HCLSoftware

HCL MyXalytics

Security Trust Center Document

Version 1.0

Table of Contents

Document Revision History

This guide is updated with each release of the product or when necessary.

This table provides the revision history of this HCL MyXalytics Trust Center.

Version No.	Version Date
November, 2025	HCL_MyXalytics_Security_Trust_Center_Document_v1.1

1 HCL MyXalytics Trust Center

At HCL Software, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundations of our products. The HCL Software security strategy covers all aspects of our business, including corporate and organizational security policies, incident management and response, business continuity and disaster recovery, secure software development processes, and privacy.

This Trust Center provides a transparent overview of the principles and practices governing HCL MyXalytics, giving you the confidence to leverage our product for visibility and insights for your hybrid-cloud environments.

1.1 Introduction

The HCL MyXalytics platform is a unified reporting and predictive analytics solution designed to provide unparalleled visibility into IT systems and processes. MyXalytics provides a robust security posture designed to protect customer data, ensure service availability, and meet stringent compliance requirements.

This unified reporting and dashboarding software is an enterprise-ready solution that aggregates data from various IT tools to create insightful reports and dashboards. MyXalytics provides a consolidated view of IT operations, helping decision-makers optimize costs, reduce risk, and drive continuous operational improvements. MyXalytics is designed as a platform where not only a unified view of the entire IT landscape is provided, but also predictive analytics and FinOps can be performed as actions where it can forecast capacity and generate cost optimization recommendations from the collected data.

Data Sources

- **User**: Concerning the data in the application or the project, user details are one of the sources of data which is analyzed by using cognitive services, and a relevant response will be provided. The response can be a direct solution or further prompt understanding the query better. HCL MyXalytics can respond in a simple textual response.

- **ITSM**: HCL MyXalytics processes data from **IT Service Management (ITSM)** tools like ticketing systems and service desks. This data includes information on incidents, service requests, problems, and changes. Analysis of this data helps in optimizing service delivery, predicting potential service disruptions, and improving efficiency by identifying recurring issues and bottlenecks.

- **FinOps:** MyXalytics integrates with public cloud billing APIs and on-premises resources management APIs to enable FinOps Cost visibility and Cost optimization features (Cloud Financial Operations). It ingests data on resource usage, cost, and billing from cloud providers (like AWS, Azure, and Google Cloud). The platform analyzes this data to provide insights into cost optimization, budget forecasting, and resource allocation. Security for FinOps data focuses on strict access policies and compliance to protect sensitive financial and operational information.

- **System/Database/App monitoring:** HCL MyXalytics collects and analyzes data from various monitoring tools for systems, databases, and applications. These data sources include metrics on CPU utilization, memory usage, network traffic, database query performance, and application response times. This enables proactive

identification of performance degradation, resource bottlenecks, and system anomalies. Security protocols for this data ensure its integrity and prevent unauthorized access to the underlying infrastructure information.

- **Event management:** The product leverages event management data, which includes events and alerts from devices like Servers, Network devices, Databases and Applications. By aggregating these events HCL MyXalytics can analyze the event management efficiency.

AI and Foundation Models Integration

The platform integrates with leading AI providers to power automation:

- **Azure OpenAI**: Advanced LLMs for natural language understanding

Security

We integrate security into every phase of the product lifecycle, from concept to deployment, to protect your data and infrastructure.

Secure by Design

HCL MyXalytics is developed in-house following a secure software development lifecycle. The product undergoes a comprehensive threat modeling assessment to proactively identify, evaluate, and mitigate potential security risks from the ground up.

- **Secure-by-Design Architecture**: Adheres to best practices for data encryption, access controls, and secure authentication mechanisms.

