LANDES
RECHNUNGSHOF
BRANDENBURG

EURORAI-Seminar
“Conducting audits on cyber- and information security”
19th April 2018

Audit of IT security
- from Niche to Necessity -

Thomas Kersting

Head of Audit Division of the Court of Audit of Brandenburg

LANDES RECHNUNGSHOF BRANDENBURG

Contents

1. IT security in the news in Brandenburg
2. Basic conditions
3. Audit standards of the Courts of Audit (state and federal)
4. Audit capacity
5. Findings of the Court of Audit Brandenburg
6. Limitations for auditing the IT security
7. Conclusions for auditing IT security conducted by Courts of Audit

LANDES RECHNUNGSHOF BRANDENBURG

1 - IT security in Brandenburg in the news

- Public administration computers vulnerable to Internet attacks

  The number of serious security incidents that could not be prevented by automated defence systems has increased by more than 200% over the past five years - a total of 320 cyber attacks from 2013 to 2017.

- "Web View" Data Leak

  Police officers posted internal information about crimes in a large social network and also forwarded them to the press.

LANDES RECHNUNGSHOF BRANDENBURG

2 – Basic conditions

Conditions for the digitalisation of public administration

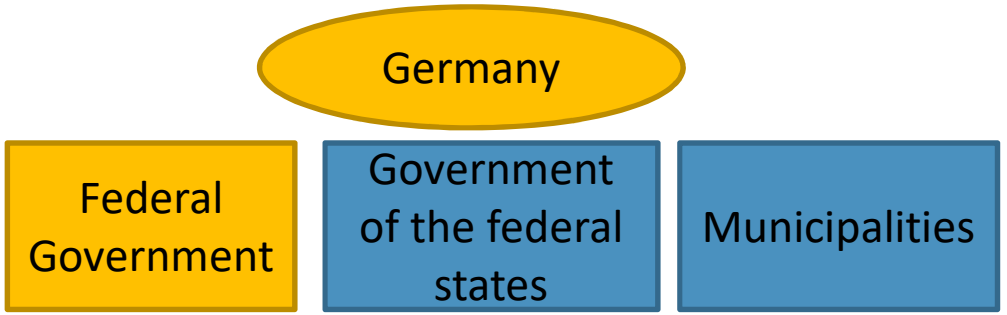
- Performance assurance through German Basic Law
- Rule of law
- Integrity of the digital public administration
- Digital information systems constitute critical infrastructure
- Risk of financial loss and loss of trust

at the same time

- Increase of IT support in public administration
- Extensive internal and external networking
- Efficient administration is location advantage

LANDES RECHNUNGSHOF BRANDENBURG

2 – Basic conditions



Variety of IT networks

=> No obligation to comply with
uniform minimum IT safety standards

Legal problem:
General prohibition of shared administration (state/federal states)

2 – Basic conditions

Constitutionally enforced cooperation

versus

(state) contractual cooperation

⇒ Article 91c of the German Basic Law

- simplifies existing IT-bodies and decision-making processes
- secures electronic communication and linkage between the federal, state and local authorities, free of media disruptions
- exclusive legislative competence of the Federal Government for a network of connections between the federal and state administrations

2 – Basic conditions

Source: Internet presentation pages of the IT-Planning Board, tasks of the IT-Planning Board (Germany has established a central body for the coordination and promotion of IT and e-government across all three tiers of government - local, state and federal).

3 - Audit standards of the Courts of Audit (state and federal)

Minimum requirements of the courts of audit of the Federation and the Federal States for the use of information technology ("Information and Communication Minimum Requirements")

- Essential fields of action for IT audits
- Common and transparent audit standards based on audit findings of the courts of audit
- Infrastructural, organisational, human and technical information security measures

