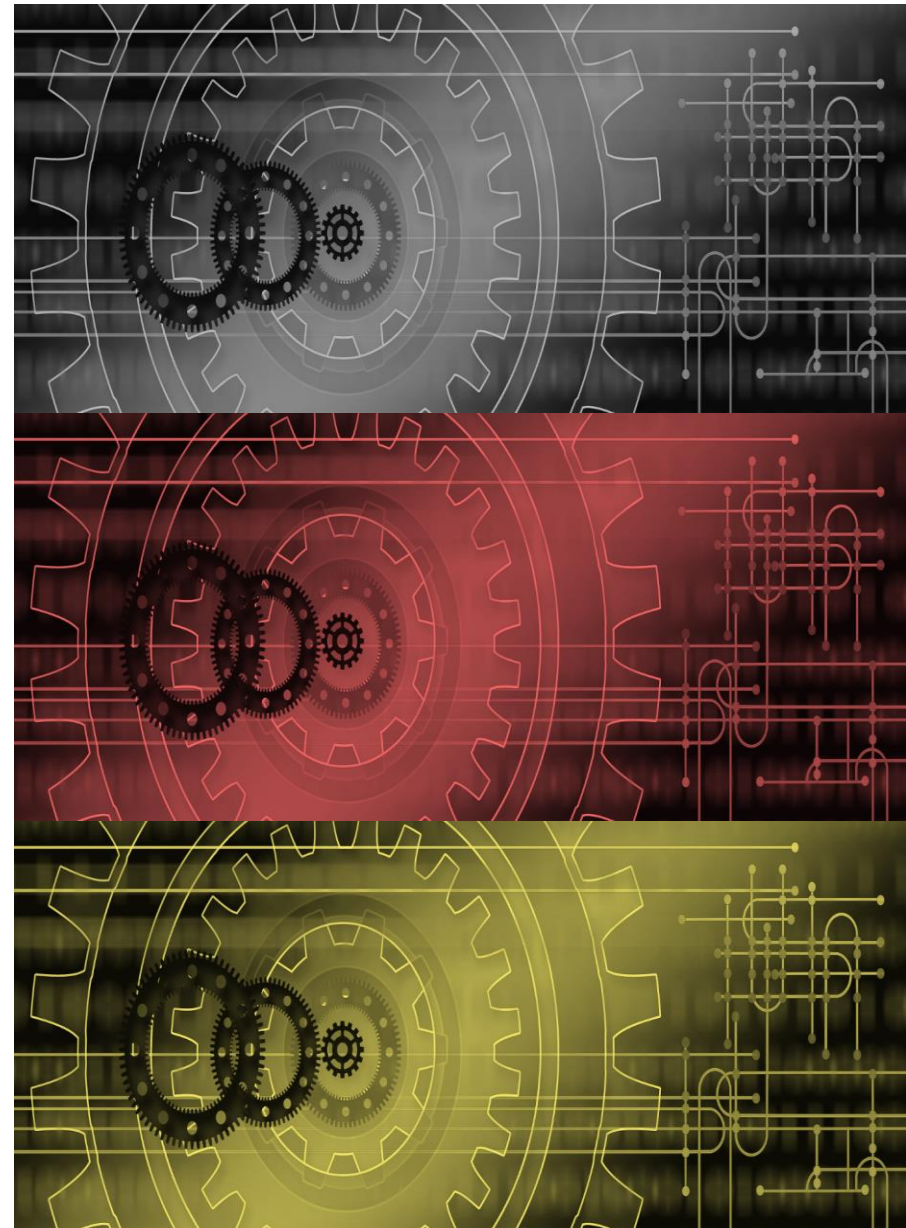
