A-LIGN

# Hilti ON!Track

Type 2 SOC 3

2025

ON!TRACK

# SOC 3 FOR SERVICE ORGANIZATIONS REPORT

## December 1, 2024 to February 28, 2025

# Table of Contents

# SECTION 1

# ASSERTION OF HILTI ON!TRACK MANAGEMENT

## ASSERTION OF HILTI ON!TRACK MANAGEMENT

March 13, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Hilti On!Track's ('Hilti' or 'the Company') ON!Track Application Services System throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that Hilti's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Hilti On!Track's Description of Its ON!Track Application Services System throughout the period December 1, 2024 to February 28, 2025" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that Hilti's service commitments and system requirements were achieved based on the trust services criteria. Hilti's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Hilti On!Track's Description of Its ON!Track Application Services System throughout the period December 1, 2024 to February 28, 2025".

Hilti uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Hilti, to achieve Hilti's service commitments and system requirements based on the applicable trust services criteria. The description presents Hilti's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Hilti's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Hilti's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Hilti's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2024 to February 28, 2025 to provide reasonable assurance that Hilti's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Hilti's controls operated effectively throughout that period.

Marco Dietz

Marco Dietz
Head of Project Management
Hilti On!Track

## SECTION 2

## INDEPENDENT SERVICE AUDITOR'S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Hilti On!Track:

*Scope*

We have examined Hilti On!Track's ('Hilti' or 'the Company') accompanying assertion titled "Assertion of Hilti On!Track Management" (assertion) that the controls within Hilti's ON!Track Application Services System were effective throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that Hilti's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Hilti uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Hilti, to achieve Hilti's service commitments and system requirements based on the applicable trust services criteria. The description presents Hilti's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Hilti's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Hilti, to achieve Hilti's service commitments and system requirements based on the applicable trust services criteria. The description presents Hilti's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Hilti's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

*Service Organization's Responsibilities*

Hilti is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Hilti's service commitments and system requirements were achieved. Hilti has also provided the accompanying assertion (Hilti assertion) about the effectiveness of controls within the system. When preparing its assertion, Hilti is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively

- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

*Independence and Ethical Responsibilities*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

*Inherent Limitations*

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

*Opinion*

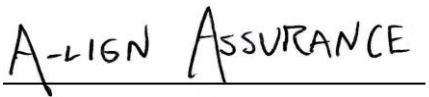
In our opinion, management's assertion that the controls within Hilti's ON!Track Application Services System were suitably designed and operating effectively throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that Hilti's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Hilti's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Hilti's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

*Restricted Use*

This report, is intended solely for the information and use of Hilti, user entities of Hilti's ON!Track Application Services during some or all of the period December 1, 2024 to February 28, 2025, business partners of Hilti subject to risks arising from interactions with the ON!Track Application Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.




Tampa, Florida
March 13, 2025

# SECTION 3

# HILTI ON!TRACK'S DESCRIPTION OF ITS ON!TRACK APPLICATION SERVICES SYSTEM THROUGHOUT THE PERIOD DECEMBER 1, 2024 TO FEBRUARY 28, 2025

## OVERVIEW OF OPERATIONS

### Company Background

Hilti stands for innovation and direct customer relationships. About 34,000 employees around the world, in more than 120 countries, contribute to making customers' work more productive, safer and more sustainable. Hilti does this with hardware, software and service offering.

Founded in 1941 by brothers Eugen and Martin Hilti, the company builds on strong roots and continuity. This long-term commitment has supported Hilti in becoming a reliable partner for customers and a trusted brand that they choose to work with.

### Description of Services Provided

Hilti ON!Track is a leading global solution specifically designed for construction companies and professionals for managing and tracking equipment, consumables, and other assets. With the increased transparency on all assets, ON!Track helps construction companies to become more productive.

Available globally, this professional solution helps manage all construction assets and equipment, regardless of the manufacturer. The software makes it easy to track and search for assets to minimize losses, to maintain inventory lists quickly and easily, to automate asset transfers between locations, and to get automated alerts as reminders for repairs, servicing, and inspections. It also has a powerful module to manage consumables and commodities with functionalities ranging from stock level monitoring to replenishment proposals.

