HCLSoftware

HCL iControl

Security Trust Center Document

Version 1.0

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Table of Contents

List of Figures

Document Revision History

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

This table provides the revision history of this Guide.

Version Date	Description
September, 2025	HCL iControl Security Trust Center v1.0

1 Our Commitment to Security & Trust

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundation of our products. The HCLSoftware 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 iControl, giving you the confidence to use our solution.

2 Introduction and Product Overview

This document provides a comprehensive overview of the security architecture, controls, and policies governing HCL iControl. It is intended for security architects, administrators, and compliance officers to understand the security posture of the product and their shared responsibilities in maintaining a secure environment.

2.1 Product Description

HCL iControl is an Enterprise Control Center (ECC) solution that provides businesses with real-time business flow observability. It delivers end-to-end visibility for all stakeholders, from CXOs to operations teams, by creating meaningful views from both business and technology perspectives. As an advanced business intelligence product, iControl helps organizations build resilience and minimize risks through real-time observability and predictive analytics. It enables users to understand business flow performance, identify where breaks occur, and determine which technological components are impacting business outcomes.

2.2 Deployment Models

HCL iControl is available in two distinct deployment models:

- **Standalone:** A containerized application designed to be deployed and managed by the customer on public cloud infrastructure, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.
- **Splunk App:** An application that is installed directly onto a customer-managed Splunk Enterprise instance.

This document will address the security posture of both deployment models, highlighting differences where applicable.

3 Shared Security Responsibility

HCL iControl follows a shared responsibility model for security. This partnership is crucial for maintaining a secure environment.

- **HCL's Responsibility:**
  - Designing and developing a secure application following secure coding practices.
  - Providing a product free from known vulnerabilities or disclosing the known vulnerabilities beforehand.
  - Clearly documenting the security features and configurations available to the customer.
  - Being transparent about the use of third-party components and encryption.
- **Customer's Responsibility**
  - Securely configuring and managing the underlying infrastructure (Cloud environment or Splunk Enterprise platform).
  - Implementing and managing access controls (authentication and authorization).
  - Configuring platform-level security features, such as encryption for data at rest in Splunk.
  - Managing the data ingested into iControl, including its classification and compliance with privacy regulations.
  - Regularly applying security patches and updates to the underlying platform.
  - Monitoring the security of their environment and responding to security incidents.

