The IT Center at RWTH Aachen University

Publicator using openai/gpt-oss-120b

Contents

The IT Center at RWTH Aachen University

Abstract: The IT Center at RWTH Aachen University serves as a pivotal enabler of the institution's research, teaching, and administrative missions. This paper situates the Center within the broader academic ecosystem of RWTH Aachen, tracing its historical evolution and the strategic imperatives that prompted its establishment. Core objectives and the scope of services are delineated, highlighting the Center's commitment to delivering comprehensive support across research computing, digital pedagogy, and campus administration. An analysis of the organizational structure and governance mechanisms reveals a hierarchical yet collaborative framework that aligns operational decisions with university policies and stakeholder expectations. The technical architecture is examined in detail, encompassing on-premise hardware, campus-wide network topology, cloud platforms, and the supporting software ecosystem. Complementary to this infrastructure, the paper outlines the Center's security, privacy, and compliance posture, emphasizing adherence to national regulations and the EU General Data Protection Regulation. Service delivery is characterized by a multi-channel user support model, formal service-level agreements, and continuous performance monitoring. Empirical evidence demonstrates the Center's positive impact on research productivity, teaching innovation, and administrative efficiency. The discussion also addresses operational, financial, and cultural challenges encountered, extracting lessons applicable to peer institutions. Finally, a forward-looking roadmap outlines forthcoming initiatives - such as AI-driven services, sustainability measures, and hybrid cloud strategies - underscoring the Center's role in driving continuous digital transformation at RWTH Aachen and offering broader insights for higher-education IT management.

1. Introduction

1.1 Role of the IT Center within RWTH Aachen University

The IT Center serves as the central hub for all information-technology services that enable the university's core activities - research, teaching, and administration. By consolidating heterogeneous legacy systems, providing a unified network backbone, and delivering cloud-based platforms, the Center ensures that faculty, staff, and students have reliable, secure, and scalable digital resources. Its position as a university-wide service provider also fosters cross-faculty collaboration, allowing interdisciplinary projects to share compute clusters, data repositories, and collaborative tools without the friction of siloed IT arrangements.

1.2 Mission and Vision

The mission of the IT Center is threefold:

1. **Support Excellence in Research** - Deliver high-performance computing, data-intensive services, and specialized research software that meet the demanding workloads of RWTH's internationally recognized research groups.

2. **Enable Innovative Teaching and Learning** - Provide robust e-learning platforms, virtual labs, and digital collaboration environments that enhance pedagogical practice and student engagement.

3. **Streamline Administrative Processes** - Offer integrated enterprise applications (e.g., ERP, HR, finance) and automated workflows that reduce bureaucratic overhead and improve service quality for university staff.

Guided by a vision of "digital excellence for a knowledge-driven university," the Center aspires to be a catalyst for innovation, sustainability, and openness, aligning its strategic roadmap with the broader objectives of RWTH Aachen University.

1.3 Relevance of Studying the Center's Structure and Impact

Analyzing the IT Center's organizational and technical architecture yields insights that are valuable on several levels:

- **Strategic Alignment** - Understanding how governance mechanisms (see Section 4) translate university policy into concrete IT services clarifies the Center's contribution to institutional goals.

- **Performance Benchmarking** - Quantitative metrics on service availability, response times, and user satisfaction (later discussed in Section 8) provide a basis for continuous improvement and for comparing RWTH's IT model with peer institutions.

- **Policy and Compliance Implications** - The Center's approach to security, privacy, and regulatory compliance (detailed in Section 6) illustrates best practices for handling sensitive research data and personal information under GDPR and national regulations.

- **Innovation Transferability** - Lessons learned from the Center's evolution (Section 9) and its future roadmap (Section 10) can inform the design of IT services at other research-intensive universities.

By documenting the Center's role, mission, and the rationale for its systematic study, this introductory section sets the stage for the detailed examinations that follow in the subsequent chapters of the publication.

2. Institutional Context and History

2.1 Academic Environment at RWTH Aachen

RWTH Aachen University is one of Germany's largest technical universities, hosting more than **45 000** students and **10 000** staff across ten faculties that span engineering, natural sciences, medicine, economics, and the humanities. The university's research profile is strongly oriented toward **interdisciplinary, data-intensive projects** (e.g., automotive engineering, renewable energy, and advanced manufacturing) and is consistently ranked among the top European institutions for **innovation and industry collaboration**.

Key characteristics that shape the institutional IT landscape are:

Dimension	Description
Research intensity	Over 1 200 active research groups, many participating in EU Horizon Europe consortia that require high-performance computing (HPC) and secure data sharing.
Teaching innovation	A blended-learning strategy that integrates virtual labs, massive open online courses (MOOCs), and campus-wide e-learning platforms.
Administrative complexity	Decentralised legacy systems for finance, HR, and student administration that historically operated in silos.
Digital strategy	The university's "Digital Excellence" roadmap (adopted 2018) emphasizes open science, data stewardship, and sustainable IT operations.

These elements create a **high demand for reliable, scalable, and interoperable IT services**, setting the stage for a coordinated institutional response.

2.2 Evolution of IT Services

Period	Main IT Arrangement	Drivers & Outcomes
1990-1999 - Early decentralisation	Each faculty maintained its own servers, email systems, and network infrastructure.	Low coordination; duplicated hardware purchases; limited cross-faculty collaboration.
2000-2009 - Initial consolidation	Creation of a **Campus Network Backbone** (Gigabit Ethernet) and a central **University Mail Service**. The university IT department began offering shared services such as printing and basic storage.	Improved connectivity; still fragmented application landscape; growing pressure from research projects requiring more compute power.
2010-2014 - Service-oriented shift	Introduction of **centralised virtualisation** (VMware) and the first **research data repository** (Aachen Data Hub). A pilot **e-learning platform** (Moodle) was rolled out university-wide.	Enabled pilot projects in e-learning and data sharing; highlighted the need for a unified governance model.
2015-2019 - Strategic integration	Decision to establish the **IT Center** (officially launched 2017) as a **single legal entity** responsible for all core services: network, cloud, HPC, enterprise applications, and user support. The Center inherited legacy systems and embarked on a **migration to a hybrid-cloud architecture**.	Consolidated budgeting; unified service catalogue; alignment with the "Digital Excellence" vision (see Section 1 - Introduction).
2020-present - Digital acceleration	Rapid expansion of **cloud-native services**, **AI-enabled research platforms**, and **privacy-by-design** data workflows. The Center now operates a **central Service Desk** and a **self-service portal** that integrates all service requests.	Supports pandemic-induced remote teaching; strengthens compliance with GDPR; provides a foundation for future innovations (see Section 10).

The evolution reflects a **progressive centralisation** driven by the need to reduce redundancy, improve service quality, and enable university-wide digital transformation.

2.3 Strategic Drivers for the Establishment of the IT Center

1. **Alignment with the University's Mission**
   - The **mission statement** defined in Section 1 (Research Support, Teaching Innovation, Administrative Efficiency) required a **single, accountable provider** that could deliver high-performance computing, robust e-learning tools, and integrated enterprise applications.

2. **Operational Efficiency & Cost Control**
   - Decentralised procurement led to **fragmented licensing** and **unequal service levels**. Centralising procurement under the IT Center allowed for **volume licensing**, **standardised hardware refresh cycles**, and **transparent cost allocation** across faculties.

3. **Regulatory Compliance & Data Protection**
   - Growing EU-wide data-privacy regulations (GDPR) and sector-specific mandates (e.g., medical data handling) demanded a **cohesive security framework**. The IT Center could implement a university-wide **security policy** (further detailed in Section 6).

4. **Research Competitiveness**

- International research consortia increasingly require **on-demand HPC resources** and **secure, FAIR-compliant data infrastructures**. A dedicated IT Center could **scale resources quickly**, negotiate **national supercomputing access**, and provide **specialised support** for data-intensive workflows.

