Businesses’ security needs are changing rapidly. On the one hand, companies need to block malicious attacks on their computer systems and data. On the other hand, they have to enable internal and external access to data, but only in a strictly defined and controlled manner. In the past, networks, systems and applications were protected by point solutions. But that is no longer enough. Enterprises today need to view their organizational structures and processes holistically and take an integrated approach to IT and telecommunications. And there are a variety of other, organizational issues to be considered, such as corporate governance systems, risk management, corporate culture, organizational models, and compliance with legal and regulatory requirements, contracts, and internal policies. A comprehensive security management system encompasses and addresses all of the above. ICT Security Services from T-Systems are a complete, modular range of security solutions that provide ideal support for your business and are precisely tailored to your needs.

Support & Enabling Services complement and round off T-Systems’ portfolio. Onsite Services support the customer in the field and on site with standardized ICT solution building blocks (service cluster). Service Desk Services give the customer consistent support with the same contact person throughout the handling of an inquiry. Transparency and improvement of the ICT infrastructure and processes are permanent tasks. Application Performance Management is an end-to-end analysis and monitoring tool that shows the customer’s critical business processes from the user’s perspective. ICT Security Services from T-Systems help companies handle the ever-growing danger from cyber attacks.
We offer you comprehensive services of all kinds – from business-process level downwards and from security policies and models to the realization of concrete systems. T-Systems tests the level of security achieved, performs threat and risk analysis, develops architectures and solutions, and produces detailed lists of tasks and activities.

We also implement information security management systems, e.g. in compliance with ISO 27001.

1. ENTERPRISE SECURITY MANAGEMENT

Security must be regarded today as an integral part of operational risk management. The principles and standards drawn up in an effort to protect organizations, their business processes and their ICT systems are only enforceable in practice if they are completely embedded in those business processes. T-Systems designs and implements technical solutions on the basis of a multi-stage refinement process. Once in place, they ensure compliance with all in-house policies and regulatory requirements.

**Architecture and processes:** Defines the principles, standards and processes, and creates the framework for the corresponding systems. Project and program management methods provide the necessary structural framework. Design and development of architectures, security concepts, systems and software for different use cases including specific key management solutions.

**Applications, risk and compliance:** For identifying and evaluating risks and planning countermeasures. Entails auditing organizational structures and making all applications as secure as possible. An assessment of your systems and products helps eliminate security gaps right from the start and comply with data-protection and governance requirements.

**Security and vulnerability management:** Only threats that have been identified and evaluated can be reliably prevented. Having accomplished this step, an organization can then develop plans for responding to security incidents. ICT-aided compliance reporting, visualizations and forensic techniques help to block threats of every kind.

2. IDENTITY AND ACCESS MANAGEMENT

In today’s interconnected world, increasingly intensive and complex collaboration within and beyond company boundaries has become the norm. Identity and Access Management lay the foundations required to use ICT resources and applications in a controlled way. At the heart of this solution are digital identities, roles and permissions that provide secure access to business processes both within and between enterprises. Outsourcing and cloud (dynamic) services cannot be implemented without access control mechanisms. What’s more, IAM brings flexibility and productivity to an organization’s change processes.
**Users and identities:** The creation of digital identities, definition of permissions, and automated validation enable you to control access to ICT resources.

**Smart cards:** A security module and an organizational tool in one. These compact all-rounders are employed both for basic and for custom functionality, e.g. identification systems.

**Trust centers:** The secure generation and verification of digital identities forms the basis for reliability and trust. Digitally sign and encrypt your messages by means of Public Key Infrastructure technology – either as a service or as a dedicated system. SSL certificates ensure effective protection of data transmissions.

### 3. ICT INFRASTRUCTURE SECURITY

Enterprises need to shield their ICT infrastructures from threats, identify attacks on their systems, applications and networks, and protect their data and data streams. In light of the trend toward mobility, there is a demand for flexible solutions that enable secure access to corporate networks and applications, and secure data exchange. We provide solutions that protect your ICT systems, filter your data streams, and manage and control the flow of information. For this purpose we use VPN and firewall solutions, anti-virus, anti-spam and other filtering solutions, intrusion detection and prevention, and solution components for mobile ICT and secure communications.

**Desktop environment security:** Users process their data locally, accessing servers from their desktop environments via networks. Various protective and control mechanisms are employed, such as content security, encryption of data and hardware, and secure virtual desktop environments and device security offerings.

