DIGITAL OPERATIONS RESILIANCE ACT (DORA)

Overview, Workshops and Services

Mai 2023

Blue River Experts

Member of the **Art of Innovation** Network

Table of Contents

1 Executive Summary 2
2 The Digital Operations Resilience Act (DORA) 3
2.1 Scope 3
2.2 ICT Governance and Risk Management 3
2.3 ICT Related Incident Classification and Reporting 4
2.4 Digital Operational Resilience Testing 4
2.5 ICT 3rd Party Risk Management 4
2.6 Critical ICT 3rd Party Service Providers and Oversight Framework 4
2.7 Information Sharing Arrangements 5
2.8 Supervision and Enforcement 5
2.9 Other Regulatory Requirements 5
3 Timeline, Next Steps 5
4 DORA Workshops & Webinars 6
4.1 Awareness Webinar 6
4.2 Executive Management Workshop 7
4.2.1 Common Knowledge 7
4.2.2 Executive Management 7
4.3 Process Management Workshop 9
4.3.1 Common Knowledge 9
4.3.2 Process Management 9
4.4 Technical Implementation Module 11
4.4.1 Technical Implementation 11
5 DORA Services 12
5.1 DORA Maturity Analysis 12
5.2 DORA Project Plan 12
5.3 DORA Implementation 12
6 Other Services for the Financial Sector 13
6.1 Financial Services Regulatory 13
6.2 Governance, Privacy and Cyber Security 13
6.3 Technology Consulting 13
6.4 Risk Advisory and Risk Consulting 13
6.5 Security Audits 13
6.6 Security Engineering 13
6.6.1 Application Security 13
6.6.2 Infrastructure Security 14
6.6.3 Cloud Security 14
6.6.4 Kubernetes Security 14
6.7 Cyber Response 14

1 Executive Summary

DORA aims to ensure that the European financial sector can maintain operational stability in the event of a major disruption - the core objective is to prevent and mitigate cyber threats.

The goal is to establish a unified framework for effective and comprehensive management of Cyber Security and ICT risks in financial markets

DORA applies to all financial entities and third-party IT providers and was approved on January 16, 2023. A mandatory compliance with DORA is expected at the beginning of 2025.

DORA will have a huge impact on the operational resilience of financial services companies. It will require them to adopt a more holistic approach to resilience and develop advanced capabilities in areas like impact assessment, reporting, and testing. DORA is expected to serve as a catalyst for companies to expedite strategic transformation in how they manage digital risks.

Senior management and boards will need to assess the business consequences of operational disruptions and effectively employ mitigating measures to address them. Everyone involved should be aware of the following areas that will be described in more detail on the next pages:

- Scope
- Governance and Risk Management
- Incident Classification and Reporting
- Digital Operational Resilience Testing
- 3rd Party Risk Management
- 3rd Party Service Providers and Oversight Framework
- Information Sharing Arrangements
- Supervision and Enforcement
- Other Regulatory Requirements

In order to prepare, implement all required modifications and become compliant by 2025 we offer a number of workshops:

- Awareness Webinar
- Executive Management Workshop
- Process Management Workshop
- Technical Implementation Module

and services:

- Maturity Analysis
- Project Plan
- Implementation Support

We also offer related services for all companies in the financial sector:

- Financial Services Regulatory Advice
- Governance, Privacy and Cyber Security Advice
- Technology Consulting
- Risk Advisory and Risk Consulting
- Security Audits
- Security Engineering
- Cyber Threat Detection and Response

2 The Digital Operations Resilience Act (DORA)

DORA aims to ensure that the European financial sector can maintain operational stability in the event of a major disruption - the core objective is to prevent and mitigate cyber threats.

The post-2008 regulatory reform of the financial sector mainly focused on strengthening the financial resilience of the sector and looked at ICT risks only as a side matter. The intention of DORA is to address the gaps in the financial services legislation, which to date has only provided a fragmented approach to operational resilience. Furthermore, one of the most significant implications of DORA is that it also addresses all third-party service providers that are deemed critical.