3.1 Standalone Version

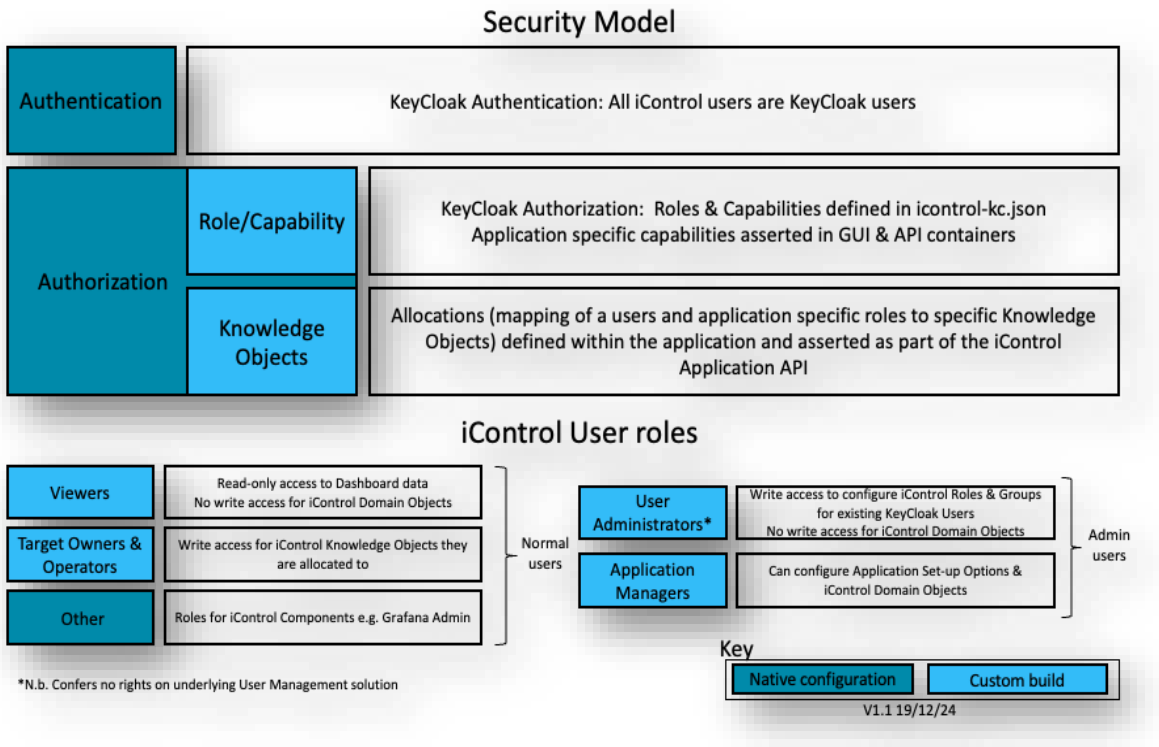

Figure 1 – iControl Security Model Standalone

This diagram shows how the key elements of Identification, Authentication and Authorization are controlled within the Standalone version of iControl: Key Cloak acts as an Identity Broker for underlying Identity

Providers and provides Authentication & Single Sign-on across the different components (e.g. Web, API, reporting tools). Application roles (and associated capabilities) are defined as custom roles within a dedicated KeyCloak realm with fine-grained authorization controls (for users and groups) configured within the iControl application.

