# Quantum and Post-Quantum Security Integration and Migration

## *A Glimpse into the Future of Enhanced Infrastructure Complexity*

https://quant-x-sec.com | xb@quant-x-sec.com

image source: midjourney

10/10/23

xb@quant-x-sec.com

QUANT-X SECURITY & CODING

mastering digital complexity

# Who We are

*Founded in 2019 | Located at Hanover, Germany | 10 employees: Men and Women of Letters*

## IT EXPERTS / CONSULTING

- Information Security
- Project Management
- Software Engineering
- IT Operations

## RESEARCH & DEVELOPMENT

- Software Engineering
- Security Analyses & Proofs


xb@quant-x-sec.com

# Quantum Technology Related Activities

*“Preserve confidentiality, integrity and availability of data in the future”*

- Quantum and Post-Quantum Security Integration
- Quantum and Post-Quantum Security Migration
- Project Management for Infrastructure Changes
- Quantum Security Proofs and Validation

image source: iStock



xb@quant-x-sec.com

# R&D - Quantum and Post-Quantum Integration

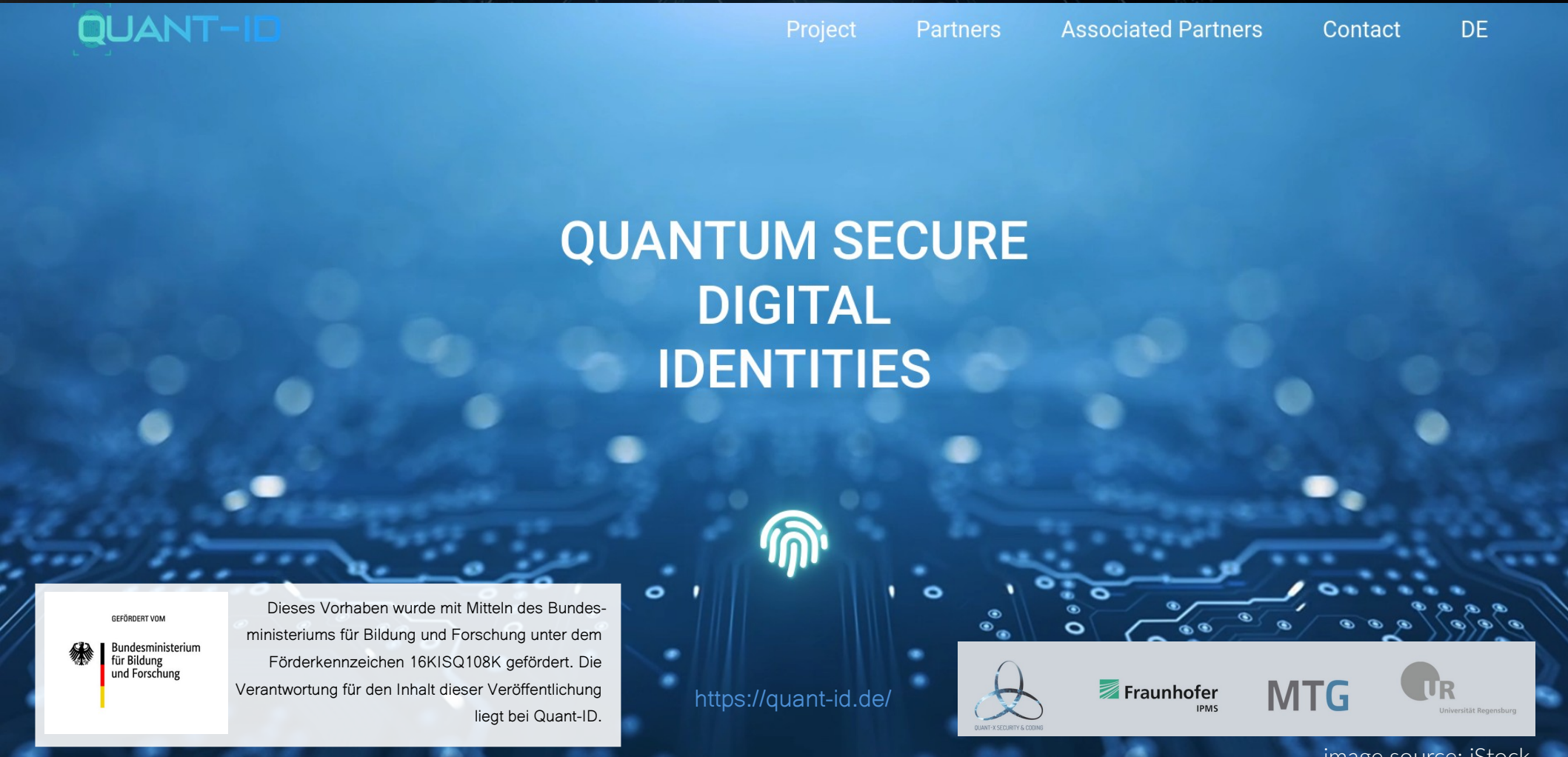



image source: iStock

# Quantum and Post-Quantum Security Migration

*Impact on Information Security Management*



xb@quant-x-sec.com

# Attacks on Regular SSH Port of a VM in the Internet

**2) Check Hacking Attempts**

You will see all hacking attempts on the VM. Therefore we need to configure the VM such that these attempts will be reduced and cannot be successful. Note the frequency of these attempts!!!

```
 sudo nano /var/log/auth.log

Example output:
Sep 10 02:05:00 h3004228 sshd[418705]: Failed password for invalid user contador from 49.113.85.117 port 58987 ssh2
Sep 10 02:05:02 h3004228 sshd[418705]: pam_unix(sshd:auth): check pass; user unknown
Sep 10 02:05:04 h3004228 sshd[418705]: Failed password for invalid user contador from 49.113.85.117 port 58987 ssh2
Sep 10 02:05:07 h3004228 sshd[418705]: Received disconnect from 49.113.85.117 port 58987:11: disconnected by user [preauth]
