Choose certainty.
Add value.

Developing a Cyber Security Strategy

Presented by:
Martin Voelk, Senior Secuirty Analyst
TÜV SÜD America
October 3, 2017

TÜV SÜD at a glance

150+
YEARS OF
QUALITY, SAFETY
& SUSTAINABILITY

1,000
LOCATIONS
WORLDWIDE

€2.3
BILLION
IN ANNUAL
REVENUE

24,000
EMPLOYEES

43%
OF REVENUE
OUTSIDE GERMANY

574,000
CERTIFICATES

100%
INDEPENDENT &
IMPARTIAL

1 -STOP
SOLUTIONS
PROVIDER

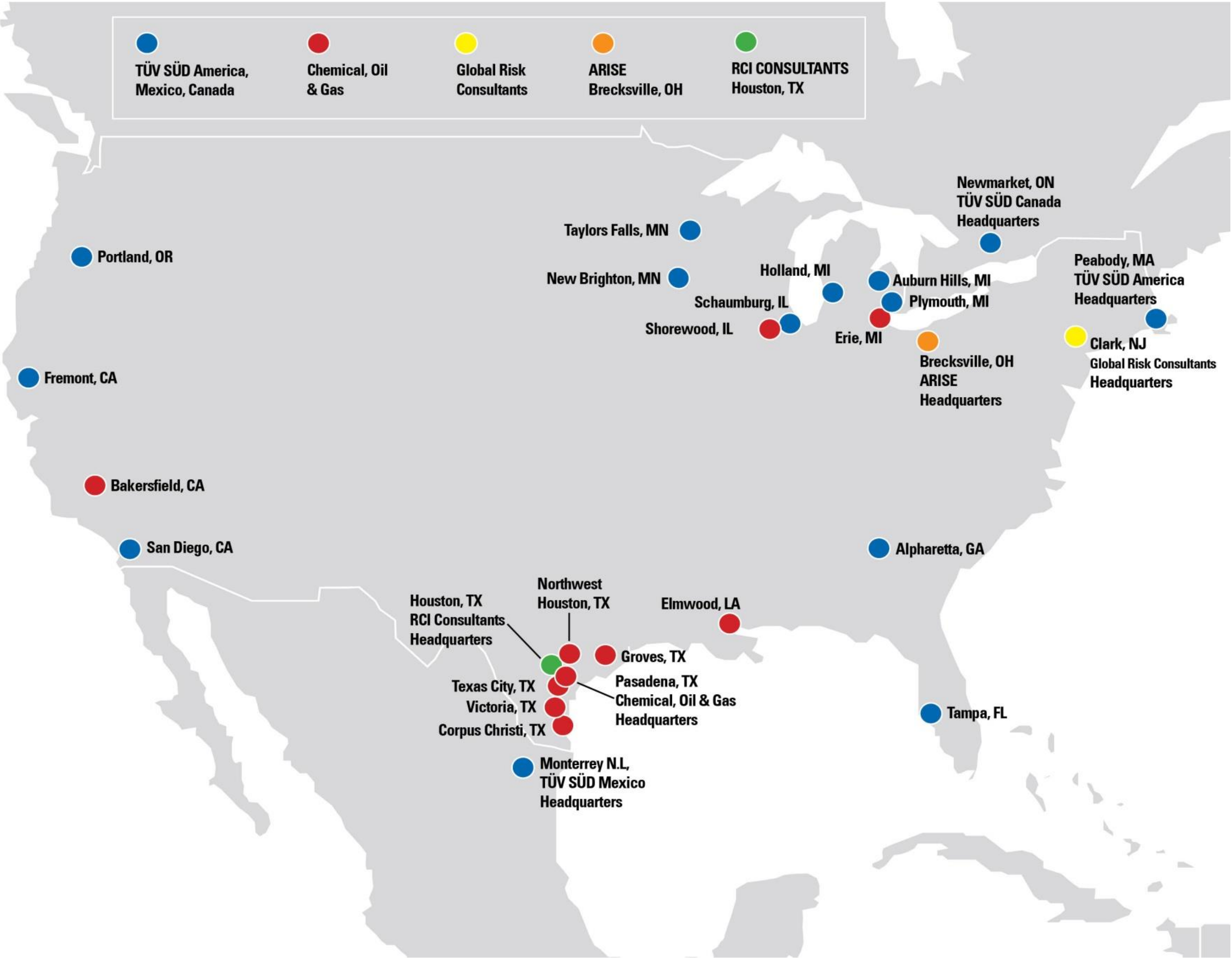
Note: Figures have been rounded off.

TÜV SÜD America Inc.

- TÜV SÜD America Inc., founded in 1987, is the North American subsidiary of TÜV SÜD AG.

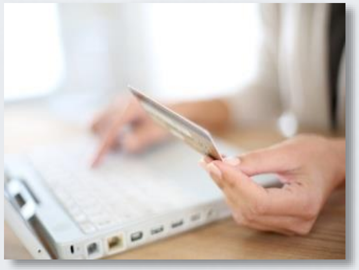
- TÜV SÜD America Inc. provides complete services through its divisions:
  - Management Service
  - Product Service
  - Industry Service
  - Chemical, Oil & Gas
  - Global Risk Consultants (GRC)
  - RCI Consultants

TÜV SÜD America locations


● TÜV SÜD America, Mexico, Canada
● Chemical, Oil & Gas
● Global Risk Consultants
● ARISE Brecksville, OH
● RCI CONSULTANTS Houston, TX
Newmarket, ON TÜV SÜD Canada Headquarters
Taylors Falls, MN
Portland, OR
New Brighton, MN
Holland, MI
Auburn Hills, MI
Plymouth, MI
Peabody, MA TÜV SÜD America Headquarters
Schaumburg, IL
Shorewood, IL
Erie, MI
Brecksville, OH ARISE Headquarters
Clark, NJ Global Risk Consultants Headquarters
Fremont, CA
Bakersfield, CA
San Diego, CA
Alpharetta, GA
Northwest Houston, TX
Houston, TX RCI Consultants Headquarters
Elmwood, LA
Groves, TX
Texas City, TX
Victoria, TX
Corpus Christi, TX
Pasadena, TX Chemical, Oil & Gas Headquarters
Tampa, FL
Monterrey N.L, TÜV SÜD Mexico Headquarters