3.2 Splunk App

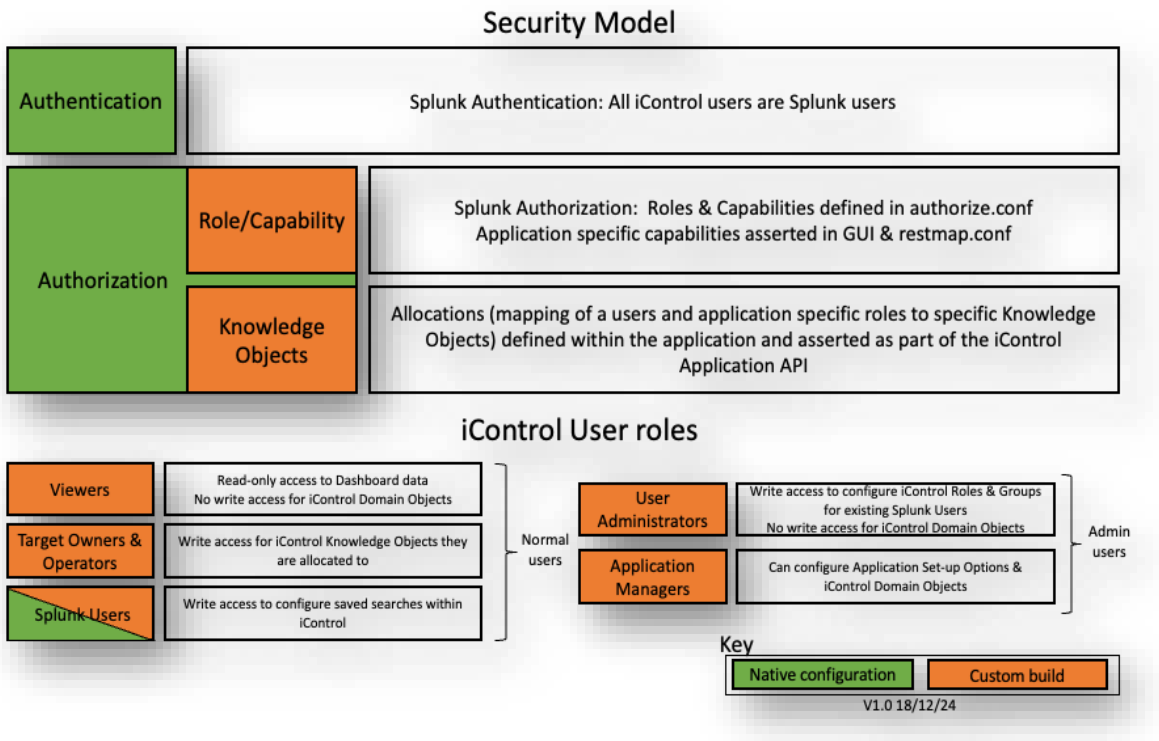

Figure 2 – iControl Security Model Splunk

This diagram shows how the key elements of Identification, Authentication and Authorization are controlled within the Splunk version of iControl: All iControl users are native Splunk users, so Splunk provides the underlying Identification, Authentication and Authorization. iControl application roles (and associated capabilities) are defined as Splunk application roles with fine-grained authorization controls (for users and groups) configured within the iControl application.

4 Architecture Overview

4.1 Standalone Version (AWS, GCP, Azure)

The standalone version of iControl is delivered as a containerized application, orchestrated using Kubernetes.

- **Core Application:** The iControl application logic runs in containers.
- **Data Storage:** The application utilizes platform-native storage services.
- **Secrets Management:** Kubernetes secrets are used for managing sensitive information like API keys and credentials. These are encrypted using the cloud provider's native key management services.

4.2 Splunk Application

The Splunk app version of iControl installs directly into a customer's Splunk environment. Its components and security are deeply integrated with the Splunk platform.

- **Dashboards and Views:** iControl provides a set of dashboards, views, and custom commands within the Splunk UI.
- **Data Processing:** The app leverages the customer's existing Splunk indexers and search heads to process and visualize data.
- **Configuration:** All configuration is managed through the Splunk UI or configuration files on the Splunk server.
- **Dependencies:** The security and performance of the iControl Splunk app are directly dependent on the health, configuration, and security of the customer's Splunk Enterprise deployment.

5 Access Control

5.1 Authentication

- **Standalone version (AWS, GCP, Azure):** The iControl standalone version has Keycloak as the identity broker bundled within the helm chart. iControl uses OIDC/OAuth 2.0 based standard authorization code flow user authentication from the web frontend as well as for any direct API integration. Keycloak as identity broker supports IDP integration with providers across a wide range of protocols (including but not limited to OIDC, OAuth2, SAML etc). It is the responsibility of the client to configure Keycloak to IDP integration depending on the IDP service being used for user authentication in a client's ecosystem.
- **Splunk App:** Authentication is entirely inherited from the underlying Splunk platform. Customers are responsible for configuring Splunk's authentication mechanisms. This can include:
  - Native Splunk user accounts and passwords.
  - Integration with external authentication systems like LDAP, Active Directory, or a SAML 2.0 Identity Provider.

5.2 Authorization

iControl uses a fine-grained authorization mechanism that is driven by two dimensions - user capabilities sourced from role definitions and entity level access-control list dynamically added based on business rules within backend before API endpoints respond back with data.

User capabilities influence the user's access to specific features within the application. For example - A user not having capability to view flows, will not see the Flows option in the main navigation menu. On the other hand, entity level ACLs drive the ability of a user to do operations on entities. For example - For a given user if a flow level ACL mandates delete is not possible, then the user will not be able to delete that specific flow.

- **Standalone version (AWS, GCP, Azure):**
  The pre-defined role definitions are part of the iControl helm chart and added into Keycloak during deployment. Any custom role creation can be done by clients post deployment using the Keycloak admin console. The standard roles include view-only, read-write and admin kind of roles. New custom roles using a mix of permissions can be created as per client specifications.
- **Splunk App:**
  Authorization is entirely managed by Splunk's native RBAC system. Access to iControl dashboards, views, and data is controlled by the roles and capabilities assigned to users within the Splunk instance. Customers can restrict access to sensitive iControl data by assigning users to Splunk roles with appropriate permissions and restricting access to specific Splunk indexes.

