legal entities are subject to the ACA's audits



Federation/provinces/
municipalities



Foundations/
funds



Social insurance
providers



Hospitals



Businesses



Chambers



Our audit criteria

Legality

Compliance

Economy

Efficiency

Effectiveness

Recent IT-Audits

- + **IT-Security Audits** Federal level (2024), **Province Carinthia (2024)**, City of Vienna (2026)
- + Coordination of Cyber-Security (2022)
- + **AI in the federal Administration (2025)**
- + Digitalisation fund for the federal Administration (not published yet)
- + Switch from the citizen card/mobile phone signature to the electronic identity card (E-ID) (2023) -> Follow up – Audit (not published yet)

AI in the federal administration

Audit Topics:

- Framework
(EU, federal laws, strategies)
- Budget, personnel
- Internal ministry regulations
- AI applications (overview)

Audit period:

2021–2023 (in some cases until June 2024)



AI strategies und guidelines

National AI Strategy from 2021

- Strategic goals: trustworthy AI, innovation hub, competitiveness
- Measures specified in varying degrees of detail
- Responsibilities for implementation not assigned
- No information on budget

<https://www.ki-strategie.at/>

Ethics guidelines of the Federal Ministry of the Interior for public service 2023/24

- Information and checklist on trustworthy AI
- But: Non-binding

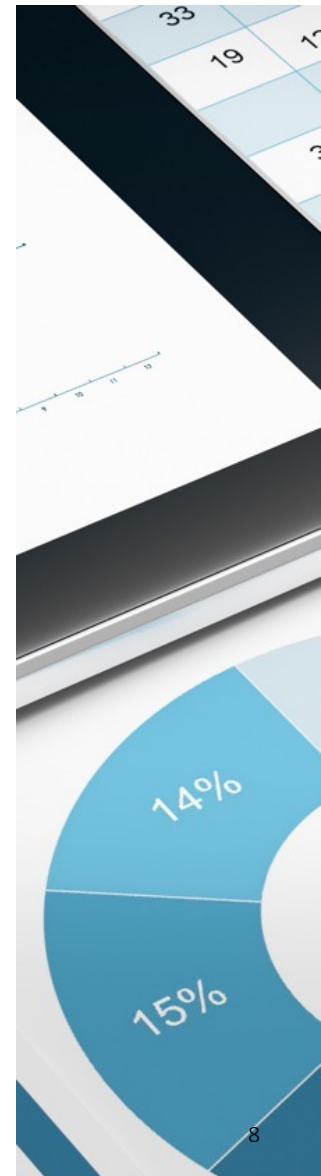
<https://oeffentlicherdienst.gv.at/verwaltungsinnovation/digitale-verwaltung/praxisleitfaden-digitale-verwaltung-und-ethik/>



AI applications in the ministries

- 20 application descriptions for 35 AI applications
- e.g., translation, predictive analysis, risk assessment, data evaluation, software development, image processing

Assessment criteria ACA	20 application descriptions
Consideration of ethics guidelines	8
AI-specific risk classification	1
AI-specific development or life cycle model	5
AI-specific standards or certifications	0



Main Recommendations 1

National coordination

- + Requirements of the AI Act, e.g., risk and quality management, documentation and transparency obligations
- + Uniform interpretation, classification scheme
- + Fulfillment of tasks by AI authorities, coordination
- + Intensify exchange with the federal states

=> New “AI coordination” competence created for the Federal Chancellery

Main Recommendations 2

Individual departments

- + Develop internal departmental strategies for the use of AI
- + Supplemental department-specific data strategies
- + Regulations for employees on how to deal with AI
- + Mandatory awareness training
- + Training and further education of AI-specific personnel
- + Implementation of measures from the national AI strategy
- + Contribution to nationwide documentation of the use of AI

Main Recommendations 3

AI applications

- + Development of a standard procedure for project planning and implementation including AI-specific criteria (risk classification, certifications, life cycle models, trustworthy)
- + Specifications for the (internal or commissioned) development of AI applications

Costs

- + Separate budget for AI not always possible, but separate specification of the share of the total budget is useful

Recent IT-Audits

- + IT-Security Audits Federal level (2024), Province Carinthia (2024), City of Vienna (2026)
- + Coordination of Cyber-Security (2022)
- + **AI in the federal Administration (2025)**
- + Digitalisation fund for the federal Administration (not published yet)
- + Switch from the citizen card/mobile phone signature to the electronic identity card (E-ID) (2023) -> Follow up – Audit (not published yet)

IT-Security Audits (Province of Carinthia)

Audit Topics:

- Fundamentals of IT security
- IT security organization
- IT security for staff and teleworking
- Technical measures to increase IT security
- **Security incident in 2022:
Cyberattack on the province of
Carinthia**
- Cooperation with other stakeholders