Digital transformations are extending to all value processes, changing business models and increasing the digital risk for all industries

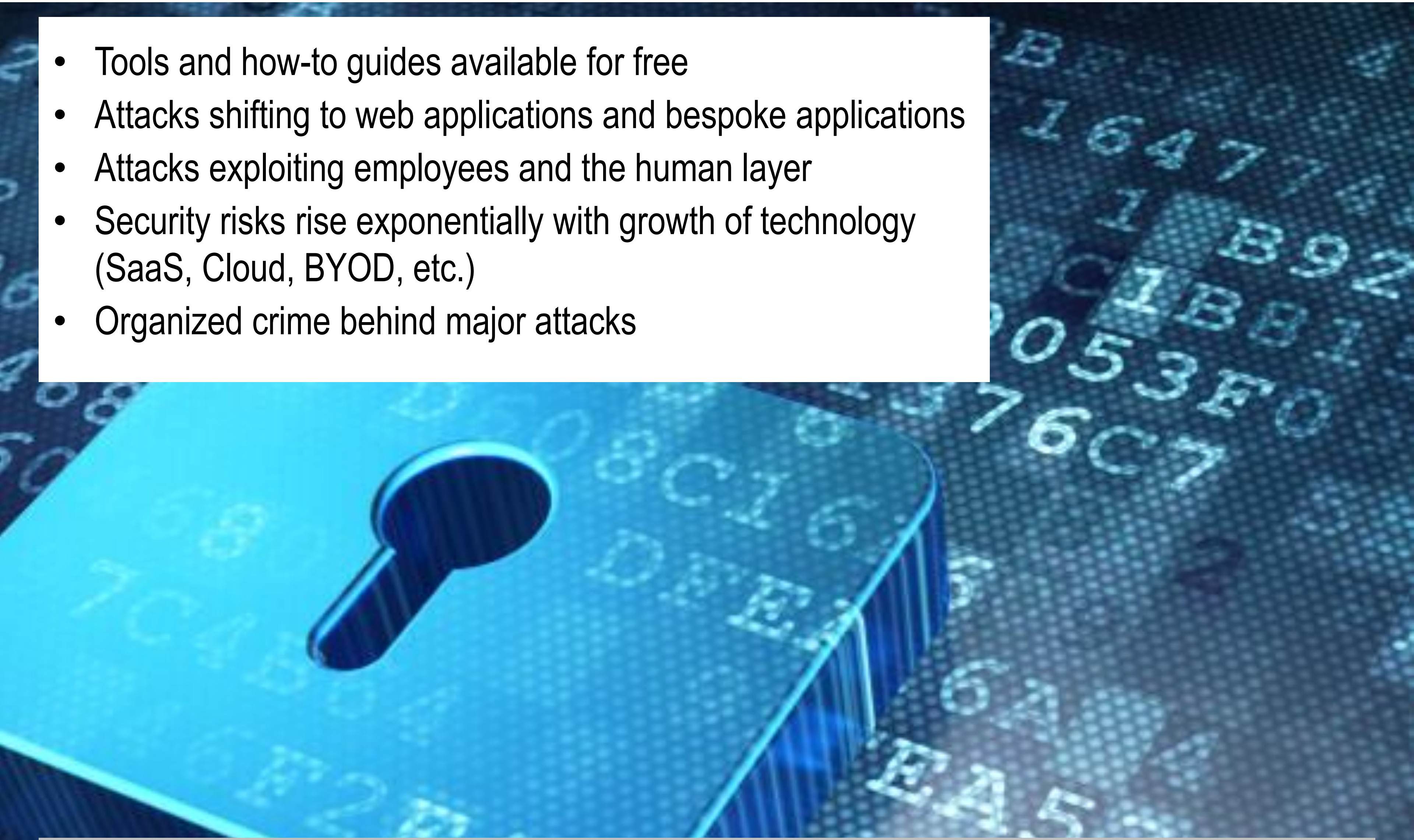
Digital risk has been extending across value processes and industries

	1990s	2000s	2016 & beyond
Industries	**Banks** 	**Online shops** 	**Critical infrastructure**
Processes	▪ Digital processes ▪ Integrated processes ▪ Online services	▪ Big data ▪ Smart data ▪ Digital assets	▪ Connected devices ▪ Mobile services ▪ Mobile transactions

Global Awareness: Facts & Figures

- 49% increase in targeted attacks in 2016
- 67% of large corporations infected with malware bots
- 50 million reported breaches per month (tip of the iceberg)
- 5 Zero Day vulnerabilities per month
- Cyber Crime cost an estimates $150 Billion per year
- UK, US and EU corporations in top 5 hit lists
- New exploits are discovered daily
- Web applications make up 70% of Tech breaches
- Human weakness & insiders allow most breaches

Cyber security breaches made easy



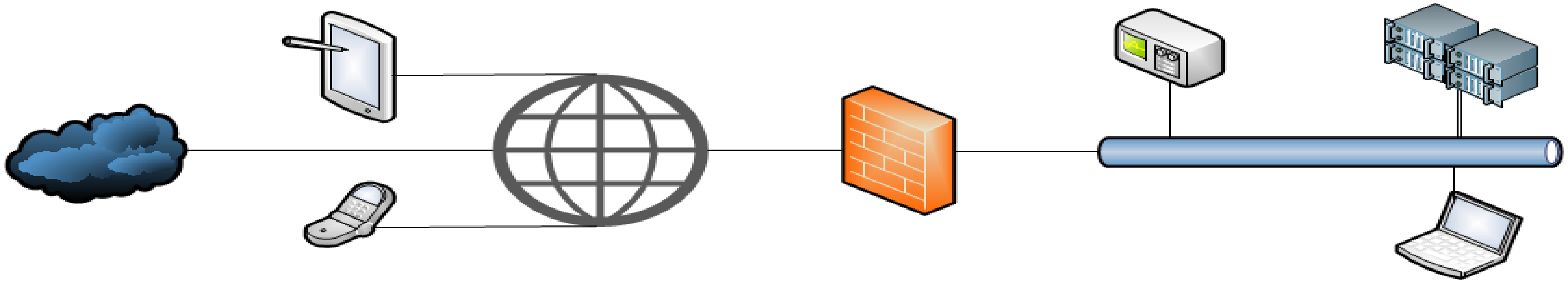
- Tools and how-to guides available for free
- Attacks shifting to web applications and bespoke applications
- Attacks exploiting employees and the human layer
- Security risks rise exponentially with growth of technology (SaaS, Cloud, BYOD, etc.)
- Organized crime behind major attacks

Who is at risk?