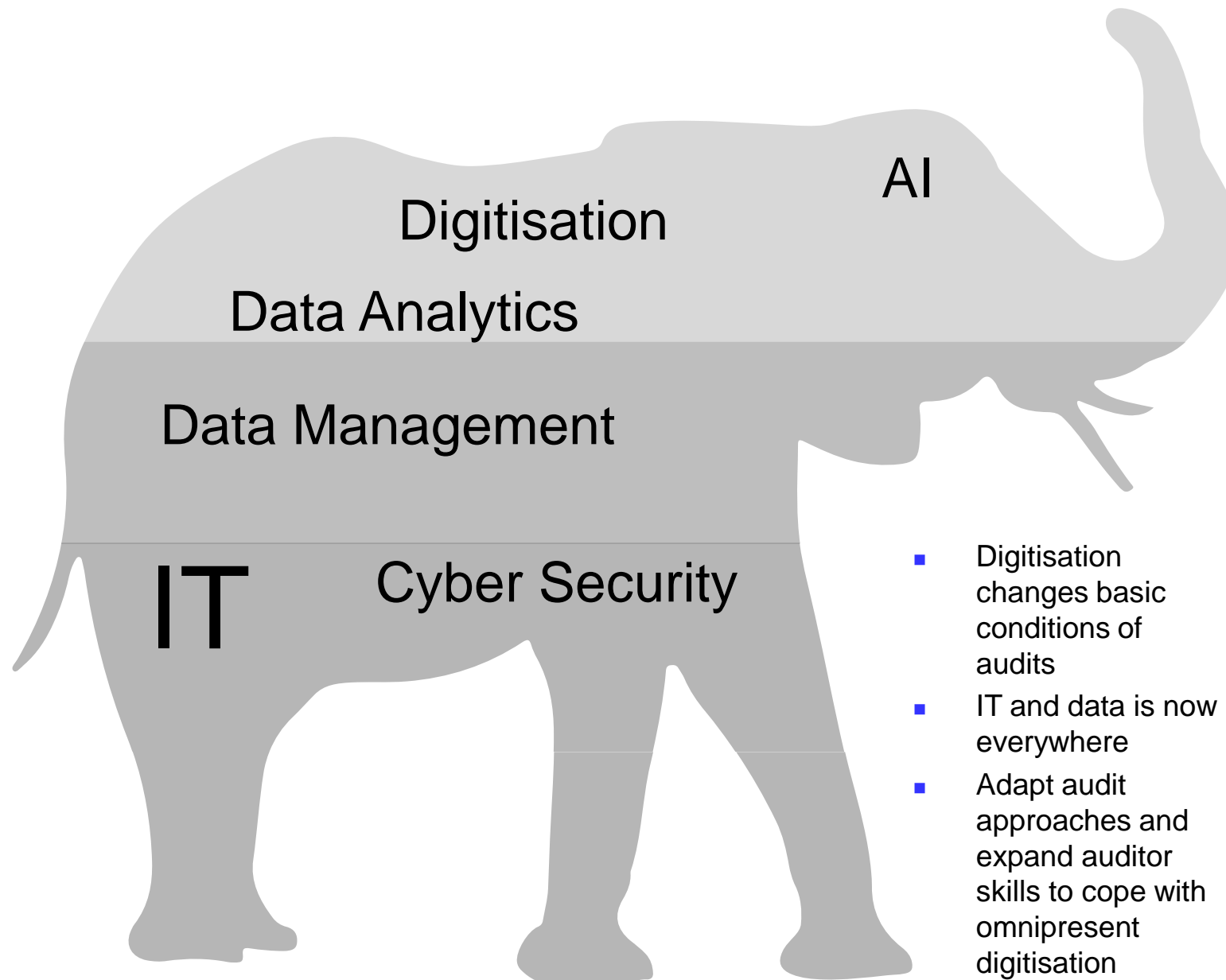