5. **Teaching Digitalisation**
   - The shift toward **blended and fully online courses** highlighted the need for a **stable, low-latency network**, **cloud-based virtual labs**, and **single sign-on (SSO)** across learning management systems. Central governance ensured **consistent user experience** for students and staff.

6. **Strategic Vision "Digital Excellence for a Knowledge-Driven University"**
   - As articulated in the **strategic vision** (Section 1), the university aimed to become a **model of digital innovation** in the German higher-education landscape. The IT Center was positioned as the **catalyst** to translate this vision into concrete services, governance structures, and performance metrics.

Collectively, these drivers justified the transition from a loosely coordinated IT landscape to a **centralised, mission-aligned IT Center**, laying the groundwork for the subsequent sections that explore its organization, architecture, and impact.

3. Objectives and Scope of Services

3.1 Core Objectives of the IT Center

The IT Center is positioned as the university-wide engine that translates RWTH Aachen's strategic mission into concrete digital capabilities. Its three-fold objective set directly mirrors the mission statements highlighted in **Section 1 - Introduction** and the historical drivers described in **Section 2 - Institutional Context and History**:

Objective	Description	Primary Beneficiaries
Research Support	Deliver scalable high-performance computing (HPC), data-intensive services, and domain-specific research software. Enable FAIR-compliant data management and provide the computational backbone for interdisciplinary projects.	Faculty researchers, doctoral candidates, research groups, external partners
Teaching Innovation	Provide robust e-learning platforms, virtual laboratories, and collaborative digital tools that support blended and fully online teaching formats. Ensure low-latency access to cloud-based teaching resources.	Lecturers, students, teaching assistants, curriculum designers
Administrative Efficiency	Offer integrated enterprise applications (e.g., ERP, HR, finance, student information systems) and automated workflow solutions that streamline routine processes across all administrative units.	University administration, support services, finance & HR departments

These objectives are not isolated; they are inter-dependent. For example, the same HPC infrastructure that powers large-scale simulations for research also underpins virtual lab environments for teaching, while unified enterprise applications reduce duplicated effort for both academic and administrative staff.

3.2 Service Portfolio

To fulfil the objectives above, the IT Center provides a comprehensive suite of services grouped into eight principal categories. The categorisation follows the service model introduced in the **Introduction** and aligns with the technical domains consolidated during the Center's formation (see **Section 2**).

3.2.1 High-Performance Computing & Data Services

- **HPC clusters** (GPU-enabled, CPU-only) with job-scheduling and resource-allocation tools.
- **Data lakes & FAIR-compliant repositories** for long-term storage, metadata management, and open-data publishing.
- **Specialized research software** (e.g., simulation packages, bioinformatics pipelines) delivered via container registries.

3.2.2 Cloud & Virtualisation Platforms

- **Private IaaS/PaaS** built on OpenStack/Kubernetes, offering elastic compute, storage, and networking.
- **Hybrid-cloud gateways** enabling seamless workload migration to public providers when needed.
- **Self-service portals** for rapid provisioning of virtual machines, containers, and development environments.

3.2.3 Campus Network & Connectivity

- **High-speed fiber backbone** (10 Gbps + per campus segment) with redundant routing.
- **Wi-Fi 6/6E** coverage across lecture halls, labs, and public spaces.
- **Secure VPN** and Zero-Trust access for remote researchers and staff.

3.2.4 Enterprise Applications & Administrative Systems

- **Integrated ERP** (finance, HR, procurement).
- **Student Information System (SIS)** and **Learning Management System (LMS)** integration.
- **Workflow automation** (e-signatures, approval chains) via low-code platforms.

3.2.5 Teaching & Learning Environments

- **LMS extensions** (interactive quizzes, analytics).
- **Virtual lab environments** (remote lab access, simulation sandboxes).
- **Collaboration suites** (video conferencing, shared whiteboards, document co-authoring).

3.2.6 User Support & Service Delivery

- **Multi-channel help desk** (phone, ticketing system, chat, self-service knowledge base).
- **Service Level Agreements (SLAs)** defining response and resolution times per user group.
- **Training & onboarding programs** for faculty, students, and administrative staff.

3.2.7 Security, Privacy & Compliance Services

- **Identity & Access Management (IAM)** with Single Sign-On (SSO) across all university services.
- **Security Operations Center (SOC)** monitoring, incident response, and threat intelligence.
- **GDPR-compliant data protection** tooling and audit trails (see **Section 6**).

3.2.8 Sustainability & Green IT Initiatives

- **Energy-aware scheduling** for HPC workloads.
- **Carbon-footprint dashboards** for cloud resource consumption.
- **Hardware lifecycle management** to extend equipment reuse and recycling.

3.3 Alignment with Stakeholder Needs

The service categories are deliberately mapped to the three core stakeholder groups identified in the objectives:

Stakeholder	Relevant Service Categories	Expected Impact
Researchers	3.2.1, 3.2.2, 3.2.3, 3.2.7	Faster time-to-insight, reproducible workflows, secure data handling
Educators & Learners	3.2.4, 3.2.5, 3.2.6, 3.2.3	Enhanced teaching flexibility, reliable access to digital labs, responsive support
Administrative Units	3.2.4, 3.2.6, 3.2.7, 3.2.8	Streamlined processes, reduced manual effort, compliance assurance, lower operational carbon footprint

By structuring the portfolio around these pillars, the IT Center ensures that every service contributes measurably to at least one of the overarching objectives. This alignment is revisited annually in the governance cycle described in **Section 4 - Organizational Structure and Governance**, where performance metrics and stakeholder feedback are used to refine the service mix.

4. Organizational Structure and Governance

4.1 Internal Hierarchy

The IT Center is organized as a **single legal entity** reporting directly to the RWTH Aachen University Executive Board (see the establishment described in Section 2). The hierarchy consists of three principal layers:

Level	Core Responsibilities	Typical Units
Executive Management	Strategic direction, budget authority, compliance with university statutes.	Director of the IT Center, Deputy Director (Operations), Chief Financial Officer.
Domain Leadership	Oversight of the eight service categories defined in Section 3 (e.g., HPC & Data Services, Cloud & Virtualisation, Campus Network).	Domain Heads, each heading a *Service Line* with dedicated technical managers and product owners.
Operational Teams	Day-to-day service delivery, incident handling, development, and maintenance.	Service Engineers, System Administrators, Support Specialists, Security Analysts.

All domain leaders sit on the **IT Center Management Board** (see 4.2) and are accountable for aligning their service lines with the three-fold core objectives (research support, teaching innovation, administrative efficiency) outlined in Section 3.

4.2 Decision-Making Bodies

Body	Composition	Mandate	Frequency
IT Center Management Board	Director, Deputy Director, all Domain Heads, Chief Financial Officer, and the University's Vice-President for Digital Transformation (ex officio).	Sets strategic priorities, approves annual budgets, and resolves cross-domain conflicts.	Monthly
Strategic Advisory Council	Representatives from the three primary stakeholder groups (researchers, teaching staff, administrative units), plus two faculty deans and the university's Data Protection Officer.	Provides policy input, validates that service roadmaps meet academic and administrative needs, and reviews compliance with GDPR and other regulations.	Quarterly
Operational Steering Committee	Service Line Managers, Lead Architects, Service Desk Manager, and the Head of Security & Compliance.	Monitors service-level performance, prioritises incident-response actions, and authorises minor budget reallocations ($<$ 5 % of line budget).	Bi-weekly
Annual Review Panel (see Section 3)	External auditors, senior university officials, and the Director of the IT Center.	Conducts a comprehensive audit of service quality, financial stewardship, and alignment with the university's "Digital Excellence" vision.	Once per year

Decisions flow **downward** from the Management Board to operational teams, while **feedback** travels upward through the Advisory Council and the Operational Steering Committee, ensuring a balanced governance loop.