Cybercrime climbs to 2nd most reported economic crime affecting 32% of organizations.[1]

[1]PWC Global Economic Crime Survey 2016

Who is at risk?



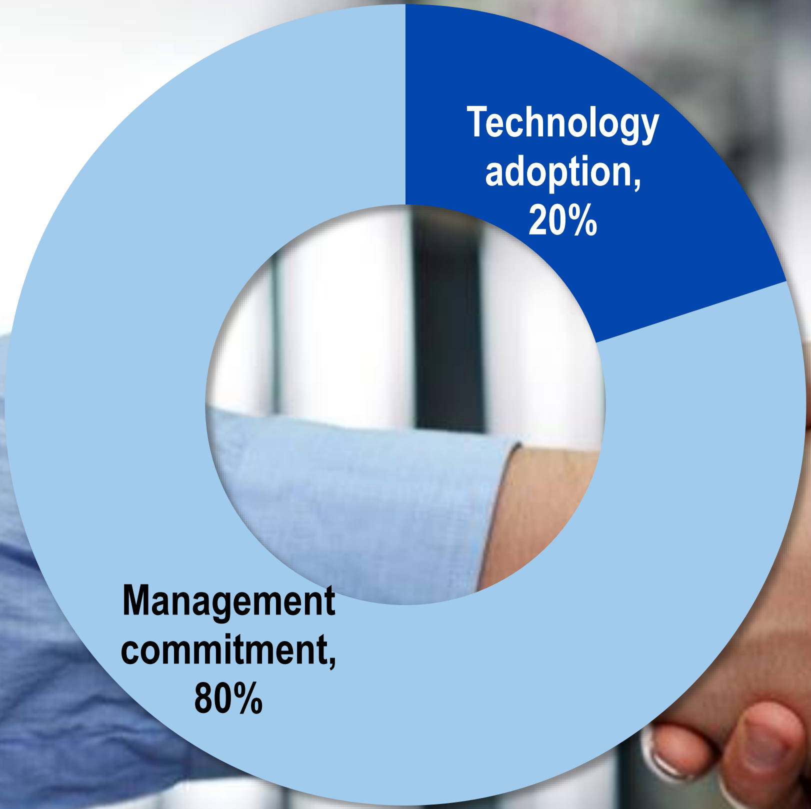
Cloud	Mobile & Wireless	Internet	Security Boundary	Management & Applications	Servers, Workstations
Confidentiality Authorization Violation Unauthorized Use	Authorization Violation EM/RF Interception Theft	Denial Of Service (Dos) Eavesdropping Confidentiality Intercept / Alter Masquerade Replay Traffic analysis	Bypassing Controls Physical intrusion Resource exhaustion Service spoofing	Indiscretions By Personnel Integrity Violation Media scavenging Repudiation Theft Trapdoor Trojan horse	Authorization Violation Unauthorized Use

Who is at risk?

- 68% of companies don't believe their organizations have the ability to remain resilient in the wake of a cyberattack.[1]
- Company size does not matter – attacks have happened at large entities and businesses to small business owners that could be financially devastated from the fallout and losses incurred from a cyber-attack.
- 60% of all attacks were carried out by insiders
- Nearly 100% of all AP encryption can be hacked by an attacker
- 70% of all technical attacks are based on web applications

[1] *The Second Annual Study on the Cyber Resilient Organization. Independently conducted by Ponemon Institute LLC.*

Achieve your IT Security Management objectives through management commitment and technology adoption