The goal is to establish a unified framework for effective and comprehensive management of Cyber Security and ICT risks in financial markets, by harmonizing security and resilience practices across the EU and introducing a unique, coherent supervisory approach across all relevant sectors.

DORA applies to all financial entities and third-party IT providers (e.g., cloud computing services, SaaS providers, data centers). The proposal was adopted by the EU Parliament and Council in November 2022 and was approved on January 16, 2023. A mandatory compliance with DORA is expected at the beginning of 2025.

DORA introduces significant change for entities supervised by ESMA or EIOPA, as well as for banks that already have to comply with the existing EBA guidelines on banking supervision - in addition, DORA introduces a Union-wide supervisory framework for critical ICT service providers appointed by the European Supervisory Authorities ESAs

With DORA being a new and complex legislation, you should be aware of the following:

2.1 Scope

DORA is applicable to more than 22,000 financial entities and ICT service providers. The regulation imposes new requirements on all financial market participants. Affected are 20 types of financial companies such as credit, payment and e-money institutions, investment firms, central securities depositories, crypto asset service providers, central counterparties, trading venues, trade repositories, alternative investment fund managers, management companies, data reporting service providers, insurance & reinsurance undertakings & intermediaries, institutions for occupational retirement provision, credit rating agencies, statutory audit and audit firms, administrators of critical benchmarks, crowdfunding service providers, securitization repositories, account information service providers. Consequently, DORA also applies to essential ICT third-party service providers.

2.2 ICT Governance and Risk Management

Under DORA, financial institutions are required to implement comprehensive internal **governance and control frameworks** to manage ICT risks. The responsibility for defining, approving, and overseeing the implementation of all arrangements related to the ICT risk management framework lies explicitly with the management body of the financial entity. The legislation outlines the relevant elements of the management body's responsibilities. Financial institutions, except for microenterprises, must also establish a monitoring role for arrangements made with ICT third-party service providers or assign a member of senior management to oversee related risk exposures and documentation.

DORA requires financial entities to establish and maintain a robust, well-documented ICT **risk management framework** that includes strategies, policies, procedures, ICT protocols, and tools, subject to regular audits. They must utilize and keep updated ICT systems, protocols, and tools and identify potential sources of ICT risk, particularly those that interconnect with internal and external ICT systems. DORA outlines specific measures that financial entities must comply with for protection and prevention, detection, response, and recovery from ICT risks. This includes implementing a comprehensive ICT business continuity policy and plan, particularly for critical or important functions outsourced or contracted through arrangements with third-party service providers. Financial entities must conduct a business impact analysis (BIA) of their exposure to severe business disruptions as part of their business continuity policy and establish a crisis management function to handle internal and external crisis communications when an ICT business continuity plan is activated.

DORA also specifies that financial entities must implement measures to establish **backup policies and recovery methods**, including an obligation for CSDs to maintain at least one secondary processing site. They must also create appropriate "learning and evolving" frameworks to gather information on vulnerabilities and cyber threats and analyze their potential impact on digital operational resilience. Mandatory digital operational resilience training must be provided to staff and senior management. Additionally, financial entities should have measures in place to monitor the effectiveness of their digital resilience strategy, as well as bespoke crisis communication plans, and internal and external communication policies.

2.3 ICT Related Incident Classification and Reporting

Under DORA, financial entities must establish and implement a specific **incident management process** to detect, manage, and report ICT-related incidents, along with significant cyber threats. They must classify these incidents and determine their impact based on a set of prescribed criteria, to be detailed in secondary legislation. Adding to the already complexity of regulatory reporting, significant ICT-related incidents have to be reported to competent authorities. Secondary legislation will establish reporting templates, their content, and time limits for submitting initial notifications and reports.

2.4 Digital Operational Resilience Testing

Financial entities must establish a comprehensive digital operational resilience testing program as part of their ICT risk management framework. The testing program should include various assessments, tests, methodologies, practices, and tools and be based on a risk-based approach, conducted by either internal or external independent parties. Additionally, significant financial entities must conduct advanced testing every three years using threat-led penetration testing.