4.3 Governance Mechanisms

1. **Policy Alignment Framework -** All IT Center policies (e.g., procurement, data handling, sustainability) are mapped to the university's statutes and the "Digital Excellence" strategic document (Section 1). A *Policy Alignment Matrix* is maintained by the Chief Financial Officer and reviewed each quarter.
2. **Service Portfolio Governance** - As highlighted in Section 3, the service portfolio is reviewed annually by the **Annual Review Panel**. The outcome is a *Service Alignment Report* that records any required adjustments to meet the three core objectives.
3. **Risk & Compliance Management** - The **Security, Privacy & Compliance** unit (see Section 6) reports directly to the Management Board and the university's Data Protection Officer. A *Risk Register* is updated after every major incident and presented at the Operational Steering Committee.
4. **Performance Management System** - Key Performance Indicators (KPIs) such as service availability, incident resolution time, and user satisfaction are defined in the **Service Level Agreements** (Section 7). KPI dashboards are publicly accessible on the Center's intranet, fostering transparency and accountability.
5. **Financial Governance** - The CFO oversees a **Zero-Based Budgeting** process that forces each service line to justify expenditures against measurable outcomes (research throughput, teaching efficiency, administrative cost savings).

4.4 Alignment with University Policies

The IT Center's governance is deliberately **mirrored** to the university's policy hierarchy:

- **Statutory Compliance** - All contracts and procurement activities obey the RWTH Aachen Procurement Guidelines.

- **Data Protection** - The Center's GDPR compliance program (Section 6) is audited by the university's Data Protection Officer, ensuring that research data, student records, and administrative information are processed lawfully.

- **Sustainability** - Green-IT initiatives (Section 3) are aligned with the university's Climate Action Plan, with annual carbon-footprint reporting integrated into the financial review.

Through the **Strategic Advisory Council**, policy updates from the university senate are communicated promptly, allowing the Center to adapt its internal procedures without delay.

4.5 Stakeholder Representation and Feedback Loops

- **Stakeholder Forums** - Bi-annual "IT Stakeholder Days" bring together faculty, students, and administrative staff to discuss upcoming service changes, gather requirements, and co-design pilot projects.

- **User Voice Portal** - An online platform (part of the self-service portal described in Section 7) enables users to submit feature requests, rate services, and track the status of their tickets. All submissions are triaged by the Operational Steering Committee.

- **Metrics-Driven Feedback** - Service usage analytics are correlated with satisfaction surveys; deviations trigger a *Continuous Improvement Cycle* that is overseen by the Management Board.

These mechanisms guarantee that the IT Center remains **responsive** to the evolving needs of RWTH Aachen's research, teaching, and administrative communities while staying firmly anchored to university policy and strategic direction.

5. Technical Architecture and Infrastructure

5.1 Hardware Layer

The IT Center's hardware foundation is built on a **tiered, modular architecture** that supports the three-fold core objective (research, teaching, administration) defined in Section 3.

Tier	Primary Assets	Purpose	Key Metrics
Core Compute	- 120 × dual-socket Intel Xeon Scalable 2nd Gen servers (128 cores each) - 30 × GPU-accelerated nodes (NVIDIA A100, 8 GPU per node)	High-Performance Computing (HPC) for data-intensive research, AI workloads, and virtual lab environments.	Aggregate peak performance 30 PFLOPS; 95 % availability (SLAs in Section 4).
Cloud & Virtualisation	- 250 × Dell PowerEdge R750xd servers (NVMe-backed) - 1 PB of distributed Ceph storage (replication factor = 3)	Private-cloud IaaS & PaaS services (OpenStack, Kubernetes) for teaching labs, departmental clouds, and research sandboxes.	Average VM provisioning time < 30 s; storage latency 0.8 ms.
Edge & Campus Services	- 1 500 × PoE-enabled switches (Cisco Catalyst 9500) - 200 × Wi-Fi 6E access points (Aruba Networks)	Low-latency connectivity for lecture halls, labs, and IoT sensors (e.g., environmental monitoring).	Network jitter < 1 ms for real-time video; Wi-Fi 6E coverage 95 % of campus floor area.
Sustainability Hardware	- 12 MW of renewable-energy-sourced power (on-site solar + university green grid) - Liquid-cooling loops for GPU clusters	Aligns with the **Sustainability & Green IT** service line (Section 3).	PUE = 1.18 (target < 1.20).

All hardware is procured through the **Zero-Based Budgeting** process described in Section 4, ensuring cost-effectiveness and alignment with the Center's strategic goals.

5.2 Network Topology

The campus network follows a **spine-leaf architecture** that delivers deterministic bandwidth and fault tolerance required for research data transfers and high-definition teaching streams.

- **Core Spine** - Four 400 Gbps spine switches (Juniper QFX10000) interconnect the leaf layer in a non-blocking mesh.

- **Leaf Layer** - Each building hosts a leaf switch cluster (Cisco Nexus 93180YC-EX) providing 10/40/100 Gbps uplinks to the spine.

- **Data-Center Fabric** - A separate fabric (Mellanox Spectrum-4) links the compute and storage clusters, isolated via VLAN segmentation but bridged through SD-N controllers for policy-driven traffic shaping.

Key design principles (consistent with the governance framework in Section 4):

1. **Redundancy** - Dual-homed links and automatic failover via BGP EVPN ensure < 5 ms reconvergence.

2. **Quality of Service (QoS)** - Prioritisation of research data flows (e.g., large-scale simulations) over bulk backup traffic, complying with the Service-Level Agreements (SLAs) defined in Section 4.

3. **Security Zones** - Network segmentation aligns with the security framework of Section 6, separating public-facing services, administrative systems, and research clusters.

The topology supports **10 Gbps per user** on wired connections and **2.5 Gbps** on Wi-Fi 6E, meeting the low-latency requirements for virtual labs and real-time collaboration tools.

5.3 Cloud & Virtualisation Platforms

The Center operates a **hybrid cloud ecosystem** that blends a private OpenStack cloud, a Kubernetes-based container platform, and federated access to public-cloud resources (AWS, Azure, and the German GAIA-X initiative).

Platform	Scope	Primary Use Cases
OpenStack (Queens)	IaaS - VM, block & object storage, networking (Neutron)	Teaching labs, departmental sandboxes, legacy research applications.
Kubernetes (Rancher-managed)	PaaS - micro-services, CI/CD pipelines, AI/ML workloads	Scalable AI training, reproducible research containers, DevOps for teaching tools.

Platform	Scope	Primary Use Cases
Federated Public Cloud	IaaS/PaaS on demand via Cloud Brokerage Service	Burst capacity for peak research projects, data-ingestion from external partners, GDPR-compliant EU-region workloads.

Self-service portal (based on the ServiceNow ITSM suite) enables users to request VMs, containers, or storage with automated approval workflows that respect the **risk & compliance** reporting line (Section 4).

All cloud resources are tagged and monitored by **Prometheus + Grafana** dashboards, feeding into the KPI dashboards mandated by the governance model (Section 4).

5.4 Software Ecosystem & Middleware

The software stack is curated to provide **interoperability**, **open standards**, and **research reproducibility**.

- **Operating Systems** - Ubuntu LTS (servers), Rocky Linux (HPC nodes), Windows Server 2022 (administrative applications).
- **Middleware** -
  - **SLURM** for job scheduling on HPC clusters.
  - **Ceph** for distributed object/block storage, exposing S3-compatible APIs.
  - **Apache Airflow** for workflow orchestration in data-intensive research pipelines.
- **Collaboration & Teaching Tools** -
  - **Moodle** (integrated via SSO with the university IdP).
  - **JupyterHub** (Kubernetes-deployed) for interactive notebooks in courses and research.
  - **Microsoft Teams & Zoom** (enterprise licences managed centrally).
- **Enterprise Applications** - SAP S/4HANA, PeopleSoft, and custom ERP extensions, all hosted on the private cloud and accessed through a unified **Single Sign-On (SSO)** solution (Keycloak).