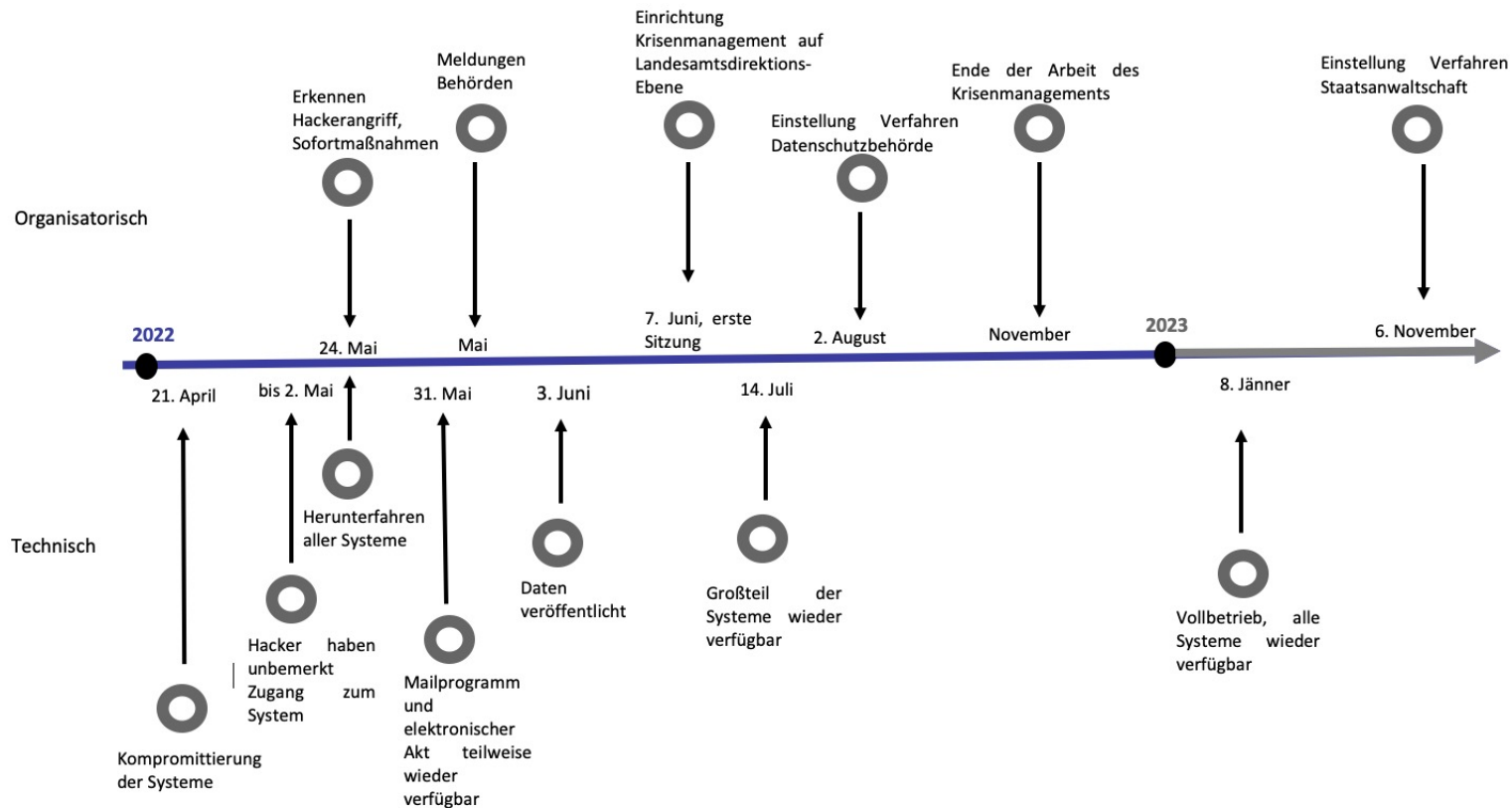
Audit period: 2020–2023



IT-Security Audits (Province of Carinthia)



Security Incident



Data leakage due to the security incident

Estimated volume approx. 250 GB:

- Personal data (residence permits, passports, identity cards, etc.)
- Data on procedures (awards, invitations, etc.)
- Personal files of government members and state employees

Crises Management

- The province of Carinthia has had a “Crisis Management Guide” since 2017
-> No update has been made by the provincial director.
- The IT department took over IT crisis management in coordination with the provincial directorate for presidential and communication affairs as soon as the attack became known
- After the stolen data was published on June 3, 2022, an IT crisis team and cyber response group were set up at the level of the Provincial Office to deal with the crisis
- All necessary information and notifications were provided (authorities, population, administration, and employees)

Immediate and recovery measures

- Establishment of a rapid response team (quickly available task force)
- Setup of a new firewall
- Implementation of DDoS protection

(Re-)Availability of IT systems after the Cyber-Attack:

May 24, 2022	Orderly shutdown of all systems
May 29, 2022	First restorations successful
May 31, 2022	Mail system available again
July 14, 2022	Most systems available again
July 26, 2022	Internet access restored
November 22, 2022	Systems available again (except for thin clients)
January 8, 2023	Full operation

Costs of measures related to the IT security incident

	2022	2023	2024	2025	2022 bis 2025
	In Tsd. EUR				
Rapid Response Service	195,00	–	–	–	195,00
Firewall	280,00	10,00	10,00	5,00	305,00
Sofortmaßnahmen Wartungsvertrag <i>{pd⁷⁹}</i>	228,00	228,00	228,00	228,00	912,00
Stunden Unterstützungspool <i>{pd⁸⁰}</i>	275,50	–	–	–	275,50
Cyber Defense Center	180,00	351,50	340,50	340,50	1.212,50
Maßnahmen aus Forensik Bericht und Ergebnisse der geplanten Überprüfungen – Schätzung	250,00	150,00	100,00	50,00	550,00
SIEM / SOC – Schätzung	–	400,00	200,00	200,00	800,00
Security Management System (Modell + Lizenzen) <i>{pd⁸¹}</i>	13,00	7,00	7,00	5,50	32,50
Weitere Maßnahmen	648,50	286,50	297,50	237,50	1.470,00
Summe	2.070,00	1.433,00	1.183,00	1.066,50	5.752,50

¹ Kostenschätzung vom 18. Juli 2022



R
H



**Rechnungshof
Österreich**

Unabhängig und objektiv für Sie.

Thank you for your attention

#youcancountonus

www.rechnungshof.gv.at

mayrbaeurl@rechnungshof.gv.at

 [FB facebook/RechnungshofAT](https://www.facebook.com/RechnungshofAT)

 [@rechnungshofat](https://www.instagram.com/rechnungshofat)