Duck Creek
Technologies

WHITEPAPER

The Digital Operational Resilience Act

duckcreek.com

Contents

Introduction	3
Duck Creek Enterprise Risk Management Framework	3
Duck Creek Digital Operational Resilience	4
Duck Creek Infrastructure Design	4
Function and Health of Application Infrastructure	6
Security Incident Response	7
Business Continuity Management	8
Security	9
Duck Creek Penetration Testing Program	11
Third Party Management	12
Conclusion	14

Introduction

In today's rapidly evolving digital landscape, ensuring operational resilience has become a critical priority for insurance carriers. The Digital Operational Resilience Act (DORA) mandates stringent requirements for managing ICT risks, aiming to enhance the stability and security of ICT systems. This white paper delves into how Duck Creek's comprehensive approach to DORA compliance not only meets these regulatory standards but also strengthens the company's overall digital resilience.

Duck Creek Enterprise Risk Management Framework

Duck Creek has established an Enterprise Risk Management (ERM) Framework that addresses ICT risks quickly, efficiently, and comprehensively, in alignment with DORA. This framework includes strategies, policies, procedures, ICT protocols, and tools necessary to protect information and ICT assets from risks, including damage and unauthorized access. The framework is implemented and approved by Executive Leadership and is subject to periodic review to ensure ongoing compliance and effectiveness.

Duck Creek's ERM framework supports the company in achieving its strategic and operational objectives while ensuring compliance with DORA. It is an essential part of governance and aims to drive a culture where everyone takes responsibility for risk, empowers employees to make informed decisions, enhances performance, and improves organizational resilience. The ERM framework includes procedures and guidelines for implementing the principles outlined in the policy, ensuring that risk management is an integral part of the company's operations and aligns with DORA's requirements for robust risk management and operational resilience.

Duck Creek Digital Operational Resilience

Duck Creek environments are meticulously designed and continuously monitored to ensure robust digital operational resilience, in alignment with DORA. This proactive approach encompasses advanced monitoring systems, redundancy measures, and stringent security protocols, all aimed at maintaining the highest standards of operational stability and security. By adhering to DORA's requirements, Duck Creek ensures that its infrastructure is resilient against disruptions, capable of swift recovery, and consistently secure, providing customers with reliable and compliant services.

Duck Creek Infrastructure Design

Duck Creek customer environments are thoroughly configured for high availability and include physically and logically dispersed regions. These environments are designed with redundancy to ensure there is no single point of failure, aligning with the requirements of DORA.

High Availability

Duck Creek employs a robust infrastructure that includes multiple layers of redundancy to ensure that services remain available even in the event of hardware or software failures. This includes the use of load balancers to distribute traffic across multiple servers, ensuring that no single point of failure. The environments are designed with failover mechanisms that switch to backup systems in case of a primary system failure, ensuring minimal disruption to services and continuous operations without significant downtime. These measures support DORA's emphasis on operational resilience and service continuity.

Redundancy

Duck Creek's environments are built with redundancy at every level, including network, storage, and compute resources. This means that there are multiple instances of critical components, so if one component fails, another can take over without impacting the overall system. The use of geographically distributed data centers further enhances redundancy. By having data centers in different locations, Duck Creek ensures that even if one data center experiences an outage, the others can continue to provide services. This geographical dispersion aligns with DORA's requirements for robust and resilient infrastructure.

Capacity Planning

Duck Creek ensures it has the necessary capacity to meet customers' requirements by understanding those requirements during contracting and onboarding. If capacity needs expand, customers can work with Duck Creek to increase their contracted services, and Duck Creek will allocate the appropriate amount of resources to meet the customers' requirements. Customers are also able to purchase performance environments where they can test performance and identify whether they have enough capacity to meet their business needs. This proactive capacity planning supports DORA's focus on maintaining adequate resources to ensure operational resilience.

Disaster Recovery

Duck Creek has a comprehensive disaster recovery plan in place that includes regular backups of critical data and systems. These backups are stored in multiple locations to ensure they are available even in the event of a major disaster. The disaster recovery plan also includes regular testing to ensure that all systems and processes are functioning as expected and that the team is prepared to respond quickly and effectively in the event of an emergency. These disaster recovery measures align with DORA's requirements for effective incident response and recovery.