6 Data Encryption

HCL iControl leverages strong, industry-standard encryption to protect data. The cryptographic capability is active by default and cannot be modified by the user.

6.1 Encryption in Transit

- **Standalone version (AWS, GCP, Azure):**
  The frontend web application uses SSL connectivity with TLS 1.2+ encryption to secure the communication channel for all data exchanged between the user's browser and the iControl application.
- **Splunk App:**
  Encryption in transit is dependent on the customer's Splunk Enterprise configuration. It is the customer's responsibility to enable and enforce HTTPS (TLS) on their Splunk Web port (typically 8000) and Splunk management port (typically 8089) to secure all communication.

6.2 Encryption at Rest

- **Standalone version (AWS, GCP, Azure):**
  iControl leverages the native, pre-packaged encryption services of the respective cloud platform (AWS, GCP, Azure) for the secure storage of sensitive data at rest, such as application secrets.
  - The encryption services use **AES-256** bit encryption to protect data.
  - Specifically, the symmetric key algorithms used are:
    - AWS: AES-256-GCM
    - GCP: AES-256
    - Azure: AES-256
- **Splunk App:**
  Encryption of data at rest is entirely dependent on the customer's Splunk Enterprise configuration. HCL strongly recommends that customers enable Splunk's native index encryption to protect all data stored within Splunk, which iControl will then inherit. The customer is responsible for managing the encryption keys and settings.

6.3 Secrets Management

- **Standalone version (AWS, GCP, Azure):**
  When running as a containerized application, iControl uses the cloud platform's provided encryption services for encrypting secrets used by the Kubernetes engine. These secrets are stored in encrypted form within the Kubernetes etcd nodes on the respective platform, leveraging the "Encryption at Rest" capabilities described above.
- **Splunk App:**
  The iControl Splunk app leverages Splunk's Encrypted Credentials storage for any sensitive information it needs to store, such as API keys for integrations. It is the customer's responsibility to ensure their Splunk instance is properly secured.

7 Data Management

7.1 Data Archival

Data archival and retention policies need to be configured within the managed DB instances where iControl data persisted. The DB instances are provisioned and managed as per customer's own archival and retention policies. iControl doesn't influence those in any way.

7.2 Data Return and Destruction

Not applicable to iControl as product deployment is done within the client's infrastructure.

7.3 PII and Sensitive

HCL iControl does not inherently collect Personally Identifiable Information (PII). The customer is responsible for the data they choose to ingest into iControl and for ensuring that no unnecessary sensitive or PII data is processed.

8 Availability and Disaster Recovery

8.1 Standalone Version (AWS, GCP, Azure)

The standalone version runs on Kubernetes based stack. This brings in the auto scaling capabilities of k8s into play. The default configuration comes with replicas count of 2, thereby provisioning 2 pods per component for high availability. It is ensured that the 2 pods are created on nodes that are hosted in different zones. Clients can follow the best practices for HA of respective cloud providers when creating a kubernetes cluster to ensure nodes are created in multiple zones.

The pods that run as part of iControl deployment have necessary liveness and readiness probes implemented which enable auto-healing of pods in case of pods go down.

With regards to disaster recovery, database recovery is outside scope of product deployment as databases are hosted within cloud service provider's managed SQL services. As far as product deployment recovery is concerned, clients are expected to follow the disaster recovery procedures and practices that each cloud service provider recommends for production grade Kubernetes based infrastructure.

8.2 Splunk App

The availability and disaster recovery of the iControl Splunk app are **directly dependent on the customer's Splunk Enterprise architecture**. Customers are responsible for implementing a resilient Splunk deployment, which may include Splunk indexer clustering for HA and Search Head Clustering for search availability.