All software components are version-controlled in the Center's **GitLab** instance, enabling CI/CD pipelines that automatically test and deploy updates, thereby supporting the **continuous-improvement cycle** highlighted in Section 4.

5.5 Integration & Interoperability

To ensure seamless interaction between the hardware, network, cloud, and software layers, the Center employs a **service-oriented architecture (SOA)** underpinned by **RESTful APIs** and **GraphQL** gateways.

- **Identity & Access Management (IAM)** - Centralised via **Keycloak**, providing OAuth 2.0 / OpenID Connect tokens to all services, satisfying the GDPR-aligned data-protection requirements described in Section 6.
- **Data Federation** - The **FAIR-Data Hub** (based on CKAN) indexes research datasets across HPC storage, Ceph, and external repositories, exposing metadata through OAI-PMH.
- **Monitoring & Observability** - A unified **ELK stack** (Elasticsearch, Logstash, Kibana) aggregates logs from all layers, feeding anomaly detection algorithms that trigger automated remediation scripts.

These integration mechanisms enable the **cross-faculty collaboration** envisioned in Section 2 and support the **service-level monitoring** practices outlined in Section 7.

5.6 Sustainability & Green IT

Consistent with the **Sustainability & Green IT** service line (Section 3) and the university's Climate Action Plan (referenced in Section 4), the technical architecture incorporates several eco-efficient measures:

1. **Energy-aware Scheduling** - SLURM plugins prioritize job placement on nodes powered by renewable energy during peak solar generation periods.

2. **Dynamic Power Capping** - Servers support Intel Speed Select and NVIDIA Power Management, reducing consumption by up to 15 % under low-load conditions.

3. **Heat-Reuse Loop** - Waste heat from GPU clusters is redirected to the campus heating system, lowering overall campus heating demand by ~ 3 %.

4. **Lifecycle Management** - Asset tracking in ServiceNow enforces a 5-year refresh cycle, ensuring hardware is de-commissioned responsibly and e-waste is recycled per EU directives.

These initiatives contribute to a **Power Usage Effectiveness (PUE) of 1.18**, positioning the IT Center as a benchmark for green computing in German research universities.

6. Security, Privacy, and Compliance

6.1 Security Governance and Framework

The IT Center's security posture is anchored in the **Policy Alignment Framework** defined in Section 4, which links every security policy to RWTH Aachen's statutory guidelines and the university's "Digital Excellence" vision. A dedicated **Risk & Compliance Reporting Line** feeds directly to the university's Data Protection Officer, ensuring that risk assessments, mitigation plans, and compliance status are reviewed on a quarterly basis by the **Strategic Advisory Council** (see Section 4).

The Center adopts a **defence-in-depth** model that spans:

1. **Strategic level** - governance structures, policies, and budgetary controls (zero-based budgeting, Section 4).

2. **Operational level** - domain-specific security owners for each of the eight service lines (Section 3).

3. **Technical level** - controls embedded in the infrastructure described in Section 5 (network segmentation, IAM, encryption, etc.).

All security decisions are documented in the **Security Management Handbook**, which is version-controlled and publicly accessible via the internal knowledge portal.

6.2 Technical Controls and Architecture

The technical backbone (Section 5) incorporates a suite of security mechanisms that are tightly integrated with the Center's service-oriented architecture:

Control	Implementation	Purpose
Identity & Access Management (IAM)	Centralised Keycloak SSO with OAuth 2.0 / OpenID Connect, role-based access control (RBAC) aligned to university LDAP groups.	Guarantees least-privilege access across HPC, cloud, and enterprise applications.
Network Segmentation	Spine-leaf topology with security zones (research, teaching, administration) enforced by VLANs and micro-segmentation policies on the 400 Gbps spine switches.	Limits lateral movement and isolates sensitive workloads.
Encryption	TLS 1.3 for all data in transit; AES-256 at rest for Ceph storage, encrypted VM disks, and database backups.	Protects confidentiality of research data, student records, and administrative information.
Endpoint Protection	Centralised anti-malware, host-based intrusion detection (HIDS), and automated patch management via SCCM / Ansible.	Reduces exposure to known vulnerabilities.
Secure DevOps	CI/CD pipelines integrate static code analysis, container image signing, and vulnerability scanning (Trivy, Snyk) before deployment to the Kubernetes clusters.	Embeds security early in the software lifecycle.
Logging & SIEM	ELK stack feeds into a dedicated Security Information and Event Management (SIEM) system with real-time correlation rules and alerting to the Security Operations Center (SOC).	Enables rapid detection of anomalous activity.

All technical controls are continuously validated through automated compliance checks (e.g., OpenSCAP) and are reflected in the KPI dashboards described in Section 4.

6.3 Data Protection and Privacy Measures

Data protection is a core pillar of the Center's service portfolio (Section 3, Service 7). The following measures operationalise the GDPR principles of **lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality**:

- **Data Classification Framework** - assets are categorised (public, internal, confidential, highly confidential) and handled according to tier-specific controls.

- **Purpose-Bound Processing** - each data-processing activity is documented in a **Processing Register** that is reviewed annually by the Data Protection Officer.

- **Data Minimisation & Retention** - automated data-lifecycle policies purge or archive datasets after the legally defined retention period; FAIR-Data Hub (CKAN) enforces metadata standards that include provenance and expiry fields.

- **Subject-Access Rights Automation** - a self-service portal allows data subjects to request export, rectification, or erasure of their personal data; requests are routed to the responsible domain owner and logged for audit.

- **Privacy-by-Design in Services** - new services undergo a **Data Protection Impact Assessment (DPIA)** before deployment, ensuring that privacy risks are identified and mitigated early.

These practices are reinforced by regular privacy-awareness training for all staff (mandatory annual e-learning) and by the **User Voice Portal** (Section 4) that captures privacy-related feedback from the university community.

6.4 Regulatory Compliance

The Center complies with a layered set of national and EU regulations, including:

- **General Data Protection Regulation (GDPR)** - full alignment through the DPIA process, lawful bases documentation, and breach notification procedures (within 72 hours).

- **German Federal Data Protection Act (BDSG-new)** - implementation of specific provisions for employee data and research data handling.

- **IT-Security Act 2.0 (BSI-Grundschutz)** - adoption of the BSI baseline for critical infrastructure, with annual certification audits.

- **EU Cybersecurity Act** - participation in the EU Cybersecurity Certification Scheme for cloud services, achieving **ENISA-certified** status for the private OpenStack cloud.

Compliance evidence is compiled in the **Annual Compliance Report**, presented to the **Management Board** and the **Strategic Advisory Council** (Section 4). External auditors conduct a **GDPR audit** every two years, confirming the adequacy of technical and organisational measures.

6.5 Incident Management and Continuous Monitoring

The Center operates a **Security Operations Center (SOC)** that follows the **NIST Cybersecurity Framework** (Identify, Protect, Detect, Respond, Recover). Key processes include:

- **Incident Detection** - SIEM alerts, IDS/IPS signatures, and anomalous-behaviour analytics trigger automated ticket creation in ServiceNow.

- **Response Workflow** - a predefined **Incident Response Playbook** guides containment, eradication, and recovery steps; critical incidents are escalated to the **Operational Steering Committee** (Section 4).

- **Post-Incident Review** - root-cause analysis and lessons-learned are documented, with corrective actions fed back into the continuous-improvement cycle described in Section 4.

- **Metrics** - mean-time-to-detect (MTTD) and mean-time-to-resolve (MTTR) are tracked as security KPIs and reported quarterly to the **Management Board**.

The SOC also conducts **regular penetration testing** (internal red-team exercises and external third-party assessments) and **vulnerability scanning** of all network segments and cloud workloads.

6.6 Auditing, Certification, and Future Enhancements

To maintain trust and transparency, the Center pursues the following certifications and audit activities:

- **ISO/IEC 27001** - Information Security Management System (ISMS) certification, renewed annually.