Security and Compliance

Duck Creek's environments are designed with security in mind, incorporating multiple layers of security controls to protect against unauthorized access and data breaches. This includes the use of encryption, firewalls, and intrusion detection systems. Compliance with industry standards and regulations is a key priority for Duck Creek. The company regularly undergoes audits and assessments to ensure that its environments meet the highest standards of security and reliability. These security and compliance measures support DORA's emphasis on maintaining a secure and resilient operational environment.

Function and Health of Application Infrastructure

Duck Creek's comprehensive application and infrastructure monitoring plays a crucial role in meeting its digital operational resilience strategy by ensuring continuous service delivery, minimizing downtime, and swiftly addressing potential issues to maintain operational stability and security. These measures are designed to comply with DORA ensuring that our operations remain robust and compliant.

1. ICT Production Incident Detection and Reporting

Duck Creek has established processes for the timely detection and reporting of production ICT-related incidents. This ensures that incidents are identified quickly and reported to the relevant stakeholders. With predefined alerting thresholds, Duck Creek can proactively address and remediate issues within customer environments and the Duck Creek back-end infrastructure. This proactive approach aligns with DORA's requirements for timely incident detection and reporting.

2. Incident Response and Recovery

Robust incident response and recovery procedures are in place to address ICT-related incidents. These procedures are designed to minimize the impact of incidents on operations and ensure a swift recovery. Specific communication timeframes based on the severity and classification of incidents are established, with templates used to ensure the proper information is communicated. This structured response framework supports DORA's emphasis on effective incident management and recovery.

3. Continuous Improvement

Duck Creek continuously reviews and updates its incident management policies and procedures to reflect changes in the regulatory environment, emerging threats, and advancements in technology. This commitment to continuous improvement ensures that our incident management practices remain current and effective, in line with DORA's focus on adaptive and evolving security measures.

Duck Creek will notify customers of production incidents, including availability and security, in accordance with contractual commitments. This ensures that customers are informed and can meet their obligations under DORA. By providing timely and accurate incident reports, Duck Creek supports customers in maintaining their regulatory compliance.

Security Incident Response

Duck Creek network and infrastructure are systematically designed and monitored for security. Comprehensive security alerting and monitoring systems are implemented to proactively identify and mitigate potential anomalous activities. These measures are designed to comply with DORA ensuring that our operations remain secure and resilient.

Security is monitored 24/7, aligning with DORA's requirements for continuous monitoring and rapid response. In the event of a security incident, Duck Creek has the capability to isolate specific network segments to prevent the spread of malicious activity. Internal procedures and processes are in place to document paths and triggers for escalation, as well as the activation of the Duck Creek Security Incident Response plan and team.

The Duck Creek Security Incident Response Plan details the identification, mitigation, containment, and resolution of security incidents, as well as tracking and notification. Incidents are classified based on severity and impact, ensuring that responses are proportionate and effective. Security incidents are tracked by the Duck Creek Security Team. Duck Creek values continual learning and improvement from incidents and conducts retrospectives after major production or security incidents, in line with DORA's emphasis on continuous improvement.

Security incidents are communicated to customers in accordance with contractual commitments. Information is provided as it becomes available, ensuring that customers have all necessary information to meet their regulatory obligations pertaining to the incident. This transparency is a key component of DORA compliance.

Duck Creek security personnel stay up to date on the latest trends and issues in cybersecurity through various newsletters and applications. Security tools used to monitor production environments are continually learning and improving based on industry trends. These continuous improvements help identify and respond to potential malicious behavior and activity, supporting DORA's focus on adaptive security measures. Regular security incident response tests involving the Executive Leadership Team ensure that our response capabilities remain robust and effective.

Duck Creek has processes in place to ensure proper reporting to customers and the media. Customers are alerted based on contractual commitments, including notifications for production and security incidents. Notifications to government entities and the media occur in accordance with applicable regulations and are communicated to customers in advance to the extent possible and permitted, ensuring compliance with DORA's reporting requirements.

Business Continuity Management

Duck Creek's business continuity program is meticulously designed to ensure the resilience and reliability of its operations, even in the face of disruptions. These measures are aligned with the requirements of DORA ensuring that our operations remain robust and compliant. Here are the key components of the program:

1. Annual Disaster Recovery (DR) Tests

Duck Creek conducts annual DR tests for each customer to validate the effectiveness of their Business Continuity and Disaster Recovery (BC/DR) processes. This allows customers to confirm that their plans are suitable for meeting their business needs and obligations, in line with DORA's emphasis on operational resilience.