# Comprehensive auditing

Challenges integrating IT into  
„regular“ audits



# Today, audits must address IT and D<sup>3</sup>



- Digitisation changes basic conditions of audits
- IT and data is now everywhere
- Adapt audit approaches and expand auditor skills to cope with omnipresent digitisation





## HRM

- Provision of IT and (AI)D<sup>3</sup> generalists
- Provision of IT and (AI)D<sup>3</sup> specialists
- Temporary provision of specific types of specialists
- Provision of IT and (AI)D<sup>3</sup> auditors with domain knowledge
- Use of multiple sourcing strategies
- Providing specialised IT and (AI)D<sup>3</sup> education for auditors
- Adapting management culture to cope with IT and (AI)D<sup>3</sup> experts



## Technology

- Disclose impact of technology change on digitisation of business processes
- Awareness of fast pace of the IT and D<sup>3</sup> market development
- Examine dependencies of authorities from suppliers
- Lay out a strategy on how to handle the large range of highly complex products found in audits
- Visualise the multiple technical layers of the infrastructure
- Provide case dependent highly specialised experts for audits



## Interdisciplinary

- Dissolve boundaries between audits of IT, D<sup>3</sup> and business
- Focus on both IT and D<sup>3</sup> as well as on business related issues
- Encourage cooperation of IT, D<sup>3</sup> and domain experts
- Teach IT and D<sup>3</sup> specialists domain knowledge
- Teach domain experts IT and D<sup>3</sup> knowledge
- Form joint audits to gain expertise and experience in cross domain cooperation



## Auditee

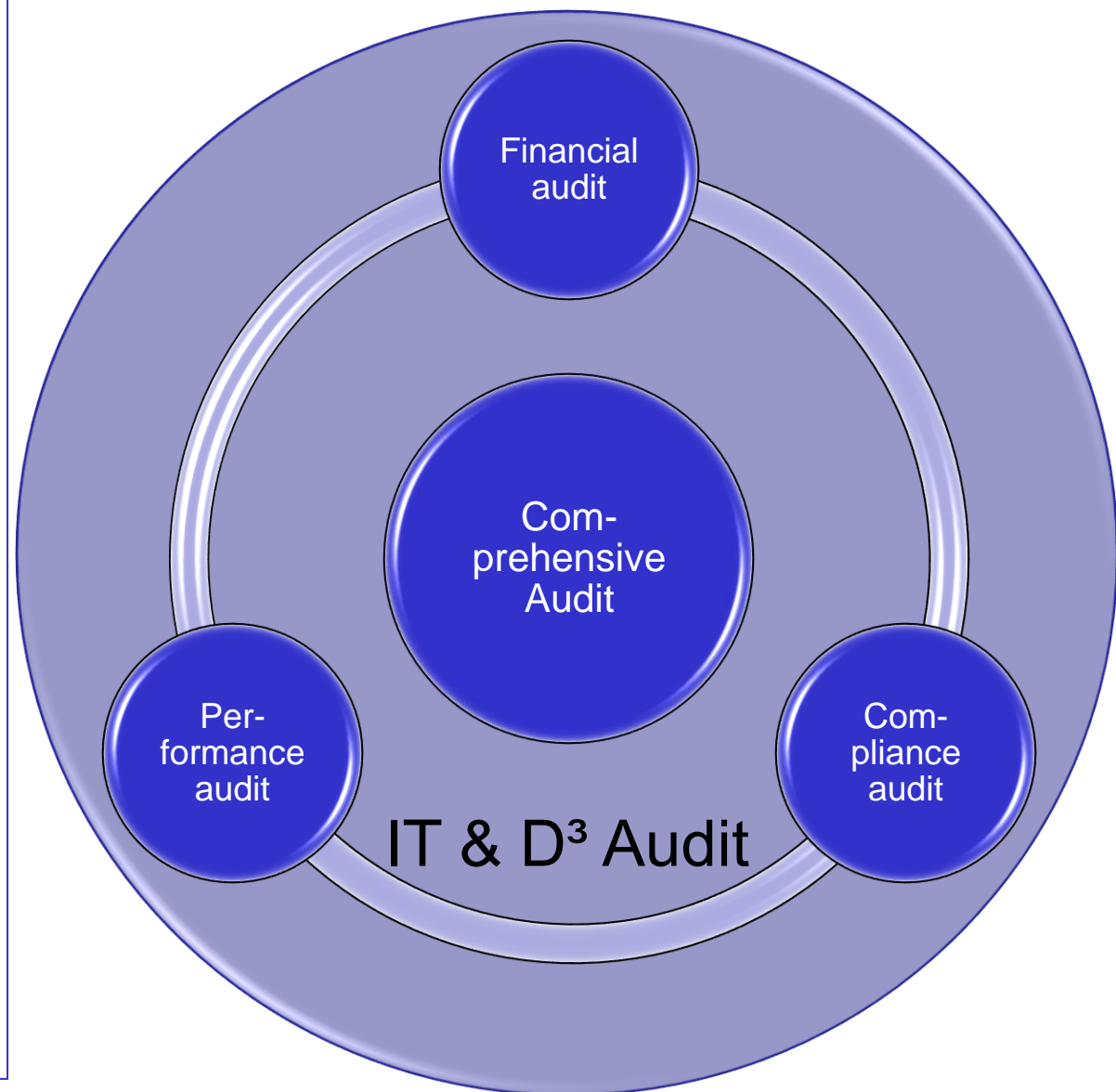
- Organisation of SAI able to handle different federal authorities
- Take precautions for the auditees lack of personnel with the required knowledge to explain facts and figures to auditor
- Examine status, pace, means and objectives of an authority's digitisation
- Provide several audit approaches to match authority's situation
- Inform about dependencies between subject-specific business processes, IT infrastructure, IT systems, IT security etc.