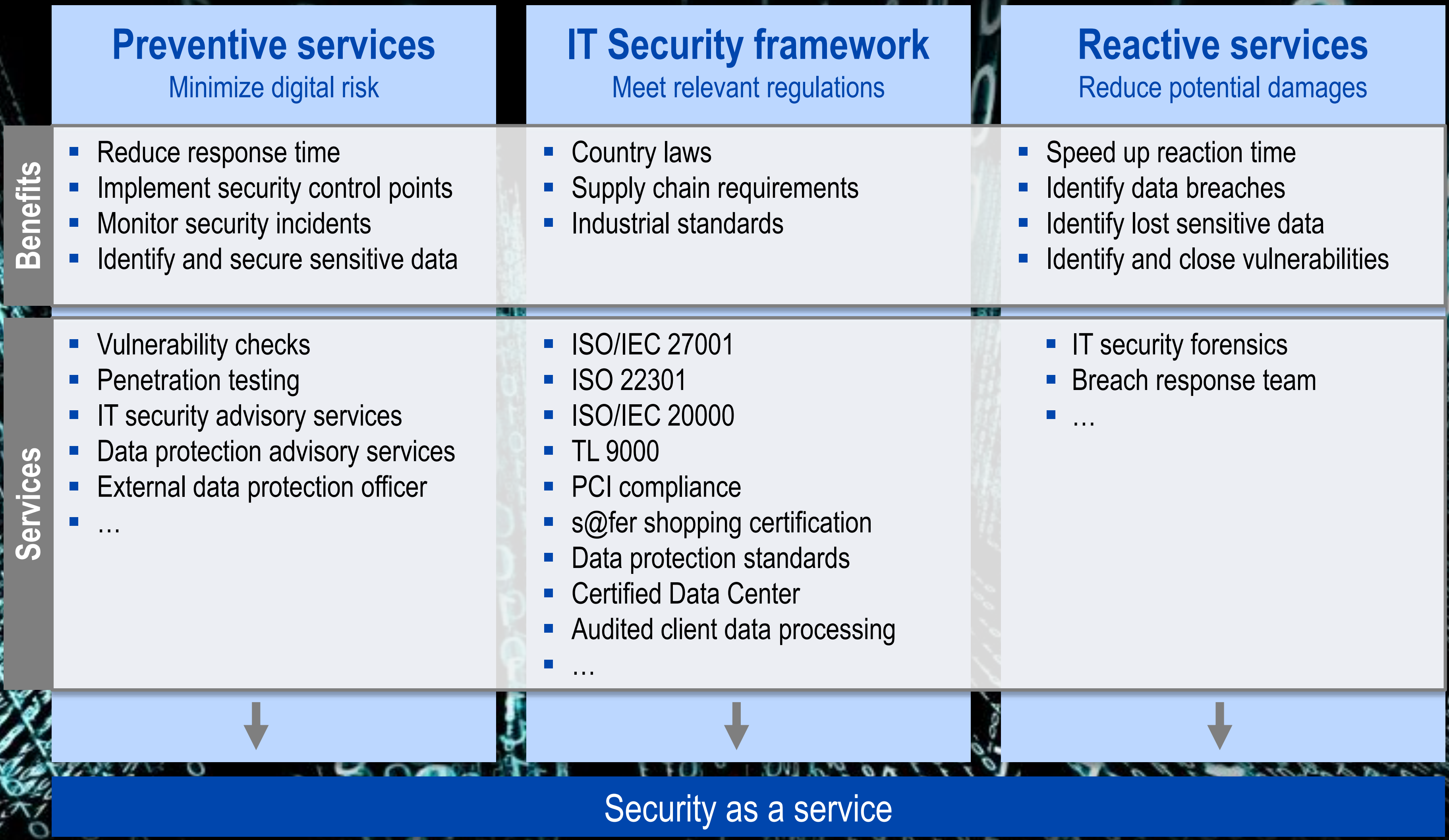
80% management commitment

- Draw up requirements
- Define responsibilities
- Raise awareness
- Define processes
- Measure/report/evaluate
- Derive measures
- Ensure continuous improvement

20% technology adoption

- Systems, tools, architecture etc.

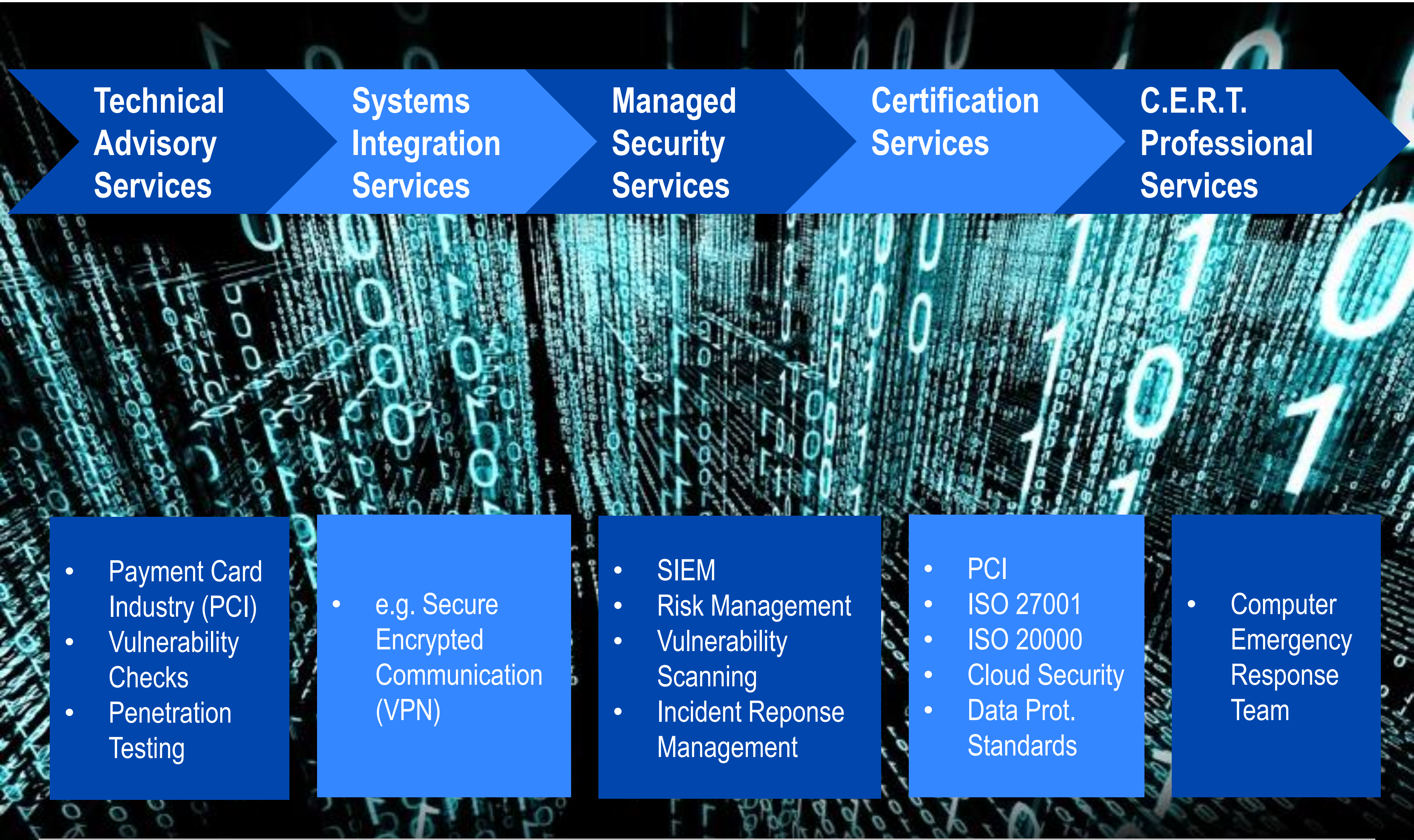
With the increasing threat landscape, a comprehensive IT security strategy can help to reduce potential damage