Sep 10 02:05:07 h3004228 sshd[418705]: Disconnected from invalid user contador 49.113.85.117 port 58987 [preauth]
Sep 10 02:05:07 h3004228 sshd[418705]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=49.113.85.117
Sep 10 02:05:11 h3004228 sshd[418715]: Invalid user ubuntu from 49.113.85.117 port 10311
Sep 10 02:05:11 h3004228 sshd[418715]: pam_unix(sshd:auth): check pass; user unknown
Sep 10 02:05:11 h3004228 sshd[418715]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=49.113.85.117
Sep 10 02:05:13 h3004228 sshd[418715]: Failed password for invalid user ubuntu from 49.113.85.117 port 10311 ssh2
Sep 10 02:05:13 h3004228 sshd[418715]: pam_unix(sshd:auth): check pass; user unknown
Sep 10 02:05:16 h3004228 sshd[418715]: Failed password for invalid user ubuntu from 49.113.85.117 port 10311 ssh2
Sep 10 02:05:17 h3004228 sshd[418719]: Invalid user admin from 141.98.11.11 port 22378
Sep 10 02:05:17 h3004228 sshd[418719]: pam_unix(sshd:auth): check pass; user unknown
...

More ways to check:
grep "Failed password for root" /var/log/auth.log

```

China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
Lithuania (LT)

# Information Security Management

ISMS (Information Security Management System)

*“A set of procedures and rules in an organization for the implementation and maintenance of information security.”*



xb@quant-x-sec.com

# Information Security Management

ISMS (Information Security Management System)

*"A set of procedures and rules in an organization for the implementation and maintenance of information security."*

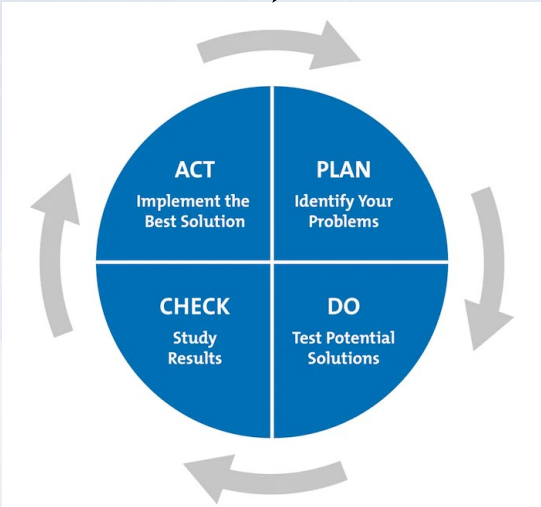



*image source: https://www.mindtools.com/*



xb@quant-x-sec.com

# Information Security Management Controls

ISMS (Information Security Management System)

*"A set of procedures and rules in an organization for the implementation and maintenance of information security."*

Control

*"Measure or procedure to reduce risk on information security"*

A control can be of organizational, operational, legal, physical, etc. nature.