This can and should be enhanced with ongoing resilience testing by implementing, for example, a **Bug Bounty Program.**

2.5 ICT 3rd Party Risk Management

DORA aims to establish a principle-based framework for the sound management of ICT third-party risks. The legislation outlines the relevant principles, including considerations for contractual arrangements, while maintaining the principle of proportionality. Financial entities must develop a strategy for managing ICT third-party risk and can only enter into contractual agreements with service providers that comply with appropriate information security standards. DORA also specifies circumstances that warrant termination of such arrangements and mandates that exit strategies must be in place for ICT services supporting critical or important functions. Additionally, financial entities must conduct a preliminary assessment of ICT concentration risk and weigh the benefits and costs of alternative solutions. Finally, DORA provides a list of elements that contractual arrangements between financial entities and ICT third-party service providers must include.

2.6 Critical ICT 3rd Party Service Providers and Oversight Framework

DORA provides a distinct set of provisions for critical ICT third-party service providers. These providers will be designated by the Joint Committee of the European Supervisory Authorities (ESAs), based on a list of criteria specified in DORA and secondary legislation. There are a few exemptions for the provision of ICT services within the same group. Alternatively, an ICT third-party service provider can choose to opt-in to the oversight regime instead of being designated from the top-down. With regard to cross-border arrangements, financial entities will not be permitted to use the services of a critical ICT third-party service provider established in a third country, unless such a service provider has set up a subsidiary in the EU within 12 months of being designated.

The Oversight Framework is a key component of DORA, which comprises the Oversight Forum and the Lead Overseer, one of the ESAs. The Lead Overseer will be granted significant powers, such as the ability to request access to pertinent information, conduct comprehensive investigations and inspections, and impose periodic penalty payments in cases where a critical ICT third-party service provider fails to comply with the measures that the Lead Overseer has mandated. DORA also outlines the procedures for the Lead Overseer to exercise its powers outside the EU.

2.7 Information Sharing Arrangements

DORA permits but does not mandate the exchange of information between financial entities regarding cyber threats. This information may include indicators of compromise, techniques, cyber security alerts, procedures, and configuration tools.

2.8 Supervision and Enforcement

DORA assigns the supervision of compliance with its requirements to the competent authorities responsible for overseeing the financial entities covered by the regulation. Such competent authorities will be equipped with all necessary supervisory, investigatory, and sanctioning powers to carry out their supervisory obligations. These powers will include access to all documents and data, on-site inspections, and investigations, as well as the ability to impose administrative penalties and remedial measures.

2.9 Other Regulatory Requirements

DORA cannot be viewed in isolation. During its legislative review, significant attention has been devoted to the interplay between DORA and other initiatives, particularly the revised Directive on Security of Network and Information Systems (the NIS 2 Directive), as well as existing initiatives such as the European Banking Authority's (EBA) guidelines on outsourcing arrangements and the EBA guidelines on ICT and security risk management. It also should be noted that a new regime for critical third-party providers is currently under development in the UK.

3 Timeline, Next Steps

DORA came into force at the beginning of 2023, and it is expected that financial entities must comply with the regulation from the beginning of 2025.

2020	Draft	In September 2020, the European Commission published the draft Digital Operational Resilience Act (DORA) as part of the Digital Finance Package (DFP).
2021/22	Consensus	After the European Parliament voted in favor of DORA on November 10, the European Council adopted the legislation on November 28, 2022.
2023	Enactment	DORA came into force in the first quarter of 2023.
2024	RTS & ITS	Technical regulatory and implementation standards will be determined by the European Supervisory Authorities
2025	Mandatory	DORA requirements are enforceable 24 months after becoming effective.

There is not much time for all affected organizations to become compliant with DORA, so we suggest getting started immediately.

Understanding DORA	DORA is a complex regulation and may overlap with other regulations already in place. A clear understanding of the requirements is an important first step.
DORA Maturity Analysis	To ensure effective and strategic resilience planning, it is important to identify key gaps in your maturity.
DORA Project Plan	Derive a roadmap with the goal of achieving desired levels of resilience while meeting DORA requirements..
DORA Implementation	With a preparation time of 2 years, there is a lot to consider, implement and document.