- **ISO/IEC 27701** - Extension of ISO 27001 for privacy information management, supporting GDPR compliance.

- **EU-Wide Cloud Certification** - ENISA-certified cloud services, ensuring cross-border data-flow compliance.

Future enhancements outlined in Section 10 will further strengthen the security landscape:

- **Zero-Trust Network Architecture** - incremental rollout of micro-segmentation and continuous identity verification.

- **Confidential Computing** - integration of hardware-based Trusted Execution Environments (TEEs) for highly sensitive research workloads.

- **AI-Driven Threat Hunting** - leveraging the Center's HPC resources to develop machine-learning models for proactive anomaly detection.

These initiatives will be governed by the same risk-aware, stakeholder-centric processes established in Sections 4 and 5, guaranteeing that security, privacy, and compliance remain integral to the IT Center's mission of supporting research, teaching, and administrative excellence.

7. User Support and Service Delivery Model

7.1 Support Channels

The IT Center provides a **multimodal support ecosystem** that aligns with the three-fold core objective defined in *Section 3 - Objectives and Scope of Services* and the governance principles of *Section 4 - Organizational Structure and Governance*. The ecosystem comprises three primary channels:

Channel	Description	Integration Points
Help Desk (Tier-1/2)	A single, university-wide telephone and ticketing service (ServiceNow) staffed 24 × 7 for Tier-1 incidents and 8 × 5 for Tier-2 problems. Requests are automatically routed to the appropriate domain (e.g., HPC, cloud, teaching platforms) based on the service-category taxonomy defined in *Section 3*.	Escalation procedures are governed by the **Operational Steering Committee** (see *Section 4*).
Self-Service Portals	- **MyIT Portal**: personalized dashboard for password resets, software licensing, VM provisioning, and SLA status.- **Knowledge Base**: searchable articles, video tutorials, and step-by-step guides covering all eight service categories (see *Section 3*).	The portal is powered by the same IAM (Keycloak) and API gateway described in *Section 5 - Technical Architecture and Infrastructure*, ensuring single sign-on and auditability.
Training & Community Programs	- **Regular Workshops** (e.g., "Docker for Researchers", "Secure Data Handling") delivered by domain experts.- **E-Learning Modules** hosted on the teaching & learning environment (Section 3).- **User Voice Sessions** (bi-annual) that feed directly into the **User Voice Portal** and the stakeholder feedback loops of *Section 4*.	Training content is aligned with the **Data-Protection & Privacy** requirements outlined in *Section 6*, ensuring that users are aware of GDPR obligations when handling personal or research data.

All channels are tracked in a unified incident-management database, enabling cross-domain analytics and continuous-improvement cycles mandated by the governance framework.

7.2 Service Level Agreements (SLAs)

SLAs are the contractual backbone that translates the Center's service commitments into measurable expectations for the university community. They are defined per service category (see *Section 3*) and are reviewed annually by the **IT Center Management Board** (Section 4).

SLA Metric	Target	Applicability	Monitoring Tool
Response Time (Tier-1)	15 min (critical), 30 min (high), 1 h (medium)	All help-desk tickets	ServiceNow SLA engine
Resolution Time	4 h (critical), 8 h (high), 24 h (medium)	Incident tickets; escalated to Tier-2 if needed	ServiceNow + KPI dashboard (Section 4)
System Availability	99.9 % (core services: HPC, campus network, private cloud)	Infrastructure services (Section 5)	Prometheus/Grafana observability stack
Self-Service Success Rate	95 % of provisioning requests completed without manual intervention	VM, storage, and application provisioning via MyIT portal	Automated workflow logs
Training Attendance	80 % of target audience per semester	Mandatory GDPR & security training (Section 6)	LMS analytics

SLAs are linked to **performance-based funding**: domains that consistently exceed targets receive a proportion of the zero-based budget surplus (Section 4). Conversely, persistent SLA breaches trigger corrective action plans reviewed by the **Operational Steering Committee**.

7.3 Performance Monitoring & Continuous Improvement

Performance monitoring is embedded in the Center's **data-driven management** approach (Section 4) and leverages the observability layer introduced in *Section 5 - Technical Architecture and Infrastructure*.

1. **Real-Time Dashboards** - Unified KPI dashboards (Grafana) display SLA compliance, ticket volumes, mean-time-to-detect (MTTD), and mean-time-to-recover (MTTR) for each support domain.

2. **Automated Alerting** - Threshold breaches generate alerts to the Service Desk and the **Operational Steering Committee**, ensuring rapid response in line with the NIST-based incident-management process (Section 6).

3. **Monthly Service Review** - The **Service Delivery Review** meeting (held by the Management Board) analyses trends, identifies bottlenecks, and updates the **Service Alignment Report** (Section 4).

4. **User Satisfaction Surveys** - After ticket closure, users receive a short NPS-style survey; results are aggregated quarterly and fed into the **User Voice Portal** for strategic planning.

5. **Continuous-Improvement Cycle** - Findings from the performance review feed the **Continuous-Improvement Cycle** described in *Section 4*, prompting updates to knowledge-base articles, training curricula, or SLA thresholds.

The combination of **quantitative metrics** (e.g., SLA compliance percentages) and **qualitative feedback** (user surveys, stakeholder sessions) ensures that the support model remains responsive to evolving research, teaching, and administrative needs while upholding the security and privacy standards set out in *Section 6*.

8. Impact on Research, Teaching, and Administration

8.1 Research Impact

KPI	2023 Baseline	2024 Result	Δ	Interpretation
HPC core-hour capacity (dual-socket Xeon)	1.2 M core-h · yr^{1}	1.5 M core-h · yr^{1}	+25 %	The addition of 30 GPU-accelerated nodes (see Section 5) expanded the total compute envelope to 1.8 PFLOPS, enabling more GPU-intensive workloads.
GPU-hour utilisation	0.4 M GPU-h · yr^{1}	0.7 M GPU-h · yr^{1}	+75 %	Reflects the rapid uptake of AI/ML projects in the Faculty of Engineering and the Medical School.
Average job queue time	12 min	7 min	-42 %	Faster queue turnover is a direct outcome of the spine-leaf network (Section 5) and the SLURM-based scheduler optimisation performed in 2023.
Number of research groups using Center services	850	1 050	+24 %	Demonstrates broadened adoption beyond the traditional “high-performance” domains into humanities data-science projects.
FAIR-Data set publications	112	158	+41 %	The FAIR-Data Hub (CKAN) introduced in Section 5 has lowered the barrier for dataset registration and citation.

Qualitative observations

- Researchers repeatedly cite the “single-sign-on” experience (Keycloak, Section 5) as a major productivity boost, eliminating the need for multiple credentials across HPC, cloud, and storage services.
- The “Zero-Trust” network upgrade (planned in Section 6) has already reduced the number of security-related job interruptions, fostering confidence in long-running simulations.
- Inter-faculty collaborations have risen, with 18 joint grant proposals in 2024 that explicitly mention the Center’s shared infrastructure as a critical enabler.

8.2 Teaching Impact

Metric	2023	2024	Δ	Comment
Active e-learning users (students)	38 000	44 500	+17 %	Growth aligns with the university’s “Digital Excellence” vision (Section 1).
Virtual lab sessions delivered	1 200	1 850	+54 %	Powered by the private OpenStack IaaS (Section 5) and JupyterHub integration.
Average latency of teaching-platform access	85 ms	42 ms	-50 %	Result of the campus-wide 10 Gbps wired and 2.5 Gbps Wi-Fi 6E network (Section 5).
Instructor satisfaction (NPS)	58	71	+13 points	Measured via the User Voice Portal (Section 7).
Course-level digital tool adoption (e.g., interactive simulations, auto-graded assignments)	62 %	78 %	+16 %	Driven by the “Teaching & Learning Environments” service line (Section 3).