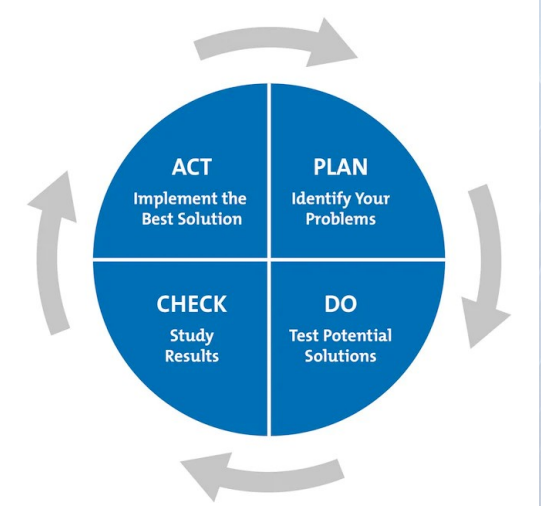



*image source: https://www.mindtools.com/*



xb@quant-x-sec.com

# Information Security Management – PDCA Cycle

**ISMS (Information Security Management System)**

*"A set of procedures and rules in an organization for the implementation and maintenance of information security."*

## Control

*"Measure or procedure to reduce risk on information security"*

A control can be of organizational, operational, legal, physical, etc. nature.

## Control Categories

- Configuration Management ...
- Information Risk Management ...
- Identity Access Management
  - Account Management (PAs and NPAs)
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management ...
- Operational Resilience ...
- 3rd Party Security ...

## Information Security Maintenance




xb@quant-x-sec.com

# Information Security Management Dimensions

## PDCA for a Control

- Configuration Management
- Information Risk Management …
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management …
- Operational Resilience …
- 3rd Party Security …

# Information Security Management Dimensions

## PDCA for a Control

- Configuration Management
- Information Risk Management …
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management …
- Operational Resilience …
- 3rd Party Security …

# Information Security Management Dimensions

## PDCA for a Control

- Configuration Management
- Information Risk Management …
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management …
- Operational Resilience …
- 3rd Party Security …

*image source: iStock*

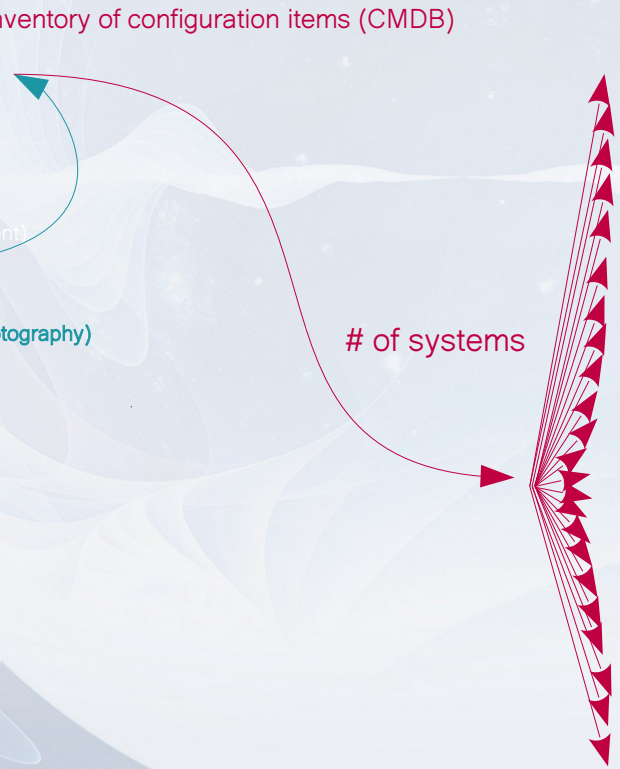


xb@quant-x-sec.com

# Information Security Management Dimensions

## PDCA on a Control

- Configuration Management
- Information Risk Management …
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management …
- Operational Resilience …
- 3rd Party Security …





xb@quant-x-sec.com

# Information Security Management Dimensions

## PDCA on a Control

- Configuration Management
- Information Risk Management …
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management …
- Operational Resilience …
- 3rd Party Security …