*Overview of the ON!Track offering*

| MODULE / BUNDLE | READY | LITE | PRO | ENTERPRISE |
|---|---|---|---|---|
| **Hilti tool management** | ✓ | ✓ | ✓ | ✓ |
| **Equipment management** | - | ✓ | ✓ | ✓ |
| **Basic Asset cost reports** | - | - | ✓ | ✓ |
| **Quantity items management** | - | - | ✓ | ✓ |
| **ON!Track Unite** | - | - | ✓ | ✓ |
| **Proactive asset tracking** | - | - | ✓ | ✓ |

*Module description*

**Equipment management (ON!Track Lite/Pro/Enterprise).** Management of Assets, workers, certificates (e.g. learning achievements, etc.), creation of reports and insights into asset usage.

**Basic asset cost reports (ON!Track Pro/Enterprise).** Basic management of jobsite Asset costs. Customizable cost reporting by Asset, jobsite, or time period.

**Quantity items management (ON!Track Pro/Enterprise).** Quantity items include consumables and commodities. Management of inventory levels and material locations, re-order alerts, reports for monitoring consumption.

**ON!Track Unite -** ON!Track Unite's openAPI and built-for-you integrations bring productivity to new heights by unifying data from multiple sources, increasing data quality and consistency, and automating processes involving ON!Track and other applications.

**Proactive Asset tracking (ON!Track Pro/Enterprise).** Hilti IoT hardware integration to ON!Track allows for digitized, proactive and automated asset management for Hilti IoT ready assets. Automation covers inventory and Hilti IoT ready assets being transferred automatically between Gateway enabled locations. Proactive tracking also includes:

- Heavy machinery management, leveraging telematics technology to manage heavy construction machinery and heavy equipment accessories in ON!Track
- Van inventory management, remotely managing inventory in mobile storage units such as service vans and integrating them in ON!Track
- Access to Service Provider's global Bluetooth network of Gateways which are scanning for Hilti Bluetooth tags, powered by a global presence of already installed telematics gateways

**Principal Service Commitments and System Requirements**

Hilti has designed its processes and procedures to meet its objectives for its ON!Track service. These objectives are established to incorporate the commitment to competence of the executive team throughout the organization.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offered provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the application are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit is in place.

Hilti establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Hilti's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

**Components of the System**

*Infrastructure*

Primary infrastructure used to provide the ON!Track Application Services System includes the following:

| Primary Infrastructure | | |
|---|---|---|
| **Hardware** | **Type** | **Purpose** |
| Backend and Processing Servers | AWS EC2 (AWS-managed AMIs, Instance size varies) | Runs ON!Track application programming interface (API) and background processing through virtualized container-based infrastructure |
| Databases | AWS RDS and AWS RDS Aurora | Runs production Postgres databases for ON!Track data with daily backups |
| Databases | In cluster REDIS | Runs production Redis for data caching of ON!Track microservices |
| Content Delivery Network (CDN) | AkamaiCDN | Content delivery network caching static data for better user response times |
| Firewall | Akamai WAF | Web application firewall to protect ON!Track against attacks (e.g. Bot attacks) |
| API Gateway | Axway API Gateway | API gateway routing traffic, validating tokens and applying rate limiting |

*Software*

Primary infrastructure used to provide the ON!Track Application Services System includes the following:

| Primary Software | | |
|---|---|---|
| **Software** | **Operating System** | **Purpose** |
| CloudWatch | Not applicable | Aggregate and store AWS system metrics and service logs for ON!Track monitoring purposes |
| CloudTrail | Not applicable | Aggregate and store AWS security and audit logs being forwarded to Security Operations Center |
| Prometheus | Not applicable | Aggregate and store application and cluster metrics of ON!Track production system |
| Grafana | Not applicable | Display ON!Track system metrics in dashboards for monitoring purposes |
| PagerDuty | Not applicable | Aggregate and alert around reported errors and metrics |
| Sentry | Not applicable | Aggregate and alert around errors reported from production ON!Track application |
| AWS Backup | Not applicable | Run daily backups of production ON!Track data |
| Google Analytics | Not applicable | Aggregate and store engagement metrics from production web, iOS and Android apps |
| Firebase | Not applicable | Aggregate and store errors and crashes and remote app configuration from production iOS and Android apps |