## Communication

- Close language gap between domain and IT / D<sup>3</sup> experts
- Intensive communication on objectives, means and ends, shared interests etc. before starting joint audits
- Form an expert network to share knowledge and experience
- Define standards and guidelines for IT / AID<sup>3</sup> audits
- Establish a central entity to manage standards, guidelines and information on IT / AID<sup>3</sup> and declare which one to use.
- Ensure knowledge transfer from temporary experts

- The German SAI regularly follows a comprehensive approach to audit work.
- The auditors combine aspects of financial, compliance and performance audits.
- All audit information is used in such a way that a holistic assessment is possible.
- That way, all three types of audits supplement each other.
- Due to digitisation IT is a subject of most audits.



## Four forms of IT audits in the realm of civil and military administration



### Holistic IT audits

- Comprehensive audits related to IT, IT security and major digitisation projects
- Enterprise governance of Information and technology of an authority or an administration



### Specialised IT audits

- Use of a specific technology
- IT and cyber security
- Software development
- IT project management



### IT system audits

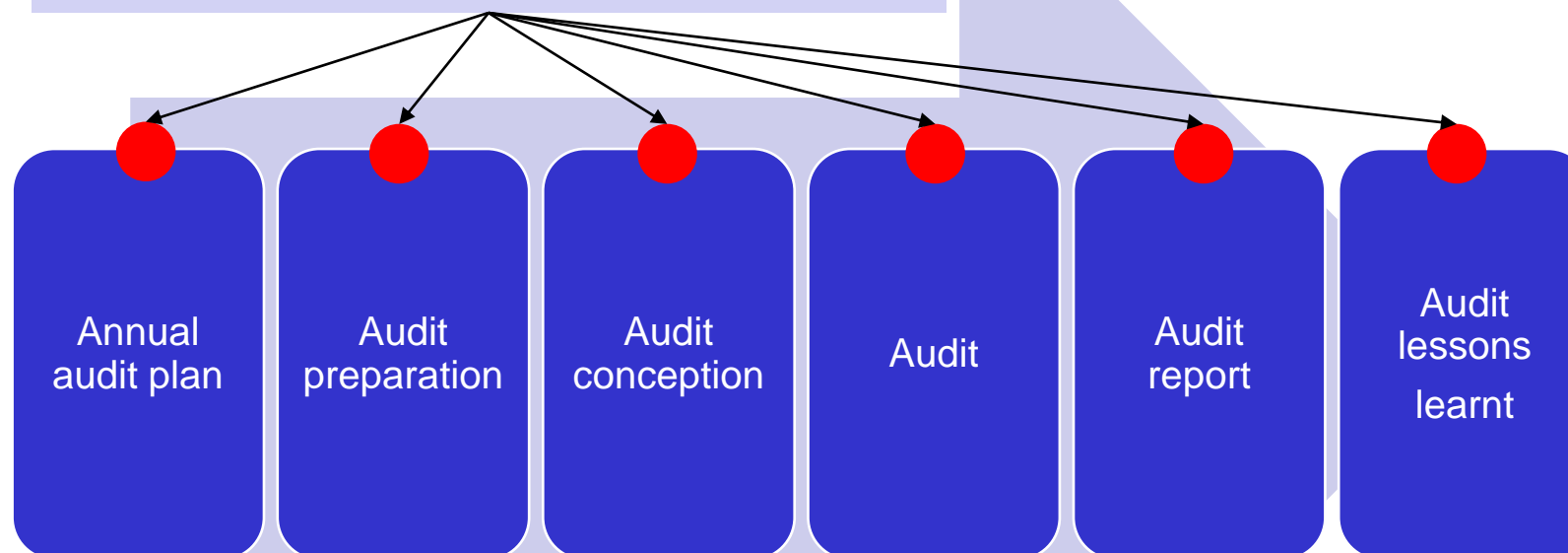
- for payment and accounting systems
- concerning regulatory and IT security issues



### Audits of IT aspects as part of

- subject, business domain or authority related comprehensive audits or
- for audits of the budgetary and economic management of authorities

## Intervention points for IT or AID<sup>3</sup> related audit aspects



Audit divisions inform each other about their risk oriented audit plans and coordinate them

Among other aspects, the audit units identify whether IT related questions are relevant for the audit project

The audit unit describes objectives and subjects to be audited as well as dependencies between audit projects. It analyses and defines in what way it has to examine IT.

Audit unit conducts the audit using the predefined procedures, tools and measures. For IT, it uses the IT audit manual which consists of numerous audit scripts.

Audit unit writes down the audit findings and reconciles findings with other audit units which may concern them because they touch their responsibility