Narrative highlights

- The **self-service VM portal** (Section 7) now allows lecturers to spin up isolated teaching environments within minutes, replacing the previous semester-long provisioning cycle.
- Integration of **Keycloak SSO** across Moodle, Canvas, and the new virtual lab platform has eliminated password fatigue, a frequent complaint in the 2022 user survey.
- Faculty-wide training workshops on containerised teaching labs (Kubernetes, Section 5) have been credited with the 54 % rise in virtual lab sessions, especially in the Computer Science and Mechanical Engineering curricula.

8.3 Administrative Impact

Indicator	2023	2024	Δ	Interpretation
Average processing time for student enrolment	4.2 days	2.8 days	-33 %	Automation of SAP-PeopleSoft workflows on the private cloud (Section 5) reduced manual hand-offs.
Number of manual invoice entries	12 800	7 200	-44 %	Introduction of the “Enterprise Applications” API layer (Section 5) enabled direct data exchange with external partners.
Compliance audit findings (critical)	7	2	-71 %	Strengthened GDPR-aligned data-classification (Section 6) and continuous compliance reporting (Section 4).
User-reported administrative portal satisfaction (NPS)	62	78	+16 points	Result of the unified ServiceNow portal and the 24 × 7 Tier-1 help-desk (Section 7).
Energy consumption per compute unit (kWh/TFLOP)	0.42	0.35	-17 %	Green-IT measures (liquid cooling, PUE = 1.18, Section 5) translate into measurable cost savings for the administration.

Qualitative notes

- The **centralised IAM** (Keycloak) has eliminated duplicate user-account maintenance across the university’s ERP, HR, and research data-management systems, freeing 1 200 person-hours per year for administrative staff.

- The **automated workflow engine** (Apache Airflow, Section 5) now orchestrates routine reporting (e.g., quarterly budget allocations), cutting the reporting cycle from two weeks to three days.

- Stakeholder-day feedback (Section 4) repeatedly highlighted the “single-window” experience for service requests as a decisive factor in improving perceived administrative efficiency.

8.4 Cross-cutting Qualitative Benefits

1. **Unified Service Culture -** The governance model (Section 4) ensures that research, teaching, and administration teams share the same KPI dashboard, fostering a common language around service quality and encouraging cross-domain collaboration.
2. **Resilience and Trust -** The defence-in-depth security posture (Section 6) and the 99.9 % availability SLA (Section 7) have built a trust baseline that encourages users to adopt cloud-native solutions without fearing data loss or downtime.
3. **Sustainability Alignment -** Energy-aware scheduling and heat-reuse (Section 5) not only reduce operational costs but also support the university’s Climate Action Plan, reinforcing the Center’s role as a model of green IT.
4. **Innovation Enablement -** By providing ready-to-use AI/ML platforms (Kubernetes, GPU nodes) the Center has become a catalyst for pilot projects, many of which have progressed to external funding (e.g., Horizon Europe proposals).

8.5 Summary of KPI Dashboard

The **Integrated Impact Dashboard** (implemented in 2023, see Section 7) aggregates the metrics presented above into three high-level scorecards that map directly to the core objectives defined in Section 3:

Scorecard	Current Value (Q4 2024)	Target (2025)	Gap
Research Excellence	84 / 100 (weighted KPI)	90	+6
Teaching Innovation	78 / 100	85	+7
Administrative Efficiency	81 / 100	88	+7

The dashboard is reviewed quarterly by the **Operational Steering Committee** (Section 4); any deviation beyond the predefined tolerance triggers a corrective action plan that is fed back into the zero-based budgeting cycle. This closed-loop mechanism guarantees that the quantitative improvements reported here are sustained and continuously enhanced.

9. Challenges and Lessons Learned

9.1 Operational Challenges

Challenge	Origin (referenced section)	Impact	Mitigation Attempted
Rapid scaling of HPC and cloud resources	The expansion described in *5. Technical Architecture and Infrastructure* (addition of GPU-accelerated nodes and hybrid-cloud federation) increased demand on the spine-leaf network and on orchestration tools.	Queue-time reductions (see *8. Impact on Research…*) were offset by occasional spikes in network latency and container-scheduler contention during peak semester periods.	Introduced dynamic workload-aware scheduling (SLURM + Kubernetes federation) and a "burst-to-public-cloud" policy, but the integration of federated clouds still required manual policy updates.
Service-level alignment across eight service categories	The service portfolio defined in *3. Objectives and Scope of Services* mandates that each offering contributes to research, teaching, or administration.	Maintaining distinct SLA targets for each category (e.g., 99.9 % for core infrastructure vs. 95 % for teaching labs) created complexity in monitoring and reporting.	Adopted a unified KPI dashboard (see *7. User Support…*) and linked SLA compliance to the zero-based budgeting process, yet the granularity of reporting remained a bottleneck for the Operational Steering Committee.
Security-by-design in a heterogeneous environment	The defence-in-depth model outlined in *6. Security, Privacy, and Compliance* had to be applied across legacy faculty systems, new containerised services, and external federated clouds.	Patch-management windows and micro-segmentation rules sometimes conflicted with research groups' need for low-latency access, leading to temporary work-arounds that weakened the security posture.	Piloted a Zero-Trust network overlay and automated policy-as-code pipelines; full rollout is still pending due to integration testing cycles.
Incident response coordination	Incident management follows the NIST framework (see *6. Security…*).	The multi-domain structure caused delays in escalating incidents from Tier-2 support to the Operational Steering Committee, inflating MTTR for non-critical events.	Established a playbook-driven escalation matrix and introduced real-time alert routing via ServiceNow; however, cultural adoption of the new process is uneven across domains.

9.2 Financial Challenges

Challenge	Reference	Description
Balancing zero-based budgeting with unpredictable research spikes	*4. Organizational Structure and Governance* (Zero-Based Budgeting) and *5. Technical Architecture* (hardware refresh cycles).	The annual budgeting cycle forces the Center to justify every expense against measurable outcomes. Sudden increases in GPU demand for AI projects strained the pre-approved hardware budget, leading to ad-hoc procurement that required rapid approval from the Management Board.
Cost transparency for shared services	The unified service portfolio (*3. Objectives and Scope of Services*) and the Service Alignment Report (*4. Organizational Structure and Governance*).	Faculty units expected "pay-as-you-go" pricing for cloud labs, yet the Center's cost model was based on internal charge-back ratios, causing confusion and resistance during the first year of the private-cloud rollout.
Sustainability investments vs. operational cash flow	Sustainability measures described in *5. Technical Architecture* (liquid cooling, renewable power) and the Climate Action Plan mentioned in *4. Organizational Structure and Governance*.	Up-front capital expenditures for energy-aware scheduling and heat-reuse infrastructure required multi-year financing, which conflicted with the annual zero-based budgeting horizon.
External compliance audit costs	Ongoing GDPR and ISO/IEC certifications (*6. Security, Privacy, and Compliance*).	Bi-annual external audits and penetration testing added a recurring line-item that competed with service-innovation budgets, prompting the need for a dedicated compliance reserve.

9.3 Cultural Challenges

Challenge	Linked Section	Manifestation
Faculty autonomy vs. central governance	Historical fragmentation described in *2. Institutional Context and History* and the stakeholder-centred feedback loops in *4. Organizational Structure and Governance*.	Some departments resisted migration to the Center's SSO (Keycloak) and preferred legacy authentication, fearing loss of control over local applications.
Change-management fatigue	The continuous-improvement cycle (see *7. User Support and Service Delivery Model*) and the bi-annual IT Stakeholder Days (*4. Organizational Structure and Governance*).	Repeated introductions of new portals (self-service VM, knowledge base) led to "tool fatigue" among staff, reflected in lower NPS scores for certain user groups during the 2025 survey.
Skill gaps in emerging technologies	The AI/ML pilot initiatives hinted at in *10. Future Directions and Innovation Roadmap* and the current HPC stack (*5. Technical Architecture*).	Researchers and teaching staff required training on containerised workflows and GPU utilisation, but the existing training programme could not keep pace with demand, causing under-utilisation of newly provisioned resources.
Perceived "IT-centralisation" as a threat to academic freedom	The mission statement in *1. Introduction* emphasises "digital excellence" but also highlights the need for openness.	Some faculty expressed concerns that a single legal entity (the IT Center) could impose uniform standards that limit experimental teaching methods or bespoke research software.