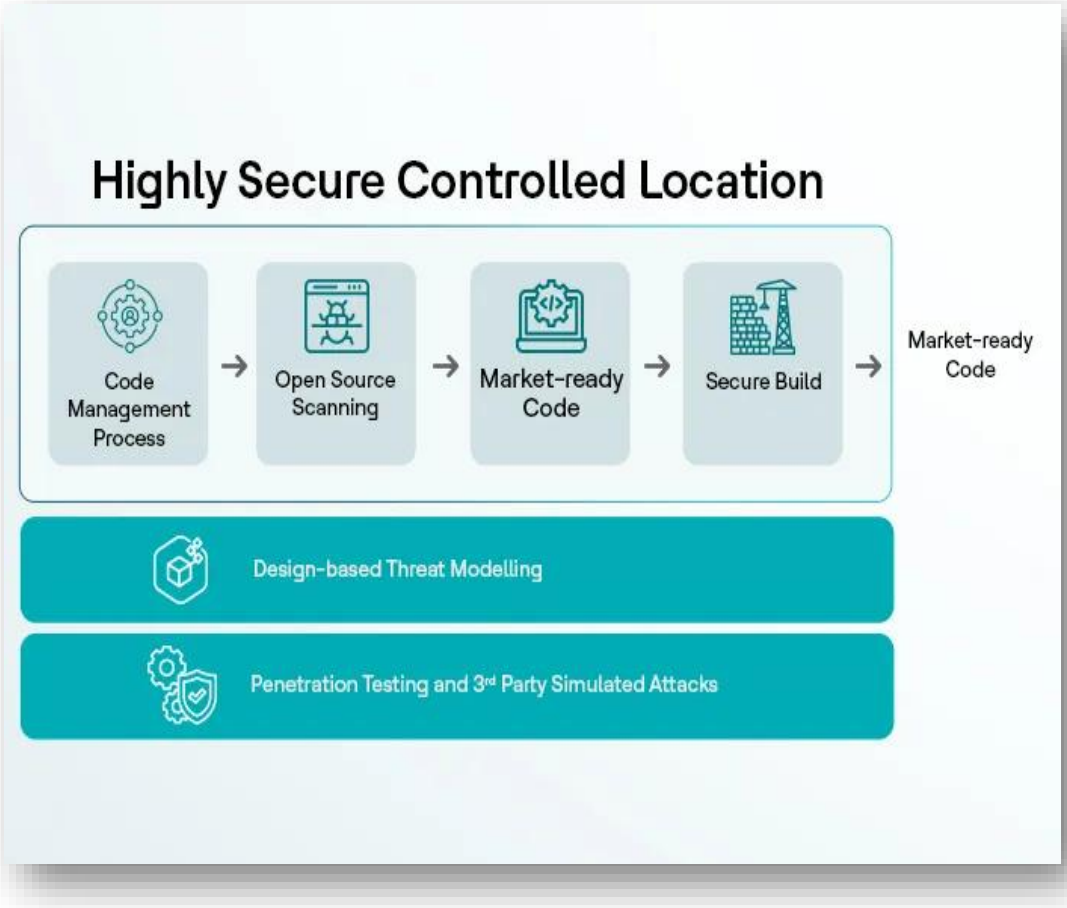
Encrypted Transmission:

  - Data at Rest: All data stored is encrypted using AES-GCM 256-bit encryption, ensuring confidentiality and integrity at rest.
  - Data in Transit: As the portal shows summarized data to users it is transmitted over secure channels such as the TLS 1.2/1.3 mechanism.

- **Audit Logs & Role-Based Access Control**: Complete tracking of user and system activity ensures traceability and accountability.
- **Third-Party Component Vetting**: All dependencies and libraries undergo rigorous vulnerability and license compliance checks.

Secure Product Development

HCL Software adheres to stringent development processes to produce the code we develop and provide for our customers. All Development practices incorporate change control and are the key criteria assessed at release approval stage including key practices around following:



- Threat Modeling - Threat modeling is the process of identifying and prioritizing potential threats to a system and finding solutions to mitigate them.
- Secure Design Review - Secure Design Review is an assessment done for a product by the HCLSoftware Security team to understand the product architecture, means of deployment / delivery and various other security measures which are in place, as per the industry standards
- Data Privacy Assessment - HCL Software's Privacy and Data Protection by Design and Default (PbD for short) addresses privacy requirements to meet those laws and regulations and asks all product teams to work with these requirements in the design phase and test them in the verification phase of the development project. HCL Software leverages the One Trust Platform to perform Data Privacy assessments for products, platforms and Operations Support
- Static and Dynamic Application security testing
- Code Quality Analysis
- Open-Source Code Composition and Vulnerability Analysis
- Penetration Testing - Performed by Internal (for every release) and External (once in calendar year) teams.