	Preventive services Minimize digital risk	IT Security framework Meet relevant regulations	Reactive services Reduce potential damages
Benefits	▪ Reduce response time ▪ Implement security control points ▪ Monitor security incidents ▪ Identify and secure sensitive data	▪ Country laws ▪ Supply chain requirements ▪ Industrial standards	▪ Speed up reaction time ▪ Identify data breaches ▪ Identify lost sensitive data ▪ Identify and close vulnerabilities
Services	▪ Vulnerability checks ▪ Penetration testing ▪ IT security advisory services ▪ Data protection advisory services ▪ External data protection officer ▪ …	▪ ISO/IEC 27001 ▪ ISO 22301 ▪ ISO/IEC 20000 ▪ TL 9000 ▪ PCI compliance ▪ s@fer shopping certification ▪ Data protection standards ▪ Certified Data Center ▪ Audited client data processing ▪ …	▪ IT security forensics ▪ Breach response team ▪ …

Security as a service

TÜV SÜD Cyber Security Portfolio



Technical Advisory Services

- Payment Card Industry (PCI)
- Vulnerability Checks
- Penetration Testing

Systems Integration Services

- e.g. Secure Encrypted Communication (VPN)

Managed Security Services

- SIEM
- Risk Management
- Vulnerability Scanning
- Incident Reponse Management

Certification Services

- PCI
- ISO 27001
- ISO 20000
- Cloud Security
- Data Prot. Standards

C.E.R.T. Professional Services

- Computer Emergency Response Team

IT security framework
ISO/IEC 27001

What is ISO/IEC 27001?

- ISO/IEC 27001 is the leading international standard for information security management.
- Its intention is to bring information security under explicit management control.

Who should use ISO/IEC 27001?

- Commercial or governmental organizations with sensitive data.
- Key industries include critical infrastructure industries (e.g. IT, telecom, financial services, etc.) though the standard is not limited to these industries.

Why is ISO/IEC 27001 important?

- Identification and management of risks to key information and systems assets.
- Review of information security practices.
- Acts as a marketing tool.

IT security framework
TL 9000

What is TL 9000?

- Quality management system developed by QuEST Forum based on the ISO 9001 system
- Designed to meet the supply chain quality requirements of the telecommunications industry by providing a consistent quality benchmarks.

Who should use TL 9000?

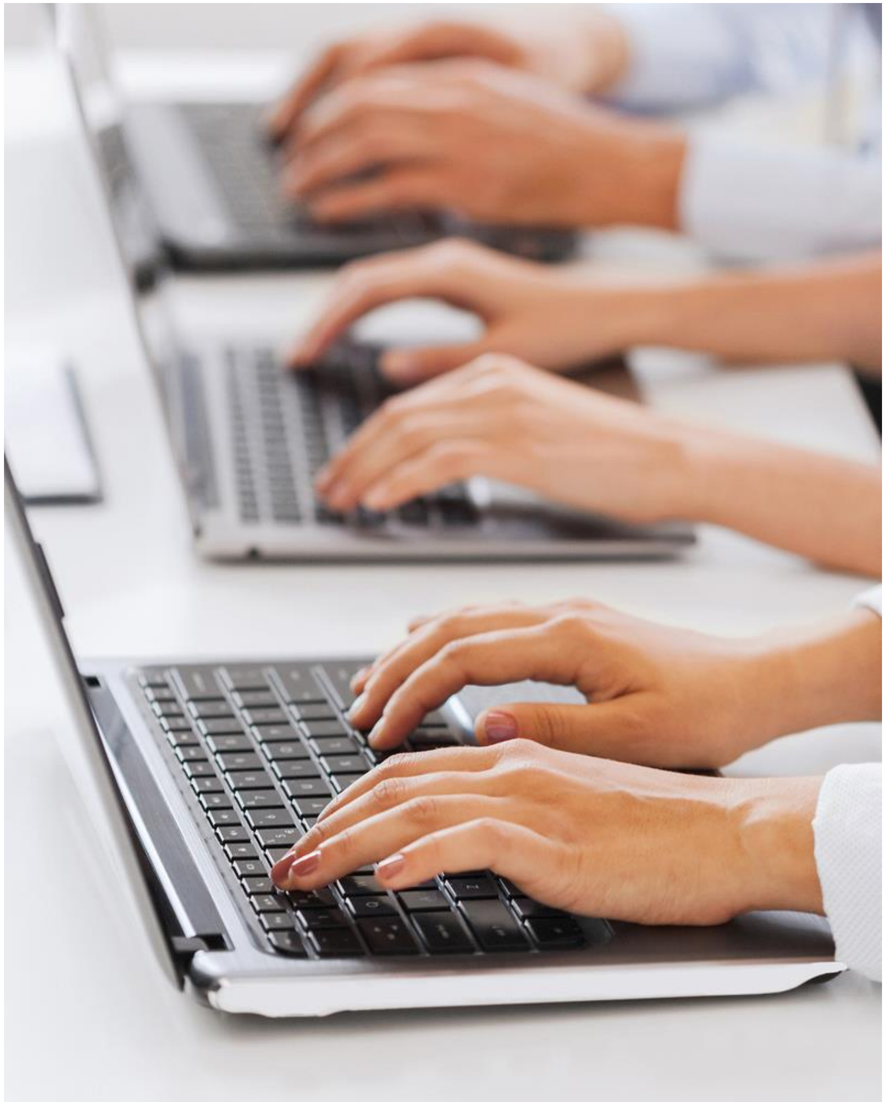
- Companies in the telecommunications industry as well as those that design networking hardware and software.

Why is TL 9000 important?

- Demonstrate compliance to the high standards required by the ICT industry.
- Validation the quality of your processes, products and services.

Preventive services

Vulnerability checks



What are vulnerability checks?

- Vulnerability checks are fully automated software based scans for common vulnerabilities.

Who should use vulnerability checks?