4 DORA Workshops & Webinars

We are offering one awareness webinar and three DORA related workshops focusing on different target audiences and / or job functions:

4.1 Awareness Webinar

During our awareness webinar we are introducing DORA and are covering roadmap, scope, and consequences of DORA. It is delivered by top level consultants with many years of experience in the financial sector, IT management and operations, and cyber security. The webinar can be delivered in one 60-minute junk or in two parts of approximately 30 minutes each. We are delivering this webinar free of charge to raise awareness and the consequences of DORA.

DORA Background

- Systemic Cyber Risk
- Attacks on Corporations
- Leverage of External Knowledge

Roadmap

Context to other Frameworks

Structural Overview

- Subject, Area of Application, Definitions, Proportionality
- Risk Management (Information Security Management System & more)
- Incident Management & Reporting
- Digital Operational Resilience Testing
- ICT-Third Party Management
- Authorities, Legal Rights of Agencies, Agency Inspections

Consequences of DORA

4.2 Executive Management Workshop

In this workshop we are covering common DORA knowledge and very specific topics for the executive management of financial entities. The overall time investment is one day; however, we are only using 90 minutes in the morning and 90 minutes in the afternoon. This is a workshop for executives delivered by executive level consultants with many years of experience in the financial sector, IT management and operations, and cyber security.

4.2.1 Common Knowledge

DORA Background

- Systemic Cyber Risk
- Attacks on Corporations
- Leverage of External Knowledge

Roadmap

Context to other Frameworks

- EBA Guidelines, ISO 27001, BSI Guidelines, ITIL4 NISG

Structural Overview

- Subject, Area of Application, Definitions, Proportionality
- Risk Management (Information Security Management System & more)
- Incident Management & Reporting
- Digital Operational Resilience Testing
- ICT-Third Party Management
- Authorities, Legal Rights of Agencies, Agency Inspections

Consequences of DORA

- Full Compliance required in 2 years
- Civil, Revenue-Dependent Non-Compliance Fines
- Possibility of additional Criminal Offence Prosecution

4.2.2 Executive Management

Leadership Responsibilities

- Cannot be contractually outsourced, they stay with management body
- Extensive Responsibilities for ICT Risk
- Data Confidentiality, Integrity, and Availability
- Roles & Responsibilities Assignment
- Strategy for Digital Operational Resilience and Risk Acceptance Level
- Business Continuity Guideline
- Response & Recovery Plans
- Auditing Plans
- Budget for Security Awareness
- 3rd Party Risk Guidelines
- Monitoring of 3rd Party Contracts
- Regular Information Security Management Training

ICT Security Strategy

- Digital Operational Resilience Strategy
- Monitoring ICT Risks &Incidents internally and globally

Explicit Management Roles

- 3rd Party Risk Manager
- ICT Risk Manager
- ICT Emergency Manager
- ICT Incident Communication Manager

Budget Allocation

- User Activities, ICT Anomalies & ICT Incident Monitoring
- Vulnerabilities & Threat Monitoring
- Impact Analysis

Information Security Management System (ISMS)

- Internal Governance Framework for ICT Risks
- Supervision by the Board of Directors
- Communication Channels
- Business Continuity Management
- Backups, Incidents

ICT 3rd Party Risk Management

- Contractual
  - Special Termination, Inspections
  - ISMS Requirements
  - Documentation
  - Exit Strategy
  - Subcontracting
  - Service Level Agreements
  - Insolvency Consequences
  - Incidents
- Operational
  - Exit Strategy Test (BCM)
  - Audits
  - Central 3rd Party Register
  - 3rd Party Risk Strategy & Guidelines
  - Trainings

Digital Operational Resilience

- Ongoing process to test and ensure Information Security Measures
  - Management Systems
  - Process Plans
  - Operational Measures