LANDES RECHNUNGSHOF BRANDENBURG

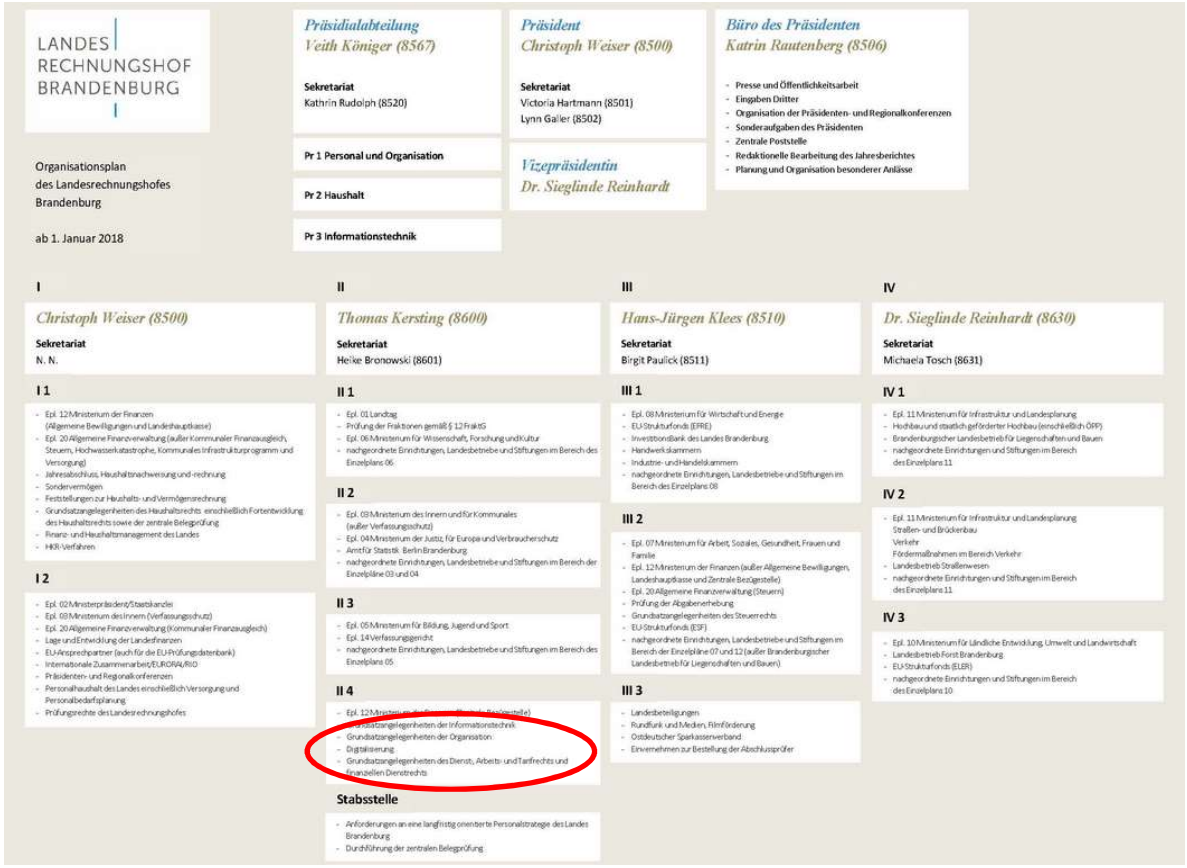
3 - Audit standards of the Courts of Audit (state and federal)

Paper of courts of audit offices information security management

- IT security is the responsibility of the management
- Integration of IT security in all organisational processes
- Appropriate / Centralized IT security management system (ISMS)
- Continuous monitoring and improvement of the effectiveness and implementation of the ISMS
- IT security officer independent of the operational IT management
- Adequately qualified IT security management personnel
- IT protection requirement / risk analysis
- Compliance with the principles of efficiency and economy
- Audits or revisions