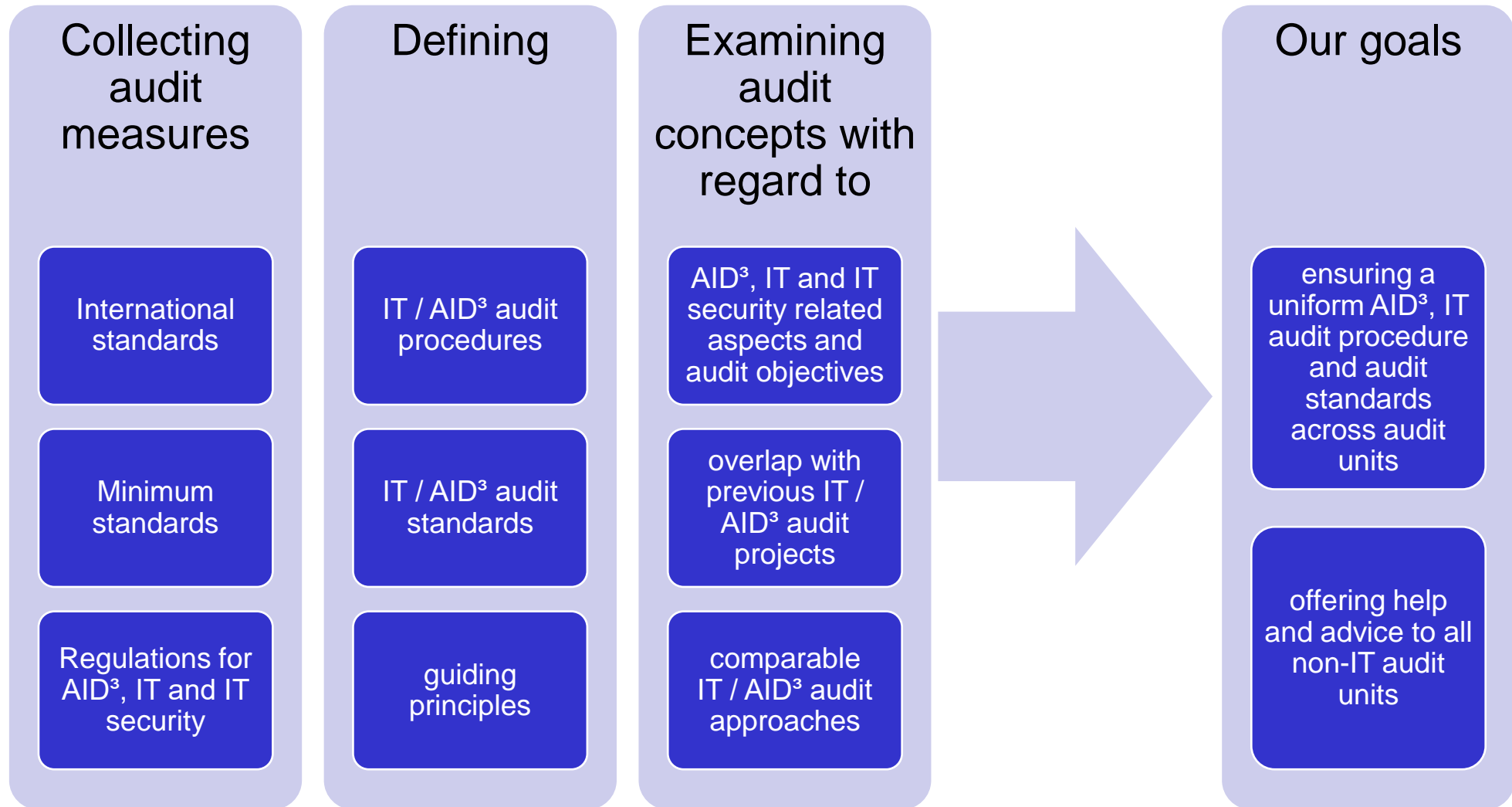
Audit results are examined concerning findings which are of general importance and can be used as role model for further audits