Internal Audit

- Annual review of
  - Information Security Management System
  - Classification of Roles
  - Responsibilities & Dependencies regarding ICT Risks
  - Cyber Threat Modelling
  - Legacy Systems
- ISMS Review (after incidents)
  - Follow-Up Process
- Response & Recovery Plans (upon implementation & major changes)
- ICT 3rd Party Strategy (regular intervals)

4.3 Process Management Workshop

In this workshop we are covering common DORA knowledge and topics specific to IT process management. The overall time investment is one day; however, we are only using 90 minutes in the morning and 90 minutes in the afternoon. The workshop is intended to be a preparation for the DORA maturity analysis and the DORA project plan. It will be delivered by top level consultants with many years of experience in the financial sector, IT management and operations, and cyber security.

4.3.1 Common Knowledge

DORA Background

- Systemic Cyber Risk
- Attacks on Corporations
- Leverage of External Knowledge

Roadmap

Context to other Frameworks

- EBA Guidelines, ISO 27001, BSI Guidelines, ITIL4 NISG

Structural Overview

- Subject, Area of Application, Definitions, Proportionality
- Risk Management (Information Security Management System & more)
- Incident Management & Reporting
- Digital Operational Resilience Testing
- ICT-Third Party Management
- Authorities, Legal Rights of Agencies, Agency Inspections

Consequences of DORA

- Full Compliance required in 2 years
- Civil, Revenue-Dependent Non-Compliance Fines
- Possibility of additional Criminal Offence Prosecution

4.3.2 Process Management

IT Security Concepts

- Data Security in Transit
- Corruption, Access, Availability
- Data-Management Risks
- Least Privilege Principal
- Authentication

Asset Management

- Registration, Classification, Connections
- Interdependencies
- 3rd Party Process Documentation
- Internal Dependencies on 3rd Parties

Capacity Management

- Sufficient for Peak Loads
- Resilient to Stress and Adversities

Change Management

- Risk Analysis on Major Changes
- Patch/Update Guidelines

Incident Management

- Alarm Thresholds/Criteria Definition
- Detection & Treatment Process
- Communication Plans
- Incident Classification
- Post-Incident Reappraisal

Business Continuity & Recovery

- Business Impact Analysis
  - Criticality Classification
  - Interdependencies
  - Redundancy Concepts
- Continuity/Recovery
  - Continuity & Recovery Plans
  - 3rd Party Recovery Plans
  - Backup Planning
- Test Management
  - Continuity, Response, Recovery
  - 3rd Party Disruption/Recovery
  - Redundancy
  - Communication Plans

Digital Operations Resilience

- Continuous Planning & Execution of Tests
- Multiple Levels
  - Management Systems
  - Processes
  - Operations
- Vulnerability Management Process

4.4 Technical Implementation Module

The technical implementation is not a stand-alone workshop but an add-on module to the process management workshop as all attendees of this module should also have consumed the common knowledge and process management module. If there is interest in this module we are delivering it as another 90-minute module in the afternoon after the process management module.

4.4.1 Technical Implementation

Technical Redundancy

- Data Bases
- Server/Data Processors
- Network Connections

Network Requirements

- Network Segmentation/Isolation
- Network-Quarantine

Data Security

- Backups, Recovery Mechanisms
- Physical Separations of Backups
- Active Transaction Security

Security & Availability Monitoring

- Incident Monitoring & Logging
- Early Warning Indicators
- Notification Mechanisms

Test Modelling

- Backups, Restoration
- Network Segmentation
- 3rd Party Disruptions

Digital Operations Resilience

- Vulnerability Assessment- & Scans
- Open-Source Analysis
- Network Security Assessment
- Physical Security Checks
- Static Code Analysis, Code Reviews
- Scenario Testing
- Compatibility Testing
- Performance Testing
- End-To-End Testing
- Penetration Testing

Threat Led Penetration Testing

- Required for significant Financial Institutions & ICT Providers
- In close cooperation with Public Institutions
- Every 3 years

5 DORA Services

The impact of DORA on the operational resilience of financial services companies cannot be overstated. It will require them to adopt a more holistic approach to resilience and develop advanced capabilities in areas like impact assessment, reporting, and testing. DORA is expected to serve as a catalyst for companies to expedite strategic transformation in how they manage digital risks. Senior management and boards will need to assess the business consequences of operational disruptions and effectively employ mitigating measures to address them.