| Primary Software | | |
|---|---|---|
| **Software** | **Operating System** | **Purpose** |
| Microsoft Entra | Not applicable | Identity and Access Management |
| AWS IAM | Not applicable | Identity and Access Management |

*People*

The ON!Track staff provides support for the above services in each of the following functional areas:

- **Senior Management** - Senior management, under the standard of due care and ultimate responsibility, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision-making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.
- **Security Committee** - The Security Committee is comprised of the Quarterly Risk Management-Information Security meeting attendees. In addition to discussing existing risks, threats and vulnerabilities, the team identifies risks mitigated by controls already in place. Remaining residual risks are included in the analysis of the effectiveness of security protection on the environment in the scope of the specific risk.
- **Head of Technology and Platform (T&P)** - The Head of T&P is responsible for the IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
- **System and Information Owners** - The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically, the system and information owners are responsible for changes to their IT systems. Thus, they usually must approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.
- **System Users** - The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, employee system and application users are provided with annual security awareness training, and customer users receive security guidance and documentation during onboarding and through support functions.

*Data*

Customer data is managed, processed, and stored in accordance with the relevant data protection laws and other regulations, with specific requirements formally established in customer contracts. Hilti utilizes only encrypted channels to process data within its system architecture. ON!Track is built to wipe customer authentication credentials immediately after authentication is complete, and the application and service offering itself requires no data-level access.

*Processes, Policies and Procedures*

Formal IT policies and standards exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Hilti policies and standards that define how services should be delivered. These are located on the Company's SharePoint Drive and in the Employee Handbook where it can be accessed by any Hilti ON!Track team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

See 'Subservice Organization' section below for more information.

Logical Access

Hilti uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Employee access to the AWS environment is controlled, by User groups in the Hilti Microsoft Entra ID authentication tool that are connected through SAML (Security Assertion Markup Language) with AWS IAM (Identity and Access Management) roles. User, role-based, access is controlled in the application and authenticates to the database.

All assets, both production and corporate, are tracked and the inventory receives routine updating. Each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Passwords must conform to defined, complex, password standards and are enforced through parameter settings in the Hilti Microsoft Entra ID.

Remote access into the production environment is tightly restricted to only authorized workers based on their role. Workers accessing the production and development systems remotely require secure, encrypted transport protocol to access and a second-factor authentication mechanism in the form of token, along with user ID and complex password.

On an annual basis, managers perform access reviews for all workers with access in the system used to develop ON!Track to assess the appropriateness of the access and permission levels and request modifications based on the principle of least-privilege, whenever necessary.

Computer Operations - Backups

Backup is done in a separate AWS region, with limited access, to protect it against regional disasters, unauthorized changes and ransomware attacks. Backup is encrypted and access control management is implemented. Daily backups for production are retained for 14 days (protection against general system failures not individual user deletions), and failure alerts are received by the Backup System and Information Owner and designees. Failed backups are investigated and resolved in a timely manner.

Hilti utilizes continuous monitoring tools with alerting enabled to assess system health and errors which would signal if there were backup system issues. In addition, Management reviews the testing performed to validate the operating effectiveness of the AWS backup and recovery controls.

Computer Operations - Availability

Hilti monitors the capacity utilization of physical and computing infrastructure to ensure that service delivery matches service level agreements by monitoring the dashboards, related metrics and alerts. Hilti evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Hilti utilizes the vendor alerts and dashboards for system metrics health to monitor the firewall, application and database servers and infrastructure routers and switches. Network traffic (e.g. Requests/sec) along with the servers' compute and memory usage, as well as storage space and interactions are monitored.