# Distribution of responsibilities

I	II	III	IV	V	VI	VII	VIII	IX
Corporate governance, constitutional bodies, EU 	Public building construction, environment, real estate, foreign affairs, development cooperation 	National economy, research, food safety, federal shareholdings, banking institutions 	Defence 	Transport, infrastructure 	Employment, social security, expenditure on staff 	Federal Chancellery, home affairs, building, privacy and data protection, cultural affairs, ITC, organisational management 	Federal Ministry of Finance, taxes, customs 	Public health, family, pensions, benefits to promote participation 
<b>I 1</b> Reporting, corporate governance, Public Accounts Committee	<b>II 1</b> Environment, nature conservation and nuclear safety	<b>III 1</b> Economy and energy, guarantees	<b>IV 1</b> Civillian branches, Federal Armed Forces (organisation/staff/budget)	<b>V 1</b> Transport and digital infrastructure	<b>VI 1</b> Federal Employment Agency, (organisation/staff/budget), employment and social security	<b>VII 1</b> Federal Chancellery, cultural affairs, internal security, intelligence services	<b>VIII 1</b> Federal Ministry of Finance, cross-cutting tax matters	<b>IX 1</b> Public health, statutory health insurance (financial and commercial management: benefits and portfolio)
<b>I 2</b> Federal finance, organisational management of the German SAI, financial rules and regulations, accounting standards, Budget Committee liaison, Federal Performance Commissioner support unit	<b>II 2</b> Foreign affairs, international organisations and institutions	<b>III 2</b> Education and research	<b>IV 2</b> Navy, equipment, information technology and in-service support	<b>V 2</b> Railway infrastructure	<b>VI 2</b> Pay and employment law, human resources of government departments and travel expenses	<b>VII 2</b> Home affairs, building and community, privacy and data protection	<b>VIII 2</b> Indirect taxes	<b>IX 2</b> Statutory pension benefits
<b>I 3</b> Office of Federal President, legislative bodies, European and international finances, EU matters	<b>II 3</b> Economic cooperation and development	<b>III 3</b> Food safety and agriculture	<b>IV 3</b> Cyber and information domain, information technology and communications of the Federal Armed Forces, joint support service	<b>V 3</b> Road works I	<b>VI 3</b> Jobseekers pay for a living	<b>VII 3</b> Digital policy, IT and network policy, digital radio and cross-government IT consolidation	<b>VIII 3</b> Direct taxes	<b>IX 3</b> Family, senior citizens, women and youth, social support grants, social compensation
<b>I 4</b> Federal investment aids granted to local governments	<b>II 4</b> Public building construction I	<b>III 4</b> Government shareholdings, public foundations, companies succeeding the traditional Post Office	<b>IV 4</b> Army, health service, defence vehicles, logistics	<b>V 4</b> Road works II	<b>VI 4</b> Employment promotion, wage compensation benefits and occupational integration assistance	<b>VII 4</b> Information technology and communications services, IT security	<b>VIII 4</b> Procedural tax law, Income Tax Act, child benefits	<b>IX 4</b> Social security accounting and cross-cutting issues, statutory health insurance (internal financial and commercial management), Federal Insurance Office
<b>I 5</b> Judiciary and consumer protection, Federal Constitutional Court, Federal Press Office, civic education	<b>II 5</b> Public building construction II	<b>III 5</b> Banking institutions, integrated financial services supervision, off-budget funds, federal debt, financial market stabilisation	<b>IV 5</b> Air Force, aircraft, Nato, pricing law	<b>V 5</b> Infrastructure projects, performance studies, public contract awarding regulations, federal trunk road management	<b>VI 5</b> Staffing expenditure, civil service law, pay and pensions, health care benefits	<b>VII 5</b> (Government) organisational management	<b>VIII 5</b> Tax and customs administration, financial controls of undeclared work	<b>IX 5</b> Farmers' social security scheme, industrial injuries insurance, benefits to promote participation
<b>I 6</b> Annual audit of the federal financial statements	<b>II 6</b> Federal buildings, organisations succeeding Treuhandaanstalt, public building construction III, management of federal real estate, departmental governance, general administrative expenditure	<b>III 6</b> Deutsche Bahn AG, Federal Railway Assets Fund	Four specialised IT audit units: <b>IV 4: IT in the DoD</b> <b>I 6: IT systems audits for payment and accounting</b> <b>VII 3: cross-government digitisation and IT consolidation</b> <b>VII 4: IT and cyber security, general aspects of IT</b>			<b>VII 6</b> Refugees and asylum seekers	All audit units are responsible for auditing aspects of IT as part of their topic or authority related audits Some audit units have their own IT experts.	