Companies should not wait until the end of the 24-month period since preparing for DORA compliance will be a substantial task. They also will have to consider Level 2 technical standards as they become available and are finalized. Starting early before the implementation period begins later this year will provide companies with valuable time to prepare. Specifically, they should anticipate increased supervisory engagement. DORA will grant national and EU-level supervisors extensive new mandates and powers in digital operational resilience. Companies should not see DORA as a mere compliance exercise, but rather, expect their relevant authorities to develop supervisory frameworks that use their new powers to encourage companies to improve their ability to assess and enhance their operational resilience capabilities. As supervisors' understanding of operational resilience increases, they will likely demand more from companies.

To satisfy supervisors, companies need to concentrate on aspects of DORA that require routine evaluations. A major area of scrutiny will be the new business impact analysis requirements in the ICT Risk Management section. Supervisors will likely question the severity of the scenarios utilized, the complexity of the testing methods, the level of detail in the underlying system mapping, and the adequacy of the remediation work done to address vulnerabilities.

In addition, it is important for companies to pinpoint capabilities that will necessitate investment or development. A considerable amount of investment in the governance, risk, and compliance framework for ICT, Cyber, and Third-Party Risk Management functions will be required due to DORA's new requirements, as well as subsequent work to address any operational vulnerabilities that are discovered. Companies should conduct a gap analysis to determine where there are deficits in capability, resources, and expertise, which will need to be addressed during the 24-month implementation period.

We can help to get ready for DORA by providing several services as outlined below.

5.1 DORA Maturity Analysis

To achieve successful and strategic resilience planning, it is crucial to pinpoint significant gaps in your maturity. A valuable exercise would be to conduct a gap analysis of current ICT risk management and governance practices, specifically from a critical function perspective. Additionally, it would be advantageous to allocate more resources towards threat and incident detection and enhance company-wide ICT security awareness training programs, with a specific emphasis on increasing awareness among management bodies.

Assessing the company's incident management and reporting maturity level would be a prudent step to evaluate its current capabilities and level of awareness regarding the various ICT incident reporting requirements that apply to the financial services sector.

We offer the determination of the project scope, considering compliance with existing regulations, a bottom-up assessment of the maturity level based on interviews, documentation, and some of the exercises described above and strategic top-down resilience planning to determine further action.

5.2 DORA Project Plan

We offer to derive a roadmap with the goal of achieving desired levels of resilience while meeting DORA requirements. This includes prioritization of gaps / measures based on comprehensive best practice and regulatory know-how and the development of a pragmatic DORA framework meeting all requirements.

5.3 DORA Implementation

With a preparation time of 2 years, there is a lot to consider, implement and document. We can help with DORA compliance by offering hands-on support ranging from strategic and operational design to technical implementation. As it is unlikely that most in-scope companies have all the required resources, our support will considerably reduce the burden on internal resources and expand our customer’s know-how pool.

We can also assist with cyber implementation and assurance services to ensure that the infrastructure is secure and resilient against potential threats. This includes penetration testing, vulnerability assessments, and incident response planning. Additionally, we can provide training to employees to help them understand and comply with DORA requirements.

6 Other Services for the Financial Sector

6.1 Financial Services Regulatory

All of our consultants have many years of experience in the financial sector and can help you navigate the evolving and increasingly complex regulatory environment. This includes advising you on all aspects of governance arrangements, outsourcing and third-party risk management.

6.2 Governance, Privacy and Cyber Security

Information Security Management Systems (ISMS) preserve the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. Our experts can help you manage the process of establishing, implementing, maintaining, and continually improving an ISMS.

6.3 Technology Consulting

To successfully implement and adopt new technologies, a comprehensive understanding of technical capabilities and operational feasibility is crucial. Our team of experts can assist in maximizing the benefits of emerging technologies. Additionally, our collaboration with legal and compliance experts enables us to develop and execute technologically advanced compliance strategies.