LANDES RECHNUNGSHOF BRANDENBURG

4 - Audit capacity



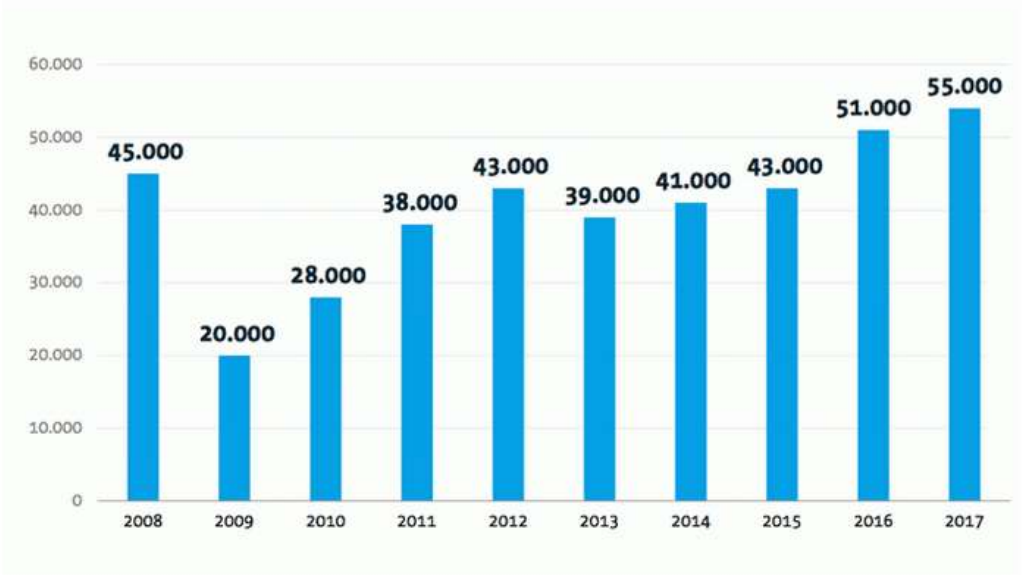
Audit of IT security
- from Niche to Necessity -

LANDES RECHNUNGSHOF BRANDENBURG

4 - Audit capacity

Lack of skilled professionals: Bitkom estimates 55,000 vacancies for IT specialists

07.11.2017 12:20 Uhr – Andreas Wilkens vorlesen



Entwicklung der Zahl der offenen Stellen für IT-Fachkräfte seit 2008. (Bild: bitkom.org)

LANDES RECHNUNGSHOF BRANDENBURG

4 - Audit capacity

IT industry creates thousands of new jobs - and complains about massive shortage of skilled professionals

- 45,000 additional IT specialists employed in 2017
- Economic outlook very positive
- Historically strongest employment growth within one year
- In 2018, forecast of an additional 42,000 jobs

Article of 14 February 2018 - https://www.heise.de/newsticker/meldung/Bitkom-IT-Branche-schafft-tausende-neue-Arbeitsplaetze-und-beklagt-massiven-Fachkraeftemangel-3969322.html

LANDES RECHNUNGSHOF BRANDENBURG

5 - Findings of the Court of Audit Brandenburg (Examples from within the Department of Justice)

Failure to protect IT equipment and systems

- Fire loads and ignition sources
- Smoke alarms turned off
- Server room used as fitness room for employees

(2013)

Fire and Catastrophe Protection

- Protection of IT security concept created BUT
- not implemented in essential parts
  - no emergency measures concept
  - no fire detectors in the server room
  - Access to the server room open - it should draw in cold air

(2014)

LANDES RECHNUNGSHOF BRANDENBURG

5 - Findings of the Court of Audit Brandenburg (Example from within the Department of Justice)

- Local server
  - unlocked, accessible to anyone
  - former sanitary facility

However:

- Supervisory authority intends to allow those conditions for now
- Controversial discussion in state parliament
- final solution still pending

(2016)

LANDES RECHNUNGSHOF BRANDENBURG

5 - Findings of the Court of Audit Brandenburg (Example State Data Centre)

State data centre with considerable risk of default

through lack of:

- emergency management, risk analysis, protective measures
- stationary fire extinguishing system
- sufficient power supply
- sufficient air conditioning

No strict separation of test, integration and production environment

- ➢ System failure in several departments

Simultaneous use as training facility

- ➢ Risk of unauthorised access

LANDES RECHNUNGSHOF BRANDENBURG

5 - Findings of the Court of Audit Brandenburg (Example State Data Centre)

LANDES RECHNUNGSHOF BRANDENBURG

6 - Limitations for auditing IT security

Limitations

- Ensuring correct implementation of firewall filter rules, routing tables, proof that network topology complies with the concepts / specifications
- Checking implemented VPN solutions
- Testing the secure hardening of servers
- Examination of all specialized applications for vulnerability from internal and external networks
- Validation of emergency concepts in real emergency situations

LANDES RECHNUNGSHOF BRANDENBURG

7 - Conclusions for auditing IT security conducted by courts of audit

- Increase resources
- Staff training digital proficiency
- Recruitment of IT professionals
- External consultancy
- Cooperation between courts of audit in order to achieve synergy
- Ensure internal IT security
  - comply with standards, if necessary. external support
  - permanent internal awareness of “good cyber hygiene”