DELFI

Security for the DELFI Environment

September 2018
Version 1.0

Schlumberger

Accreditation and Certification: Protocols for control suitability and effectiveness and service management and delivery

Our industry-standard Service Organization Controls 2 (SOC2) accreditation for security and availability and ITIL®-certified workforce ensure that the DELFI cognitive E&P environment is fully secure and all best practices are adhered to for high-quality service delivery and management. The result is superior security and availability in the DELFI environment to meet the demands of your operations.

SOC2

Schlumberger has successfully completed the SOC 2 type 1 examination from an independent accredited auditing firm for the Security and Availability trust services categories set forth by the AICPA (American Institute of Certified Public Accountants). This ensures that all industry-standard practices are followed relative to the design suitability and operational effectiveness of the controls—giving customers increased confidence in the security and availability of the DELFI environment. The accreditation is renewed as new services move to general commercial availability.

We are currently pursuing SOC 2 type 2. For more information, please read the Trust Services Criteria published by the AICPA.

ITIL®

ITIL® is a widely accepted approach to IT service management. It contains a set of best practices describing processes, procedures, and functions for high-quality service delivery and management, and it is articulated around a lifecycle, including service strategy, design, transition, operations, and continual service improvement. ITIL® is the basis of the ISO/IEC 20000 standard.

The DELFI environment operating processes are aligned with the ITIL® framework and are supported by engineers who are ITIL® certified. Operations and service management toolsets used by the Schlumberger support organization are aligned with ITIL® to provide consistent customer service with a strong focus on quality. Schlumberger has more than 500 ITIL®-certified professionals companywide.

The DELFI Cognitive E&P Environment

Protects your operations from a wide variety of threats, including network breaches from unauthorized users, unapproved changes to operational procedures, malware, and computer viruses.

The dynamic DELFI environment, which is built using an agile security development lifecycle (SDL), is continuously updated to account for new security threats. A wide range of embedded features is employed to provide unparalleled system and operational security, identity management, and network and data protection.

Culture

Security is a core attribute of the DELFI environment and Schlumberger culture. Security begins at the pre-employment stage. Our global hiring and recruitment standard is followed across Schlumberger locations, with accommodation to local law requirements in various jurisdictions.

Schlumberger personnel are required to complete security trainings on IT security and customer data handling. Training records are captured and maintained, with required periodic refresher trainings to ensure that competency is up to date.

The Schlumberger performance management process encompasses quarterly performance reviews, including a review of security trainings and reminders for compliance.

Secure Development

Our secure development approach implements secure coding, security qualification, and tenant isolation. This multi-pronged approach embeds key security measures into the code and processes for each application in the DELFI environment.

Secure development lifecycle

Schlumberger has a comprehensive software development lifecycle framework in place called software lifecycle management (SLM). SDL is fully embedded into SLM and includes the following practices:

- Security review of architecture document, design document, and threat model
- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Source code review for code quality and third-party vulnerabilities
- Penetration testing.

Security qualification

Security qualification is a standard process that checks the readiness of an application for deployment against the security standard. Application teams are expected to maintain compliance throughout development and are audited at certain development stages. If necessary, third-party security consultants are used to perform security validations.

Tenant isolation

Tenant isolation helps us optimize utilization, maximize efficiency, and minimize cost. The DELFI environment achieves it by implementing logical isolation at the application layer, network layer, or data layer. Tenant isolation ensures that the data is not accessible across tenants.

Identity Management

The DELFI environment leverages a security perimeter built around identity controls.
We implement an identity management plan that protects your data by ensuring only authorized users have access to the data they need at the precise moment they need it.

Unified identity

The DELFI environment leverages a centralized authentication service for customers to access services using a single set of credentials. Unified identity provides improved security and efficiency and a richer user experience.

Identity federation

The DELFI environment supports single sign-on (SSO) with federated authentication to securely and conveniently grant access leveraging the customer's corporate credentials. We recommend that our customers opt-in for this mechanism because it enables them to have complete control of their identities. An alternative option for customers is to to register in the DELFI environment through which users manage their identities. Both this option and SSO support multifactor authentication to protect from credential theft.

Self-service authorization

Within the DELFI environment, customers control the access entitlements through the customer account. The customer's authorized personnel can approve or reject requests to access subscriptions. Only users with an active subscription can access the DELFI environment.