Secure distribution of binary: The binaries for the product are securely distributed via MHS Portal. My HCL Software (MHS) is a web application for HCL Software customers and partners that provides a new and improved way to find and quickly download the latest HCL Software product releases as well as supported older releases. All binaries are cryptographically

signed. The system verifies signatures to prevent tampering. MHS provides seamless access to resources and tools designed to effectively manage the use of HCL Software products and services.

- Usage metering and reporting
- Access-controlled content: users only see content appropriate for them
- Enables seamless access to resources and tools to help effectively manage the entire HCLSoftware experience

1.2 Security Incident Response and Bulletins

- **Security Bulletins & Vulnerability Management**: The HCLSW Product Security Incident Response Team (PSIRT) manages the receipt, investigation, and internal coordination of reported security vulnerabilities for HCL Software product offerings. The PSIRT coordinates with product development teams who investigate reported vulnerabilities and identify the appropriate response plan. For more information, visit the HCLSoftware PSIRT page.
- The HCL PSIRT publishes Security Bulletins describing any relevant CVEs and pointing to additional details and remediation. A list of security bulletins for HCL MyXalytics can be found on the official HCL Software support and community forums.
- **Product Security Training**: Periodical training sessions are conducted for product teams on Secure Development, ISMS, Data Privacy, PSIRT Process, and more.

Data Privacy

Data privacy (also called information privacy) refers to the right of individuals to control how their personal information is collected, used, shared, and stored. It's about ensuring that personal or sensitive data is handled in ways that protect people's rights and maintain their trust.

In our relationship, the **customer is the data controller**, retaining full ownership and control over the data collected and determining the purpose of its use. For more information visit HCL Software Privacy

1.2.1 Purpose, Limitation, and Data Minimization

The platform is designed to process personal data for the sole purpose of product administration and fulfilling our contractual obligations. We practice data minimization, and the product is not designed to process any special categories of sensitive personal data. Customer Information Processed: The platform may process the following customer information as part of its standard functionality:

- Contact Information: Organizational Email Address
- Personal Identification: First Name, Full Name, Last Name
- User Account Information: Login ID
- Browsing Information - Session Time and IP Address
- Business Unit name/Company/Customer Name

1.3 Responsible AI Controls

1.3.1 Human Resources Security

Human resources security practices, background checks, and training processes are taken care of by the HCL Software team.

1.3.2 Risk management

HCL Software has a formalized risk management program that aligns with ISO 31000 and ISO 27005 best practices, as well as ISO 27001/27002.

Risk management processes are integrated with other management systems, such as the Information Security Management System (ISMS). Security controls are implemented in accordance with our ISMS to manage risk across the organization.

Responsibility for Risk Management

To drive the remediation of risks, our program reports risk status and escalates where necessary to senior management to inform business decision-making. Senior executives have overall responsibility as risk owners for mitigation, avoidance, transference, or acceptance of the risk. HCL Software uses a combination of weekly, monthly, and quarterly meetings and reports to ensure communication of risks.

Every HCL Software staff member is responsible for the effective management of risk, including the identification of potential risks, the development of risk mitigation plans, and the implementation of risk reduction strategies.

1.3.3 AI Risk Management

HCL Software has defined processes and procedures for managing and assessing information systems and operational security risks. HCL MyXalytics undergoes regular assessments to identify and assess the likelihood and impact of risks. These potential risks include unauthorized access, use, disclosure, or disruption to HCL MyXalytics systems and customers. Risks are categorized in accordance with a formally documented procedure.

Any identified risk is managed in a timely manner to safeguard the confidentiality, integrity, and accessibility of HCL MyXalytics systems and customer data.

1.4 GEN AI Data Security & Responsible AI Controls

MyXalytics takes a defense-in-depth approach to securing Generative AI systems, covering user data, model interactions, infrastructure, and ethical governance.