6.4 Risk Advisory and Risk Consulting

Our team of industry specialists, risk and compliance professionals collaborate closely with legal experts to provide a comprehensive set of skills and expertise that can effectively address the intricate risk challenges your business might face. We provide expert guidance on various operational resilience issues, ranging from designing and implementing operational resilience frameworks, to developing crisis response and scenario planning, as well as improving operational resilience capabilities and promoting best practices.

6.5 Security Audits

Such audits should be done once or twice a year. They are a systematic evaluation of your information systems by measuring how well they conform to an established set of criteria. Our audits usually assess the security of the system's physical configuration and environment, software, information handling processes and user practices. Main goals are:

- Identify security problems and gaps, as well as system weaknesses
- Establish a security baseline that future audits can be compared with
- Comply with internal organization security policies
- Comply with external regulatory requirements
- Determine if security training is adequate
- Identify unnecessary resources

6.6 Security Engineering

6.6.1 Application Security

We are pleased to offer our extensive knowledge and experience in the area of application security to collaborate with you in formulating security strategies, devising countermeasures, and executing necessary adjustments. In addition to technical aspects, we can also support you in improving your Secure Software Development Lifecycle (SSDLC) or DevSecOps process.

With tried and tested concepts, a high level of automation through security tools and our experience with small and large software development teams, we can ensure an appropriate level of security even with agile software development and short deployment cycles.

6.6.2 Infrastructure Security

Companies often have a diverse IT infrastructure consisting of various components and technologies. To prevent exploitable vulnerabilities, IT security must be considered across all areas of the infrastructure.

Infrastructure security involves more than just Microsoft Active Directory and Network Security. While these are important components, there are other building blocks that need to be considered as well. To maintain the security of infrastructure in the long run, suitable operational and security processes are required. Our consultants not only possess expertise in this area but also have experience in operations. This allows them to provide practical suggestions and concepts to support you.

6.6.3 Cloud Security

When talking about security in the context of Cloud we need to consider many areas. Therefore, people are also sometimes talking about End-to-End Security. We need to look at Endpoint Security, User Identity & Access, Network & Infrastructure Security, Application Security, Data in Transit, as well as the Safety of Data stored somewhere in the Cloud. In this context we also need to look at various compliance concepts like Data Residency, Data Sovereignty, and Data Privacy. And, to make it even more complex we need to look into multi-cloud and hybrid protection.

It's also very important to understand that Cloud Security is a shared responsibility between the provider and the customer. The provider is always responsible for the infrastructure itself including networking, compute, and storage resources. The customer is always responsible for managing users and their access privileges, the safeguarding of data assets and managing its compliance. The third category is obviously shared responsibility which depends on the service model like IaaS (infrastructure as a service), PaaS (platform as a service) or SaaS (software as a service).

Doing the right things and avoiding mistakes requires a high level of expertise and experience. We are happy to support you in all matters related to Cloud to ensure that security requirements are adequately taken into account.

6.6.4 Kubernetes Security

Hardly any developer, architect or IT manager gets past Docker and containers. Containerization has changed the way software is developed, deployed, and operated. Microservices is the new paradigm. Many information security teams around the world are wondering what this means for corporate security. Our experts are happy to support you in using these technologies safely and correctly integrating them into existing business processes.

6.7 Cyber Response

Cyber-attacks on companies and related damages are steadily increasing. Ransomware trojans have established themselves as a lucrative business area – but industrial espionage or hacktivism are also motives for criminals. Have you become victim of such an attack? Do not hesitate to contact us immediately. Our approach is not only to support you in individual areas of cyber response, but also to take over the comprehensive coordination of the incident for you as a well-rehearsed team. A team made up of the various skills required for such an assignment will support you in the technical analysis on the attack, securing your systems to prevent further damage, the reconstruction of your infrastructure and information, the clarification of legal questions and the fulfillment of legal reporting obligations, communication with employees, customers, partners, suppliers, (regulatory) authorities, insurances and media and the negotiations with the attackers.