9 Logging and Monitoring

9.1 Standalone Version (AWS, GCP, Azure)

- **Logging stack** – Alloy, Loki, Grafana
- **Application logs** – Logs generated by services running as pods, are collected by Grafana Alloy agents running on each cluster and forwarded to the target Loki instance for logs collection. Grafana is used to view the logs and conduct log analysis.
- **Access logs –** Generated by relevant components (Keycloak, backend services) and processed similar to the way application logs are processed.
- **Monitoring –** Kubernetes monitoring is done using Prometheus with alertmanager driven alerting support.

Note: Alloy, Loki, Prometheus, Grafana are the recommended logging and monitoring stack for logs collection, storage and visualization. However, clients are free to choose some other stack subject to that chosen stack being able to plug into Kubernetes pods generated logs.

Retention of logs and controlling access is outside the scope of iControl product deployment configuration and needs to be done within the logging stack being used by the customer.

9.2 Splunk App

iControl runs as a native Splunk application, application logs are written out to the Splunk internal index. Default retention period for Splunk Index data is 7 years, this is customer configurable.

9.3 All Versions

In addition to the system logging described above, audit logs for changes to iControl Knowledge objects for both product types are written out to an internal database table.

10 Secure Development and Compliance

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test and deliver effective and secure endpoint management solutions to our commercial and government customers.

10.1 Secure Development Lifecycle (SDLC)

HCLSoftware adheres to stringent development processes to protect the code we develop and provide to our customers.

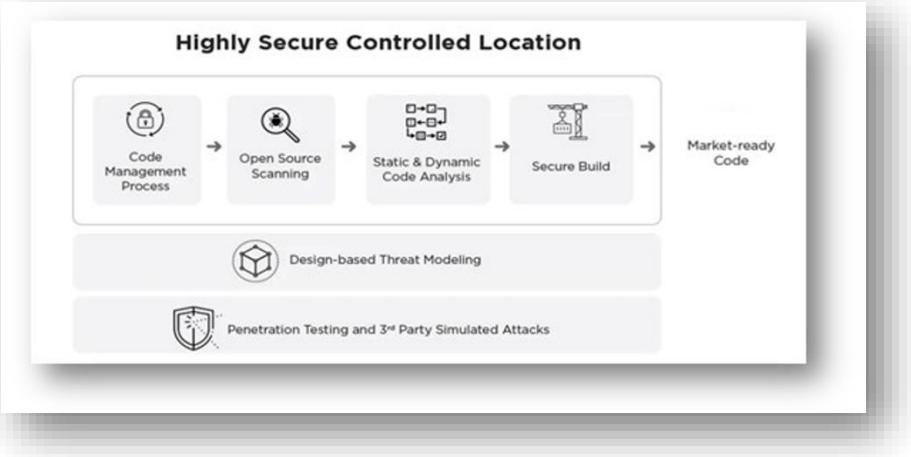

Figure 3 – Highly Secure Controlled Environment

- **Requirements & Planning**
  - **Data Privacy Assessment**: HCL's Privacy and Data Protection by Design and Default (PbD) addresses privacy requirements during design and verification phases. HCL Software uses the OneTrust Platform to perform Data Privacy assessments for products, platforms, and operations support.
  - **Quality Planning and Certification**: A Quality Planning and Certification Deck is prepared with key quality metrics and is approved by the QA Lead.
- **Design**
  - **Threat Modeling**: The process of identifying and prioritizing potential threats to a system and finding mitigation strategies.
  - **Secure Design Review**: Conducted by the HCL Software Security team to assess product architecture, deployment methods, and existing security measures based on industry standards.
- **Development**
  - **IDE-Level Code Linting**
  - **Open Source Code Composition and Vulnerability Analysis**
  - **Static and Dynamic Code Analysis**
  - **Code Quality and Code Smell Analysis**
  - **Penetration Testing**: Internal penetration testing is done for every release, and external testing is conducted annually to find vulnerabilities that attackers could exploit.

- **Maintenance**
  - **Security Bulletins & Vulnerability Management**: The HCL 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 iControl 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.
  - Regular Security Compliance runs to ensure used containers, services or configuration do not have known or newly discovered vulnerability.