1. **User Data Protection**
    - **Encryption in Transit and at Rest**: All user inputs, outputs, and metadata are encrypted using TLS 1.2/1.3 for data in transit and AES-256 for data at rest.
    - **Zero Retention of Sensitive Inputs**: User prompts or responses classified as sensitive are not retained unless explicitly required and approved by the customer.
2. **Access Control & Identity**

- **Role-Based Access Control (RBAC)**: Fine-grained access is enforced to ensure only authorized users can interact with or configure AI services.
- **Single Sign-On (SSO) & SAML 2.0 Integration**: Federated identity ensures authenticated access aligned with enterprise identity providers.
- **Audit Logs**: All access and activity logs are captured and monitored for suspicious behavior.

3. **API & Model Access Security**
   - **API Key Management**: API keys are securely generated, rotated, and stored in secure manner using AES-256 encryption.
   - **Scoped Access**: APIs are protected with least-privileged permissions and rate-limiting to avoid abuse or overuse. Public facing APIs are hosted behind the API gateway with rate limiting.
   - **Defender for Cloud**: Continuous security posture management with Azure Defender for Cloud (or similar services) ensures compliance, threat detection, and remediation for AI workloads.
4. **Content Filtering & Prompt Validation**
   - **Content Filtering**: Reporting module uses LLM's for text summarization only and content is mostly the summarized numbers against the native system generated entity names. Additional checks are in place prevent users to entering any toxic, harmful or restricted content in reports title.
   - **Prompt Injection Protection**: Report titles, entities and numbers are fed to the LLM's as artifacts and not used to set the context. Prompts to set the context are not available for users.
5. **Secure Development Practices**
   - **OWASP for GenAI**: Regular testing is conducted against OWASP Top 10 for Large Language Models (LLMs), including:
     - Prompt injection
     - Model denial-of-service (DoS)
     - Insecure plugin design
     - Sensitive information disclosure
     - Inadequate sandboxing
     - Supply chain vulnerabilities
6. **Responsible AI and Ethical Safeguards**
   - **Explainability & Auditability**: All AI outputs are traceable with logs and rationales for key decision-making.
   - **Human-in-the-Loop Review**: Product is using Gen AI models for text summarization only and no actions are triggered based on the model response. Prompts for summarization are reviewed before they are enabled on the production.

1.4.1 Secure MLOps Lifecycle Management

Data Sourcing & Preparation

- Access control to data sources via RBAC
- Automated data provenance and lineage tracking
- Data poisoning prevention through schema validation and anomaly detection

Model Training

- Encrypted communication for distributed training nodes
- Adversarial robustness testing to pre-empt evasion attacks

Model Deployment

- All deployments containerized with minimal base images
- Deployment policies enforce runtime security constraints

Model Governance

Model Lifecycle Management

- Version control: Tracking different versions of models, datasets, and features.
- Lineage tracking: Recording data sources, transformations, training parameters.

Data Governance

- Data quality monitoring: Checking for missing, corrupt, or skewed data.
- Data lineage: Traceability from raw sources to model inputs.
- Privacy compliance: Ensuring privacy is respected (e.g., through anonymization, consent logging).

Model Explainability & Interpretability

- Use of integrated model-specific explainers.
- Model Cards

Fairness & Bias Monitoring

- Pre- and post-deployment bias checks across attributes (gender, race, etc.).
- Fairness metrics: e.g., equal opportunity difference, demographic parity.

Model Performance Monitoring

- Drift detection: Concept and data drift.
- Performance degradation tracking: E.g., AUC, F1-score over time.

Auditability & Traceability

- Comprehensive logging: Who trained what, when, using which data and parameters.
- Audit trails: For external compliance and internal accountability.

Access Control & Security

- RBAC: Role-based access control on models and datasets.
- Model encryption and secure deployment.
- Secure APIs and access tokens for inference.

Retraining & Lifecycle Refresh

- Triggered by performance decay or data drift.
- Appropriate role needed for retraining.
- Tracking retraining logic, triggers, and audit logs.

2 Summary

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test and deliver effective and secure reporting and analytics solutions to our customers. For more information, please contact us.

HCLSoftware

hcltechsw.com