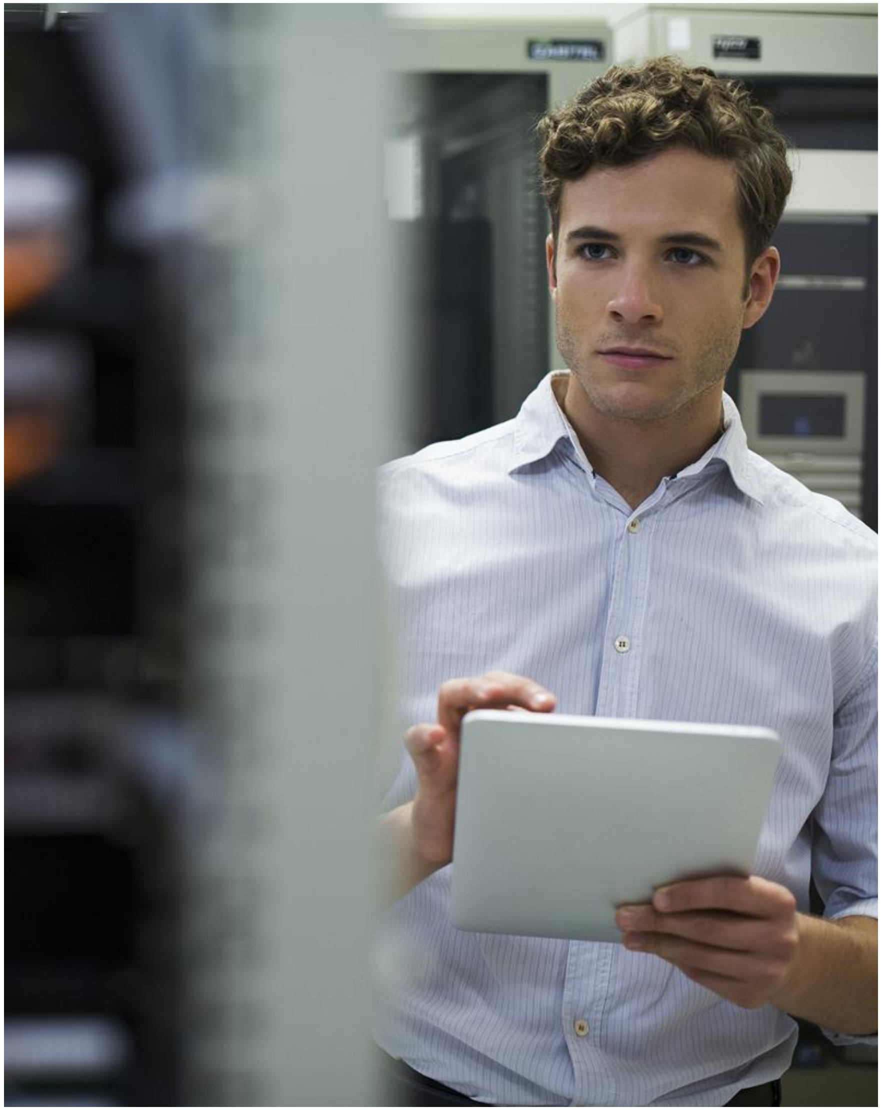
- All companies which use IT systems.

Why are vulnerability checks important?

- Vulnerability scans provide a quick overview on whether the tested systems are vulnerable to common exploits.

Preventive services

Penetration testing



What is penetration testing?

- Penetration testing assesses whether your IT systems are secure against potential external threats.
- It puts IT systems to the test by using the same methods that potential hackers would employ, revealing whether you're protected against real world attacks.

Who should use penetration testing?

- All companies dealing with sensitive information, especially high risk and critical infrastructure industries.

Why is penetration testing important?

- Independent penetration testing protects your knowledge and safeguards your assets and reputation.
- It minimises the risk of financial loss if your network is attacked, underlines your organisation's commitment to IT security, and creates confidence among the individuals and organisations you do business with.

IT- Security and Data Protection on a global basis

Description

TÜV SÜD offers worldwide auditing, assessment, validation and certification of management systems.

This encompasses various sectors and industries such as automotive, rail, aerospace, mechanical engineering, construction, metal production and processing, information technology and healthcare.

Our Solution

TÜV SÜD offers a wide variety of IT-Certification and IT-Security Services

Information security management

- ✓ ISO 27001
- ✓ ISO 20000
- ✓ PCI Compliance

IT Security Services

- ✓ Data Protection
- ✓ Penetration Testing
- ✓ Certified Data Center
- ✓ E-Commerce Security

Further more TÜV SÜD can support you with your internal standards, by offering:

- 2nd party audits for your suppliers/ dealer network

Added Value

- **One stop shop solution**: Global presence of TÜV SÜD experts auditors facilitates the IT-Security for global players.
- Experts and Auditors have **high level of qualification & many years of hands-on experience**
- **Identi*fi*cation of vulnerabilities** of customers IT-Systems with specific and clear **recommendations for actions**
- **Reduction of risk of loss of critical data** by monitoring your suppliers, service providers and your dealer network
- **High marketing potential** by using the TÜV SÜD certification mark.

Your business benefits

Detailed report including risk assessment

- Our experienced security experts will provide detailed documentation of the outcome of the penetration test and assess the risks of the identified vulnerabilities.