2. Activity Tracking and Logging

During any failover or DR event, all activities are tracked and logged in Duck Creek's ticketing system. This provides a clear audit trail and facilitates swift resolution of any issues, ensuring compliance with DORA's requirements for comprehensive documentation and accountability.

3. Backup Strategy

Duck Creek's backup strategy is tailored to align with the business needs of its customers. This strategy ensures that data is consistently protected and recoverable, meeting DORA's standards for data integrity and availability. The backup schedule includes:

1. Full Backup: Weekly
2. Differential Backup: Daily
3. Transaction Log Backup: Daily, every 15 minutes
4. System Databases: Daily

4. Restore Procedures

Duck Creek maintains detailed restore procedures to facilitate the restoration of databases. In the event of a customer failover or recovery procedure, Duck Creek engages with the customer before initiating the backup restoration or failover. This collaborative approach ensures that recovery processes are transparent and effective, in accordance with DORA's guidelines.

5. High Availability Regions

Duck Creek's high availability regions are physically and logically separated from the source production environments. This ensures that services remain available even if some components fail, supporting DORA's requirement for operational continuity.

6. High Availability and Redundancy

The Duck Creek Product Suite leverages high availability and redundancy mechanisms to ensure continuous operation. This minimizes downtime and maintains service continuity, aligning with DORA's focus on minimizing operational disruptions.

7. RPO/RTO Commitments

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) commitments are agreed upon in the contract. Duck Creek designs its products and their availability to meet industry-standard RPO/RTO, ensuring customers can trust Duck Creek's ability to maintain their core operations, as required by DORA.

8. Collaboration with Customers

In the event of a failover, Duck Creek collaborates with the customer to conduct any necessary testing to validate the success of the failover. This ensures that systems are fully operational and that any issues are promptly addressed, in line with DORA's emphasis on effective incident response and recovery.

Security

Duck Creek is dedicated to implementing state-of-the-art security measures that not only protect its platform and customer data but also enable compliance with DORA. Our comprehensive security framework, validated through SOC 2 and ISO 27001 certifications, aligns with DORA's stringent requirements for operational resilience, cybersecurity, and risk management. By integrating robust identity and access management, secure connectivity, continuous monitoring, and employee training, Duck Creek ensures that all aspects of our operations are resilient against cyber threats and disruptions.

Our commitment to security and compliance ensures our customers can trust Duck Creek to safeguard their data and maintain uninterrupted service.

Secure Connectivity

Duck Creek offers multiple methods for customers to connect to the Duck Creek platform, all of which utilize end-to-end encryption, including SSL/TLS/HTTPS. Customers can choose the most appropriate approach based on their specific requirements.

Identity and Access Management

Duck Creek integrates with customers' identity management systems to enable Single Sign-On (SSO) from the customer's authentication service. This integration allows customers to maintain control over how access is provisioned for their end users. Our Identity and Access Management policies and technical controls are designed to uniquely identify, provision, and manage operational administrators, ensuring that all access, authentication, and authorization are appropriately controlled and managed. Access is granted based on the principle of 'least privilege,' where each user is given the minimal level of access needed to perform their job. Secure access credentials are required for all OnDemand environments and system components. Two-factor authentication is used, and user access is logged, including administrative access. Privileged access is additionally controlled using a privileged access management solution, where credentials are checked out for a defined period.

Employee Training

Duck Creek employees are required to undergo annual security awareness training. New employees receive role-specific knowledge transfer and training to ensure they are well-equipped to handle security responsibilities.

Network Design and Management

Duck Creek adheres to comprehensive and industry-leading standards for network design and management of its corporate and customer environments. These standards include network segmentation, network layer access control, protection of data in transit, access control, inbound and outbound connectivity, DDoS protection, patching and vulnerability management, and secure development policies.

Endpoint Detection and Response

Duck Creek utilizes industry-leading endpoint detection software to monitor and analyze activities on machines. This software identifies the presence of malware and any malicious activities, alerting on-call personnel who follow established standards and procedures for responding to such alerts, including escalation and isolation of a network segment if necessary.

Business Continuity and Disaster Recovery

Duck Creek assists customers with their Business Continuity and Disaster Recovery (BC/DR) strategy by configuring its environments for high availability and disaster recovery. All system components have built-in redundancy to prevent system downtime.

System Monitoring and Alerting

Duck Creek has comprehensive system monitoring and alerting mechanisms in place to proactively identify any issues with capacity, availability, or system uptime.