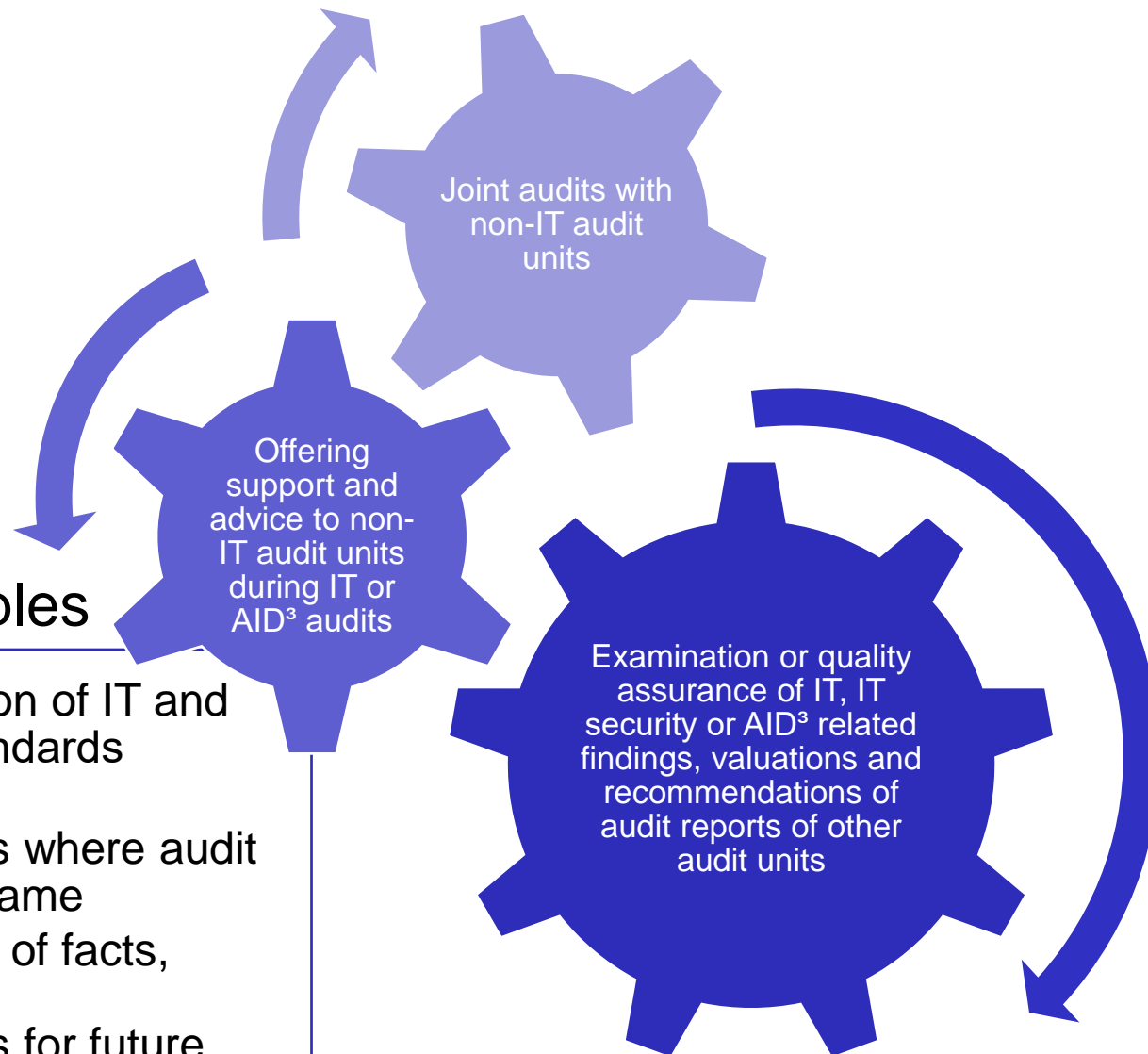
# Role of VII 3/4 w.r.t. all IT or AID<sup>3</sup> audits





## Guiding principles

- Uniform application of IT and AID<sup>3</sup> auditing standards
- Consistency of recommendations where audit findings are the same
- Central collection of facts, valuations and recommendations for future audits



## Enterprise governance of information and technology (EGIT) → COBIT 2019

- EGIT is concerned with value delivery (economic value added) from digital transformation and the mitigation of risk that results from digital transformation
- no silver bullet (or ideal way) to design, implement and maintain effective EGIT within an authority

## Our goal: Creating a common understanding of both IT and non-IT units on the basis of EGIT

- Building a generic model for EGIT in authorities based on the COBIT 2019 framework
  - Using the same language, terms and definitions
  - Designing a set of KPIs for measurement and evaluation
- The generic model must be adapted to each auditee

Thank you for listening