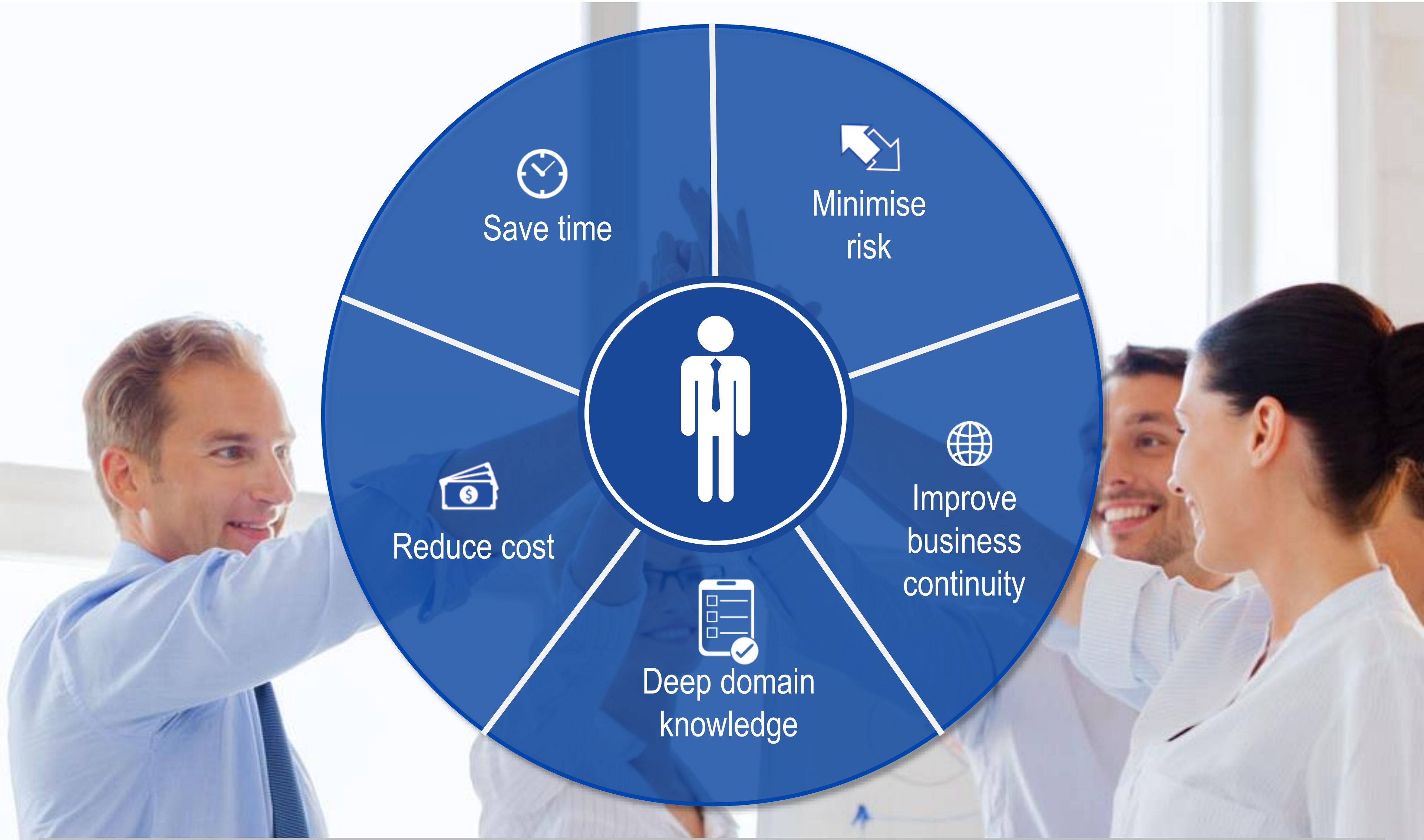
Suggestions for solutions /improvements

- By performing penetration tests, TÜV SÜD's experts not only expose security gaps; they also advise companies on how to close them and move towards next level.

Verification of the effectiveness of implemented actions

- Companies have the opportunity to verify the success and effectiveness of their corrective actions in a follow-up test.

Your business benefits



Why choose TÜV SÜD

One-stop solution	TÜV SÜD offers a wide variety of IT Certification and IT Security Services.
World wide network	Our global business network allow us to serve your local business operations.
Added business value	We identify your vulnerabilities with specific and clear recommendations for actions.
Quality experts	TÜV SÜD auditors and experts have high levels of qualification and years of hands-on experience.

The TÜV SÜD certification mark

The mark of distinction

- The TÜV SÜD certification mark demonstrates compliance to international standards or TÜV SÜD own requirements.

Benefits of the TÜV SÜD Cert Mark

- After passing certification, you can download your certification mark online.
- It can be used as a marketing tool on various channels to demonstrate your company’s commitment to quality and safety.

Flexible to your needs

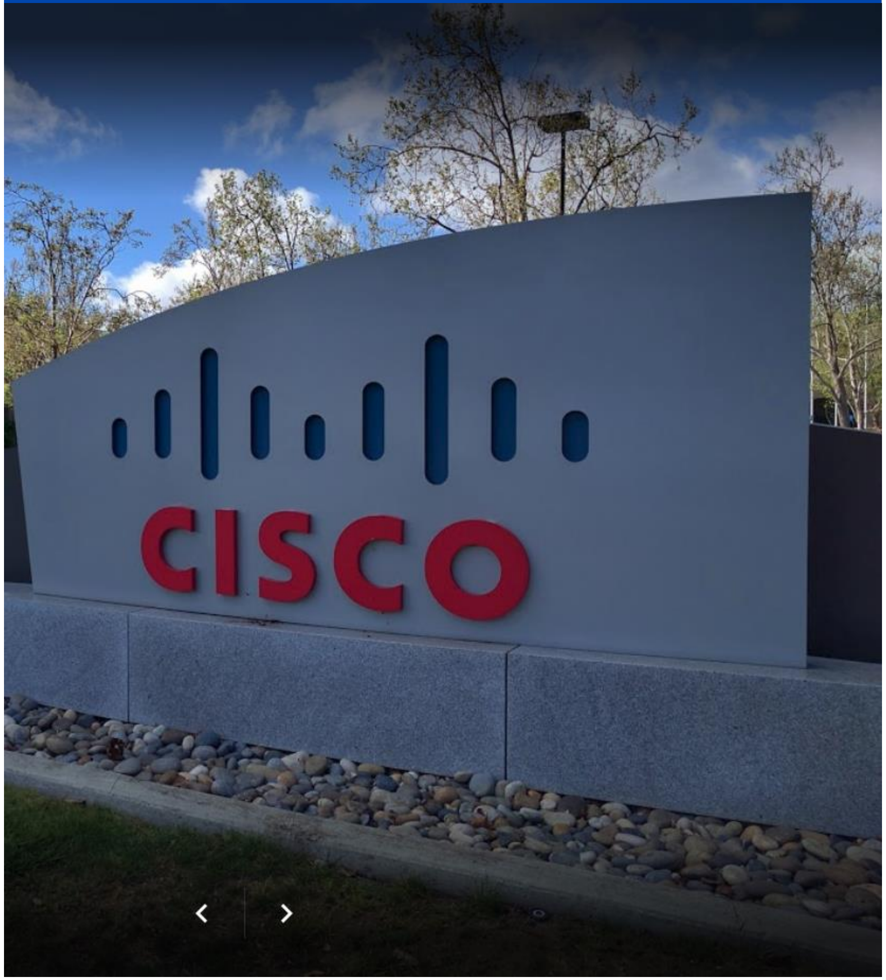
- Standalone, integrated or combination certification mark options to meet your system certification requirements.