**Host and storage security:** Data is processed and stored on servers. It is essential to safeguard the integrity of IT systems and protect services. The main protective mechanisms comprise (mainframe) content security, managed anti-spam services (cloud service) and Security Application Services.

**Network security:** Networks connect users and applications and transport all data. As a result, they represent a potential gateway for malicious attacks and are a central issue for security activities. T-Systems’ offering comprises services at technical and functional levels, management, provisioning, maintenance and professional services modules. These leverage solutions and services that prevent unauthorized and malicious manipulation of the IT components in your networks. NSS offers a secure connection between your intranet and the public internet, as well as secure connections between affiliated companies, branch offices and business units.

**Physical security:** Comprises building security solutions such as video surveillance, physical access control, intrusion and fire alarm systems and even a control center service. The technological features and functionality you require are provided together with the management modules you select. The following functionality options are available: network transport protection, content security protection, operating, provisioning, and related maintenance and project services.

### ALL ADVANTAGES AT A GLANCE

**Benefits**

- We support you at every stage of the process of implementing complex systems – from plan, to build, to run. You benefit from having a system protected by rock-solid security that meets your specifications at every point. This creates added value throughout your value chain. You gain optimized processes, lower costs and improve your profitability.

**Enabling growth**

- Your business processes become more flexible thanks to the availability of data and applications from anywhere, including access via mobile devices
- You can easily establish new online business models thanks to secure identity verification and collaboration
- You can quickly and reliably adapt your organizational structures to new market requirements

**Savings**

- Protection of investment in knowledge and ICT infrastructures
- Lower costs due to disruptions to your operations
- Lower damages due to noncompliance with legal requirements and security incidents
- Corporate risks become calculable
- Greater quality and lower costs for corporate security thanks to Managed Security Services

**Operating models**

As one of the world’s largest outsourcing service providers, T-Systems can either assume end-to-end responsibility for operating your security systems, or carry out administration, updates and maintenance tasks for your in-house systems (Security Management Center, remote management and outtasking). Our Managed Security Services also include device security management.

**International availability**

T-Systems employs around 600 security specialists with extensive certification for the external market, and maintains a presence in 25 countries. We operate six international Security Operations Centers and continuously expand our offering in line with customer requirements.
ICT SECURITY SERVICES FROM T-SYSTEMS

WHY T-SYSTEMS?

T-Systems is the leading German provider of ICT Security solutions. For more than two decades, we have been assisting government agencies and enterprises in all industries. They benefit from the experience we have gained in many large-scale projects, and can rely on the quality and objectivity of our advice and evaluations. We provide a comprehensive range of ICT security services, taking a holistic approach to each organization, its processes and technological resources. Customers receive services throughout their value chains, including consulting, development/integration, products and operations services. They benefit from a tightly meshed set of services and solutions that meet all your needs in terms of security and the fulfillment of statutory governance and compliance requirements.

T-Systems is accredited with the Federal Office for Information Security (BSI), with VISA International, MasterCard International, PCI and many other organizations worldwide.

SELECTED PARTNERS AND SUPPLIERS

CERTIFICATES, ACCREDITATIONS, QUALIFICATIONS

- ISO 9001
- ISO 14001
- ISO 20000
- ISO 27001
- OHSAS 18001
- PCI-DSS
- CISSP
- BSI IT-Grundschutz
- ISAE 3402
- CISM
- CISA
- CRISC
- ITIL
- T.I.S.P.

References:

EADS
- Compliance with very strict security requirements for development work in international high-tech projects
- Secure data exchange
- Granular access permissions with needs-based registration for employees
- Granular security based on a company-wide Public Key Infrastructure

SIMKO FOR GERMAN GOVERNMENT AGENCIES
- “Enabling secure mobile communications” (SIMKo technology) for the German government and its agencies, featuring end-to-end protection – from back-end systems to smartphones
- All data, software and operating systems are encrypted
- Recommended by the BSI for applications requiring “restricted” security level (VS-NfD)

ANVIS GROUP
- Innovative identity management speeds up administration processes and saves costs
- Proven cloud concept for easy user management
- Automated processes save time and money
- Solution can be put to use immediately and is suitable for companies of any size
- Introduction at a fixed price quickly pays off
- Audit-proof logging, comprehensive reporting
- Compliant, high operational security

MORE INFORMATION
Internet: www.t-systems.com

EXPERTS CONTACT
Bernd König
Am Propsthof 51
53121 Bonn
E-mail: bernd.koenig@t-systems.com

PUBLISHED BY
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main
Germany