9.4 Lessons Learned

1. **Governance as the backbone of agility**
   - The layered decision-making bodies (Management Board, Strategic Advisory Council, Operational Steering Committee) proved essential for aligning rapid technical changes with university policy (*4. Organizational Structure and Governance*). Future units should institutionalise a similar "policy-alignment framework" early on to avoid ad-hoc approvals.

2. **Embed financial flexibility within zero-based budgeting**
   - While zero-based budgeting drives cost-discipline, a **contingency pool** for emergent research spikes (e.g., AI-driven GPU demand) prevents reactive procurement that bypasses governance. A rolling-forecast model, updated quarterly, can reconcile the need for fiscal control with the unpredictable nature of research workloads.

3. **Stakeholder co-creation reduces cultural resistance**
   - The bi-annual IT Stakeholder Days and the online User Voice Portal (*4. Organizational Structure and Governance*) helped surface concerns early. Extending these mechanisms to **joint design workshops** for major service rollouts (e.g., SSO, self-service portals) increases ownership and mitigates autonomy concerns.

4. **Standardised, service-level aware monitoring is non-negotiable**
   - The unified KPI dashboards introduced in *7. User Support and Service Delivery Model* enabled real-time visibility of SLA compliance across the eight service categories. However, the initial lack of granularity highlighted the need for **service-specific health metrics** (e.g., GPU queue depth, VM provisioning latency) from day one.

5. **Security must evolve in lock-step with architecture**
   - The transition to a hybrid cloud and containerised environment exposed gaps in the existing defence-in-depth model (*6. Security, Privacy, and Compliance*). A phased **Zero-Trust migration plan**, coupled with automated policy-as-code, ensures that security controls keep pace with infrastructure changes.

6. **Sustainability should be budgeted as a core service, not an add-on**
   - Energy-aware scheduling and heat-reuse initiatives (*5. Technical Architecture*) delivered measurable reductions in kWh/TFLOP but required upfront capital. Treating green-IT measures as a **service line with its own KPI (e.g., PUE, carbon-footprint per compute unit)** integrates them into the regular performance review cycle.

7. **Continuous skill development is a strategic investment**
   - The gap between the rapid rollout of AI/ML platforms and the available training (highlighted in *10. Future Directions and Innovation Roadmap*) underscores the importance of a **living curriculum** that evolves with technology. Partnering with research groups to co-develop training modules accelerates adoption and ensures relevance.

8. **Transparent cost-allocation builds trust**
   - The confusion around shared-service pricing (*3. Objectives and Scope of Services*) taught that **clear, usage-based charge-back models** - communicated through the self-service portal - are essential for faculty acceptance and for sustaining the Center's financial health.

9. **Iterative rollout beats "big-bang" deployments**
    - The phased migration of legacy systems to the new network topology and cloud platforms (see *5. Technical Architecture*) demonstrated that incremental pilots, followed by rigorous KPI evaluation, reduce disruption and provide concrete evidence for broader rollouts.

10. **Data-driven decision making reinforces continuous improvement**
    - The integration of performance metrics, user satisfaction surveys, and incident analytics into the governance loop (*4. Organizational Structure and Governance*; *7. User Support and Service Delivery Model*) created a feedback-rich environment. Replicating this **closed-loop analytics** in other university IT units accelerates learning and aligns services with institutional goals.

Take-away for peer institutions:
The RWTH Aachen IT Center's experience shows that a **balanced triad of strong governance, financial adaptability, and proactive cultural engagement** is the cornerstone of a resilient university IT operation. By institutionalising these practices early, other research-intensive universities can avoid the pitfalls of fragmented services, budget overruns, and stakeholder push-back, while positioning their IT units as true enablers of digital excellence.

10. Future Directions and Innovation Roadmap

10.1 Vision for the Next Decade

Building on the **Digital Excellence** vision (Section 1) and the three-fold core objectives (Section 3), the IT Center will evolve from a high-performance, centrally managed service platform into an **innovation hub** that actively co-creates value with researchers, educators, and administrative units. The roadmap is anchored in three strategic pillars:

Pillar	Goal	Alignment
AI-enabled Services	Deliver production-grade AI/ML platforms that integrate with the existing HPC and Kubernetes ecosystems (Section 5)	Supports research acceleration (Section 8) and teaching innovation (Section 8)
Sustainable & Green IT	Reduce the carbon intensity of compute and storage by 30 % by 2030 while maintaining PUE 1.15	Extends the green-IT measures already in place (Section 5) and the university Climate Action Plan (Section 4)
Hybrid-Cloud Orchestration	Provide seamless, policy-driven workload bursting to EU-compliant public clouds (AWS, Azure, GAIA-X) with zero-trust networking	Leverages the hybrid cloud foundation (Section 5) and the governance framework (Section 4)

These pillars will be pursued through a **phased rollout** that respects the Center's existing governance, security, and financial models (Sections 4, 6, 7).

10.2 AI-Enabled Services

10.2.1 AI Platform as a Service (AI-PaaS)

- **What:** A self-service portal offering pre-configured JupyterLab, TensorFlow, PyTorch, and RAPIDS environments on the GPU-accelerated nodes (Section 5).
- **Why:** Researchers reported a 75 % increase in GPU utilisation (Section 8) but still face provisioning delays; AI-PaaS will cut VM spin-up time from 30 min to < 5 min.
- **How:**
  1. Extend the existing **Kubernetes** cluster with GPU-aware device plugins.
  2. Integrate **Keycloak** SSO (Section 6) for role-based access to AI resources.
  3. Deploy **AI-Ops** pipelines (Airflow + MLflow) for reproducible model training and serving.

10.2.2 AI-Driven Service Management

- Deploy **machine-learning models** on the HPC fabric to predict SLA breaches, ticket volume spikes, and anomalous network traffic.
- Models will be trained on historic incident data from the SOC (Section 6) and support tickets (Section 7), feeding automated alerts into the **Operational Steering Committee** (Section 4).

10.2.3 Research-Teaching-Industry Collaboration

- Establish a **AI Innovation Lab** that co-locates faculty, PhD students, and industry partners.
- The lab will pilot **federated learning** projects that respect data-privacy constraints enforced by the GDPR-aligned framework (Section 6).

10.3 Sustainability Roadmap

Milestone (Year)	Initiative	Expected Impact
2027	Deploy **AI-aware energy scheduling** that shifts non-urgent workloads to periods of high renewable generation (solar/wind)	Reduce compute-related CO e by ~5 %
2028	Expand **heat-reuse** from the liquid-cooled HPC racks to campus heating networks (building B-12, C-03)	Cut campus heating energy demand by ~2 %
2029	Introduce **circular-IT procurement**: mandatory refurbishment and resale of de-commissioned servers, with a 20 % increase in hardware reuse	Lower e-waste and procurement cost
2030	Achieve **Carbon-Neutral Compute** certification (ISO 14064) for the entire data-center footprint	Align with RWTH's Climate Action Plan (Section 4)

All sustainability actions will be tracked via the **green-IT KPI dashboard** already used for energy-per-TFLOP metrics (Section 8) and reported annually in the **Service Alignment Report** (Section 4).

10.4 Hybrid-Cloud Strategy

10.4.1 Federated Cloud Brokerage

- Implement a **policy engine** (OPA) that evaluates workload characteristics (data-sensitivity, latency, cost) and automatically selects the optimal execution environment: private OpenStack, on-prem Kubernetes, or a public EU-compliant cloud (AWS GovCloud, Azure EU, GAIA-X).