Physical security

The cloud infrastructure for the DELFI environment is deployed on the Google Cloud Platform and Microsoft Azure. These cloud service providers (CSPs) have 24x7 staffed security at their facilities, fully redundant power backup systems, physical access controls, and digital surveillance systems. More information about the physical security of the Google Cloud Platform and Microsoft Azure is available on the Google and Microsoft sites.

Network protection

Threats to the DELFI environment are mitigated with a multilayered approach to network security that keeps your data safe and accessible. Our approach focuses on perimeter protection and network segmentation to keep unauthorized users out and isolate threats.

Perimeter protection

The DELFI environment has implemented industry-standard mechanisms to protect and monitor the network perimeter. All services and resources are protected using firewall policies designed to allow only necessary network traffic and block all other traffic.

Network segmentation

The network architecture of the DELFI environment is based on the principle of network segmentation. Various components of the environment are deployed in isolated network segments and only desired network traffic is allowed.

System security

System security is the process of ensuring system integrity, confidentiality, and availability. It involves specific steps or measures to protect the system from threats, viruses, worms, malware, or remote hacker intrusions.

Endpoint protection

The DELFI environment uses a range of security software to safeguard from malicious code. Antivirus, antimalware, and vulnerability monitoring agents are deployed on every server and virtual machine.

Patch management

We follow industry standard practices for patch management. This ensures the latest versions of operating systems, software frameworks, and libraries are applied to the DELFI environment. Servers and virtual machines are deployed with validated patches and updates.

Hardening

Every server and virtual machine is hardened and locked down by default. The DELFI environment uses the Center for Internet Security (CIS) benchmark for operation system hardening. For the DELFI environment cloud infrastructure, our CSPs provide endpoint protection, patch management, and hardening.

Data protection

Safeguards, including encryption and backup and restore processes, are in place at every stage of the data lifecycle to protect and secure your data and mitigate data loss.

Encryption

Customer data is always encrypted. Customer data is protected by end-to-end encryption (AES128 bit or better), both at rest and in transit. The DELFI environment uses key management solutions provided by our CSPs for encryption keys and other credentials.

Backup and restore

Different backup and restore processes are used depending on the categorization of the data that needs protection. Some data categories use snapshots whereas others can be fully redeployed in case of a major failure. Encrypted backups are used for encrypted data.

Operational security

Operational security comprises a comprehensive set of policies, standards, and controls to ensure secure delivery of service.

Privileged access management

Privileged access is disabled by default and only enabled on request basis to perform specific administrative activity. Privileged access is managed through a centralized privileged access management (PAM) tool. All privileged access accounts are reported and reviewed monthly. All activities are recorded for audit purposes.

Change management

Schlumberger leverages the ITIL® framework for change management. Every change is evaluated, approved, and recorded in the change management system. Only authorized operations team members can execute any change, which is controlled and monitored by a change management system.

Always-On Protection: 24/7 incident detection that safeguards your data

With constant monitoring and 24/7 alerts, each service in the DELFI cognitive E&P environment is protected from brute force attacks and other cybersecurity threats.

Monitoring

Monitoring is built into each service. Different monitoring tools are used depending on the service and CSP used. Any service component that has log-on service is monitored for brute force attacks and other suspicious events, such as repeated failures to logon to accounts with elevated privileges.

Alerts

Alerting tools are used to generate alerts of unusual or suspicious activity in the system. All alerts are serviced by a 24/7 team that processes and investigates each event. Alerts are processed in accordance with the appropriate incident management process for that service. This includes escalation as required to security specialists or escalation as a recognized cyberattack.

Keeping Your Operations on Track: Incident management that mitigates risks to data security and minimizes NPT

Cybersecurity incident response teams are trained in managing a wide array of cybersecurity threats to mitigate risks to your data and get your operations back to business as soon as possible.

Defined processes

The incident management process manages service interruption or degradation to restore service to normal operation as quickly as possible.

This includes cybersecurity incidents too. An important part of incident management is the response to suspicious security events. The cybersecurity response plan helps to prepare for and meet critical needs during a major security incident.

Trained team

All employees complete a controlled training plan that gives them the skills to handle incidents efficiently and professionally. To complete training, adherence to these procedures is strictly required at all times.

Drills

Regular cybersecurity drills measure the readiness of support teams to manage cybersecurity incidents and validate security controls and processes. These drills are fully documented with root cause analysis, lessons learned, and improvement actions. Each drill is used as an opportunity to improve cybersecurity incident response processes.

Schlumberger