Vulnerability Management

Duck Creek employs vulnerability scanning tools to identify vulnerabilities in our environment. Patches are applied in accordance with their criticality to ensure the highest level of security.

Continuous Improvement

Security tools used by Duck Creek to monitor production environments are continually learning and improving based on industry trends. These continuous improvements help identify and respond to potential malicious behavior and activity.

Duck Creek Penetration Testing Program

The Duck Creek Penetration Test Program is a comprehensive initiative designed to assess and enhance the security of Duck Creek's web applications and internal networks. The program involves several key components:

1. Web Application Penetration Tests

These tests are conducted on sensitive or high-value Duck Creek SaaS web applications to identify and evaluate vulnerabilities. The approach includes a detailed review of the application's functionality and assessment based on the OWASP and NIST testing frameworks.

2. Internal Network Penetration Tests

These tests focus on identifying vulnerabilities within Duck Creek's internal network infrastructure.

3. Testing Methodology

The program follows a structured methodology to ensure a thorough assessment of security vulnerabilities. This includes knowledge of the functionality available to users and their access levels.

4. Remediation of Issues

The program categorizes findings based on severity and prioritizes remediation efforts accordingly.

5. Documentation and Standards

The program is documented in detail, including processes, standards, and roles involved in the penetration testing process.

Third Party Management

Duck Creek is committed to achieving compliance with DORA through documented processes and comprehensive vendor management. Our Record of Processing Activities (ROPA) ensures that all subprocessors are systematically tracked, reviewed, and disclosed to customers, providing full transparency and accountability.

Risk Assessments and Third-Party Reviews

We conduct comprehensive annual risk assessments and reviews of critical third parties, including subprocessors, to ensure ongoing compliance and operational resilience. These assessments help us identify and mitigate potential risks, aligning with DORA's requirements for robust risk management.

Seamless Integrations and Transparency

Duck Creek Products support a wide range of integrations with customers' internal systems and selected third-party vendors. Specific requirements are provided during implementation to ensure seamless connectivity and interaction with customers' external systems.
This approach guarantees full transparency during onboarding, with allow listing based on customer requirements to ensure only approved connections are established. Environment diagrams are shared as needed to provide a clear understanding of the integration landscape.

Subprocessor Disclosure and Inventory Support

We provide a comprehensive list of all subprocessors utilized to deliver services, supporting customers' inventory requirements by disclosing any requested information related to their environments, third-party connections, and subprocessors. This transparency aligns with DORA's emphasis on clear and accurate reporting.

Contractual Compliance and Operational Resiliency

Duck Creek's contracts address business requirements based on customer needs, identified as part of the negotiation process. These contracts include compliance with laws and operational resiliency based on committed Service Level Agreements (SLAs), backup processes, Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and security measures. Our agreements with vendors, including those providing critical functions related to the Duck Creek OnDemand (DCOD) environment, ensure that we can continue to meet our contractual obligations to customers.

Audit Rights and Termination Clauses

We ensure appropriate audit rights exist in our contracts with critical third parties, allowing us to verify compliance and operational standards. Additionally, we have appropriate termination clauses in place with our critical third parties to safeguard our operations and maintain resilience.

Conclusion

Duck Creek's commitment to DORA compliance underscores its dedication to maintaining the highest standards of digital operational resilience. By implementing a comprehensive ICT risk management framework, Duck Creek not only meets regulatory requirements but also enhances its ability to manage and mitigate ICT-related risks effectively. This proactive approach ensures that Duck Creek's systems remain secure, resilient, and capable of withstanding adverse conditions, thereby safeguarding the company's operations and customer data.

As the digital landscape continues to evolve, Duck Creek remains steadfast in its pursuit of continuous improvement and innovation. By staying ahead of emerging threats and regulatory changes, Duck Creek is well-positioned to navigate the complexities of the modern financial environment. This white paper has outlined the key strategies, policies, and procedures that Duck Creek has adopted to achieve DORA compliance, demonstrating the company's unwavering commitment to operational excellence and customer trust.

About Duck Creek Technologies

Duck Creek Technologies is the intelligent solutions provider defining the future of the property and casualty (P&C) and general insurance industry. We are the platform upon which modern insurance systems are built, enabling the industry to capitalize on the power of the cloud to run agile, intelligent, and evergreen operations. Authenticity, purpose, and transparency are core to Duck Creek, and we believe insurance should be there for individuals and businesses when, where, and how they need it most. Our market-leading solutions are available on a standalone basis or as a full suite, and all are available via Duck Creek OnDemand.