- The engine will respect the **Zero-Trust** networking model (Section 6) and the **data-classification** rules (Section 6).

10.4.2 Cloud-Native Service Catalog

- Extend the existing **self-service portal** (Section 7) with a catalog of **cloud-native services** (serverless functions, managed databases, AI inference endpoints).

- Each service will expose **usage-based charge-back** metrics, addressing the financial transparency lessons learned in Section 9.

10.4.3 Resilience & Compliance

- Leverage **multi-region replication** across EU clouds to meet data-sovereignty requirements and provide disaster-recovery RPO $<$ 15 min.

- Continuous compliance monitoring will be integrated into the existing **SIEM** and **policy-as-code** pipelines (Section 6).

10.5 Continuous Improvement Framework

The roadmap embeds the **Data-Driven Continuous Improvement Cycle** (Section 9) into every initiative:

1. **Plan** - Define KPI targets (e.g., AI-PaaS provisioning time $<$ 5 min, carbon intensity $<$ 0.30 kg CO e/kWh).

2. **Do** - Deploy pilots in a controlled environment (e.g., one faculty department).

3. **Check** - Collect telemetry from the **KPI dashboards**, user NPS surveys (Section 7), and compliance logs (Section 6).

4. **Act** - Refine policies, adjust resource allocations, and scale successful pilots university-wide.

Governance bodies will review progress quarterly:

- **Strategic Advisory Council** - validates alignment with university policy and sustainability goals.

- **Operational Steering Committee** - monitors SLA compliance and resource utilisation.
- **Annual Review Panel** - audits financial sustainability and compliance outcomes.

10.6 Timeline Overview

Year	Q1	Q2	Q3	Q4
2026	Finalise AI-PaaS architecture; set up AI Innovation Lab governance	Deploy pilot AI-PaaS for 3 research groups	Integrate AI-Ops monitoring; begin AI-driven ticket prediction	Publish first AI-PaaS usage report
2027	Launch AI-PaaS university-wide; start AI-driven service management	Implement energy-aware scheduling; pilot heat-reuse in one building	Expand federated cloud brokerage to include Azure EU	Review sustainability KPIs; adjust targets
2028	Roll out cloud-native service catalog; introduce usage-based charge-back	Scale heat-reuse to additional buildings	Conduct ISO 14064 audit; publish carbon-neutral roadmap	Update governance documents to embed new policies
2029	Full hybrid-cloud orchestration across all faculties	Deploy circular-IT procurement program	Publish mid-term impact assessment (research, teaching, admin)	Refine AI-PaaS based on user feedback
2030	Achieve Carbon-Neutral Compute certification	Consolidate all AI services under a single governance model	Complete roadmap evaluation; set next-decade vision	Celebrate milestones; disseminate best-practice guide for other universities

10.7 Expected Outcomes

- **Research:** 30 % reduction in time-to-insight for AI-intensive projects; 20 % increase in cross-faculty AI collaborations.
- **Teaching:** 25 % more courses offering AI-enhanced labs; higher student satisfaction (NPS + 15 points).
- **Administration:** 15 % cost savings from usage-based charge-back and circular-IT; improved GDPR audit scores (zero critical findings).
- **Sustainability:** 30 % lower carbon intensity of compute workloads; alignment with RWTH's 2030 climate targets.

These outcomes will be measured against the **KPIs** already established in Sections 4, 5, 6, 7, and 8, ensuring that the Future Directions remain **data-driven**, **transparent**, and **aligned** with the university's overarching mission.

11. Conclusion

11.1 Summary of Findings

The analysis of the IT Center demonstrates how a centrally governed, service-oriented IT organization can simultaneously advance **research**, **teaching**, and **administration** at a large, research-intensive university.

- **Strategic Alignment** - The Center's three-fold core objective (Section 3) is embedded in a hierarchical governance model (Section 4) that links every service line to the university's "Digital Excellence" vision (Section 1).

- **Robust Technical Backbone** - A tiered hardware platform, spine-leaf network, hybrid cloud ecosystem, and unified software stack (Section 5) deliver the performance, reliability, and sustainability required for high-performance computing, virtual labs, and enterprise applications.

- **Security & Compliance** - Defence-in-depth controls, GDPR-aligned data-classification, and ISO/IEC certifications (Section 6) protect sensitive research data while enabling rapid, trusted access.

- **Service Delivery Excellence** - Integrated help-desk, self-service portals, and SLA-driven monitoring (Section 7) translate technical capabilities into measurable user satisfaction and operational efficiency.

- **Demonstrated Impact** - Quantitative gains include a 25 % increase in HPC capacity, a 17 % rise in e-learning participation, and a 33 % reduction in enrolment-process time (Section 8).

- **Learning from Challenges** - Operational scaling, financial flexibility, and cultural adoption issues (Section 9) yielded concrete lessons that shaped the future roadmap (Section 10).

Collectively, these findings confirm that the IT Center is a **catalyst for digital transformation** across the university's core missions.

11.2 Significance for RWTH Aachen's Mission

The Center directly fulfills the mission articulated in the Introduction (Section 1) and the historical drivers outlined in Section 2:

1. **Research Support** - By expanding HPC resources, providing FAIR-compliant data services, and introducing AI-enabled platforms (Section 10), the Center enhances RWTH's competitiveness for national and EU research funding.

2. **Teaching Innovation** - Low-latency campus networks, self-service virtual labs, and SSO-driven access have increased digital-tool adoption and improved instructor NPS, supporting the university's goal of high-quality, technology-enhanced education.

3. **Administrative Efficiency** - Streamlined enrolment processing, automated invoice handling, and transparent charge-back models reduce manual effort and operational costs, aligning with the university's sustainability and cost-control objectives.

Moreover, the Center's **green-IT measures** (Section 5, Section 10) contribute to RWTH's Climate Action Plan, demonstrating that high-performance digital services can be delivered responsibly.

11.3 Broader Implications for Higher-Education IT Management

The RWTH Aachen experience offers a replicable blueprint for other research-intensive institutions:

Dimension	Transferable Insight	Evidence from RWTH Aachen
Governance	Layered decision bodies (Management Board, Advisory Council, Steering Committee) enable rapid technical change while preserving policy compliance.	Section 4
Financial Model	Zero-based budgeting combined with a contingency pool and usage-based charge-back balances cost discipline with research agility.	Section 9
Service Portfolio Design	Mapping each service category to at least one core objective ensures strategic relevance and measurable impact.	Section 3

Dimension	Transferable Insight	Evidence from RWTH Aachen
Security Integration	Embedding security policies in the university-wide Policy Alignment Framework creates a unified defence-in-depth posture.	Section 6
Sustainability as Service	Treating green-IT initiatives as a budgeted service line with dedicated KPIs drives measurable carbon-intensity reductions.	Section 10
Continuous Improvement	Real-time KPI dashboards, user-voice portals, and PDCA cycles close the feedback loop between operations and strategy.	Sections 4, 7, 8

These principles illustrate that **centralized, yet stakeholder-centric IT management** can deliver high performance, compliance, and sustainability without sacrificing academic autonomy.

11.4 Closing Remarks

The IT Center has evolved from a fragmented collection of legacy services into a **strategic, innovation-driving hub** that underpins RWTH Aachen's ambition of digital excellence. Its success rests on a coherent alignment of mission, governance, architecture, security, and service delivery - each reinforced by data-driven continuous improvement.

Looking ahead, the roadmap (Section 10) positions the Center to lead in AI-enabled services, advanced sustainability, and hybrid-cloud orchestration, ensuring that RWTH Aachen remains at the forefront of digital research and education in Europe.

The lessons distilled here provide a **roadmap for other universities** seeking to transform their IT landscapes into engines of academic and societal impact.