TÜV
SÜD
ISO 27001

TÜV
SÜD
ISO 20000

Case study: Cisco Services, a group of Cisco Systems

Cisco



Business challenge

- Effective implementation of information security practices, minimizing the risk of information security breaches.

Our solution

- ISO 27001:2013 certification on a group-wide basis.

Business benefits to client

- An efficient and effective ISMS gives confidence to Cisco Services Top Management and its customers, partners and other stakeholders that the risk of information security incidents affecting the confidentiality, integrity and availability of their data is minimized.

Client references for IT security services and frameworks

TÜV SÜD

EUROLOG
the integration company for logistics

baden IT
Innovationstechnologie

SEW
EURODRIVE

Expedia.de™
Reisen – für dich gemacht

CROWN

LEW
TelNet

interhyp

BAUHAUS®

Südtiroler Informatik AG
Informatica Alto Adige SPA

DB
Mobility
Networks
Logistics

T&S
Teleconnect & Service

VFS GLOBAL

zalando.de

mehr als Energie
infra

EDAG

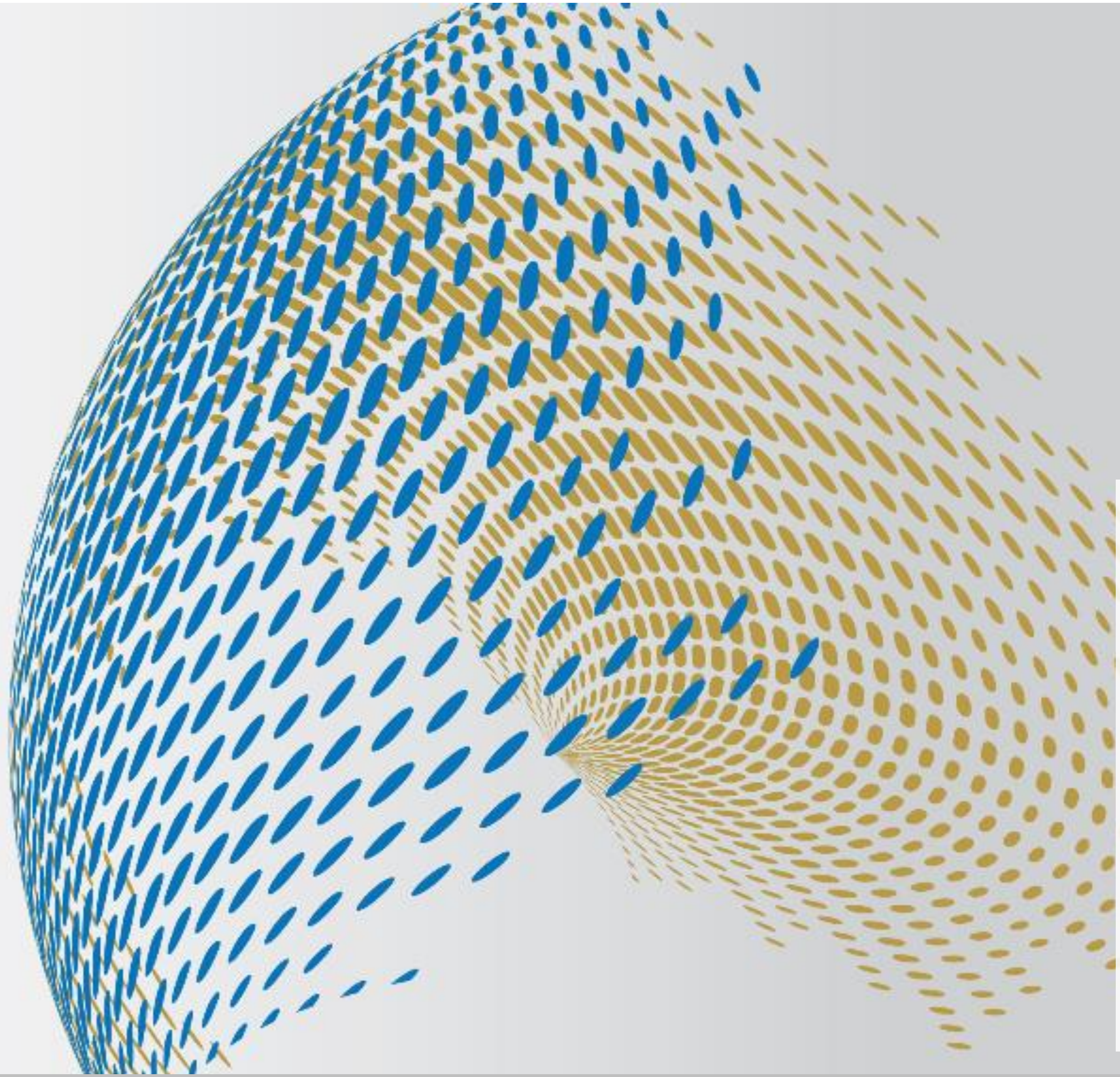
Salzburg AG

LOTTO
Baden-Württemberg

STRATO
RECHENZENTRUM

First Gulf Bank بنك الخليج الأول
عربي

Discover the advantages of partnering with TÜV SÜD America



Contact us:
www.tuv-sud-america.com
info@tuvam.com

Follow us on social media:

instagram.com/tuvsud

linkedin.com/company/tuv-sud

twitter.com/tuvsud

youtube.com/tuvsudgroup