Additionally, multiple monitoring tools are deployed on the application, and the System Users receive and review all application/web server pre-defined error alerts and take action to remediate in accordance with the incident response procedures.

Hilti has implemented an Incident Response policy and procedures to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

The ON!Track platform is hosted separately by AWS; therefore, AWS is responsible for implementing environmental security controls over the housed in-scope systems. Refer to the 'Subservice Organizations' section below for controls managed by the subservice organizations.

Change Control

Hilti maintains documented Infrastructure and Code Change Development policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance ('QA') testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. QA testing, code reviews, and user acceptance testing results, whenever applicable, are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Changes are approved prior to migration to the production environment and approvals are documented within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. It also facilitates the code review process which is required for all changes.

Infrastructure changes are performed by Hilti's infrastructure as a service provider, AWS, who houses the Hilti production environment within AWS data center locations. AWS is responsible for applying firmware and security patches; however, Hilti actively monitors vendor and security industry vulnerability notifications impacting its infrastructure servers, routers, databases, and operating systems to ensure timely patching by AWS personnel. In addition, Management reviews the testing performed by independent auditors, as documented in Section 4 of the AWS annual SOC 2 report, to validate the operating effectiveness of the AWS backup and recovery controls.

Data Communications

The Hilti system components use encrypted communication channels between each other. Network access restrictions are in place throughout the infrastructure. IP whitelisting via VPC Security group is used to only allow traffic from authorized devices and locations. Remote access is gained by a limited number of authorized administrators who must provide a second-factor authentication mechanism, in the form of token, along with user ID, and complex password for each system. AWS is utilized to alert administrators of all security configuration changes made to production servers. Unexpected and potentially unauthorized changes are investigated in a timely manner.

In addition, Hilti utilizes vulnerability scanning tools and regular security reviews to identify development and production environment vulnerabilities, including insecure connectivity protocol, on an ongoing basis. Management investigates and resolves medium and high-risk vulnerabilities noted in a timely manner.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Hilti. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

**Boundaries of the System**

The scope of this report includes all of the ON!Track Application Services System performed at the principal offices of Hilti located in Schaan - Liechtenstein (HQ), Kaufering - Germany, Pune - India and Kuala Lumpur - Malaysia.

This report does not include the cloud hosting services provided by AWS at the multiple facilities.

**Changes to the System in the Last 3 Months**

No significant changes have occurred to the services provided to user entities in the three months preceding the end of the review period.

**Incidents in the Last 3 Months**

No significant incidents have occurred to the services provided to user entities three months preceding the end of the review period.

**Criteria Not Applicable to the System**

All Common/Security and Confidentiality criteria were applicable to the Hilti ON!Track Application Services System.

**Subservice Organizations**

This report does not include the cloud hosting services provided by AWS at the multiple facilities.

*Subservice Description of Services*

AWS provides cloud hosting services, which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

*Complementary Subservice Organization Controls*

Hilti's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Hilti's services to be solely achieved by Hilti. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Hilti.

The following subservice organization controls should be implemented by AWS and included in this report to provide additional assurance that the Trust Services Criteria are met:

| Subservice Organization - AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security | CC6.4 CC7.2 | Physical access to data centers is approved by an authorized individual. |
| | | Physical access is revoked within 24 hours of the employee or vendor record being deactivated. |
| | | Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. |
| | | Physical access points to server locations are recorded by closed circuit television camera CCTV. Images are retained for 90 days, unless limited by legal or contractual obligations. |
| | | Physical access points to server locations are managed by electronic access control devices. |
| | | Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. |

Hilti management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, Hilti performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Holding periodic discussions with vendors and subservice organization(s).

**COMPLEMENTARY USER ENTITY CONTROLS**

Hilti's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Hilti's services to be solely achieved by Hilti control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Hilti's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Hilti ON!Track.
2. User entities are responsible for notifying Hilti of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Hilti services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Hilti services.

6. User entities are responsible for providing Hilti with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Hilti of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.