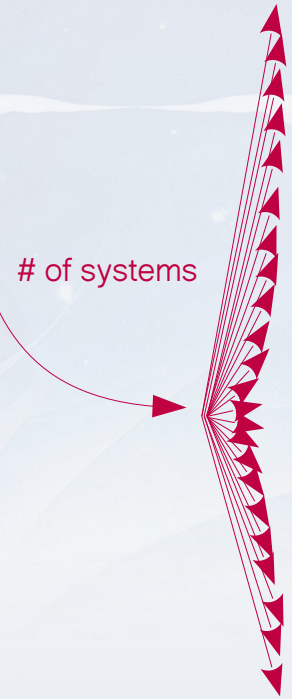



*image source: iStock*

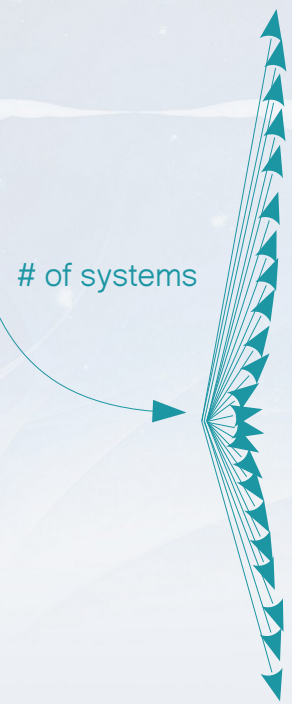


xb@quant-x-sec.com

# Information Security Management Dimensions

## PDCA on a Control

- Configuration Management
- Information Risk Management …
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management …
- Operational Resilience …
- 3rd Party Security …



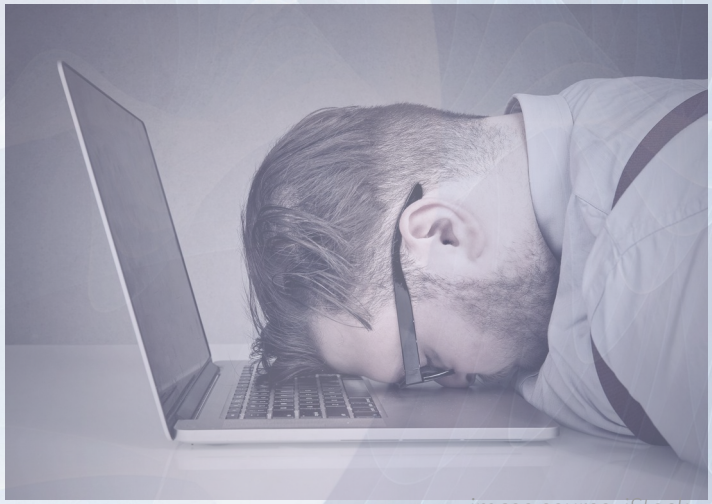



image source: iStock

*Reduce complexity by considering system and technology categories instead of each system and technology by itself*



xb@quant-x-sec.com

# Information Security Management Dimensions

## PDCA on a Control

- Configuration Management
- Information Risk Management ...
- Identity Access Management
  - Account Management
  - Authentication
  - Authorization (Permission Management)
- Platform Security
  - System Configuration
  - Connectivity and Networks (incl. Cryptography)
  - Patch Management
  - Lifecycle Management
  - Malware Resilience
- Security Monitoring
  - Vulnerability Scans
  - Penetration Tests
  - Red and Blue Teaming
  - Security Event Monitoring
  - Threat Intelligence
- Cybercrime Resilience
  - DDoS and APT Analyses and Testing
  - Emergency Response Processes
- Change Management ...
- Operational Resilience ...
- 3rd Party Security ...


1) Dependencies between controls
2) Multipliers
   a) # of systems
   b) # of system components per system
   c) # of involved experts
3) Complexity
   a) variety of used technologies
   b) variety of needed expertise

Quantum technologies will enhance the complexity of our digital infrastructures, their operations and the related ISMS. We should be aware of this fact while preparing integration and migration.

# Thank you!
# Questions?

https://quant-x-sec.com | xb@quant-x-sec.com