11 Responsible AI Usage

11.1 AI Usage Overview

Users of iControl have an optional convenience feature to create Flows and associated Business Controls using Anthropic AI API usage. This is initiated by a user from the iControl user interface. The user choose an Industry from a pulldown, enters a textual description of the desired flow, and clicks a Generate button to generate the business process and associated KPIs template.

From this point the user may manually modify the AI-generated template, refine via AI, or accept the outcome or delete the template. iControl's template generating AI is of the human-in-the-loop type (HITL). AI is not used in the execution of live Flows; it serves only as an accelerated option to create Flows and Business Controls.

11.2 Anthropic Entitlement

The purchase of HCL iControl does not entitle the customer to Anthropic API access. If the capability is to be used, it requires a BYOL entitlement from Anthropic. For pricing see link. Consideration should be given to the relatively low consumption required to the targeted template creation activities when adding Anthropic just for iControl. Consider that an organization may create many templates manually from scratch or based on existing templates from AI or manual effort. The daily operation of iControl in production does not require this AI component.

11.3 Capabilities

As of 2025, HCL iControl only uses Anthropic APIs for process flow and accompanying business controls (key process indicators) generation and refinement.

Anthropic APIs supports many different languages. iControl only prompts the model in English (US) and the UI only supports the same.

The singular use case, template generation, and the inability of the user to directly prompt Anthropic LLM severely limits the likelihood that a user could force an abuse of the AI or allow an alternative use within the context of iControl. It is possible that a malicious user could request a flow that might be counter to the intention of the organization.

11.4 Data Privacy

11.4.1 What iControl Stores

- Stores prompt data provided by the user in a PostgreSQL database that is part of the installation.
- As of June 2025, this data is stored in perpetuity. An upcoming release of iControl will limit this lifespan.

11.4.2 What iControl Shares with Anthropic

- Your API key, BII, if using an Enterprise entitlement of Anthropic, this can be used by Anthropic to identify an organization's account and is used for billing and usage tracking.

- Your IP address is via the TCP/IP-based API call (BII). Several approaches can eliminate this:
  - Use of a Proxy Server
  - Use of a Virtual Private Network (VPN)
  - API Gateway with Lambada Authorizer (for AWS GovCloud users)
- Data is encrypted both in transit via TLS 1.2 or 1.3.

11.4.3 What Anthropic Stores

- Data stores, encrypted
  - Prompts, outputs, uploaded files
  - Usage policy violations
  - Account and organization data derived from API key
- Anthropic employees generally don't access your conversations unless you explicitly consent.
- For API users (which applies to iControl) the standard retention for inputs and outputs id deletion within 30 days.
- Depending on the type of account you purchase, e.g., commercial, there may be different data retention policies including Zero Data Retention

11.4.4 What is included in Anthropic Training

- Be default, Anthropic does not use user prompts or outputs to train generative models
- User data may be used for training if
  - conversations are flagged for Trust & Safety review,
  - users explicitly report the materials,
  - or the users opt-in to training
- Review Anthropic's Privacy Policy and Terms of Service for the most up-to-date information on their data handling practices.

11.5 Human Oversight

The implementation of Generative AI in iControl delivers a human-in-the-loop AI. All templates are generated into a Draft state. No AI generated assets are automatically put into production. Generated templates require two additional human actions to become active.

1. The generated template must be promoted to a Live state in the iControl UI.
2. Generated controls need to be manually associated with data sources before they can influence an organization.

Templates generated by AI are not guaranteed to be "fit for purpose", nor for that matter are those created without AI. It is the responsibility of the customer's process to ensure a template is fit for purpose. Users are expected to verify AI generated templates before implementation. The user can use AI to refine an existing Flow, Control or Template, including narrowing the focus of the prompt to a specific step in a Flow.

11.6 Transparency

iControl does disclose a warning when input parameters are about to be sent to Anthropic LLM via the API.

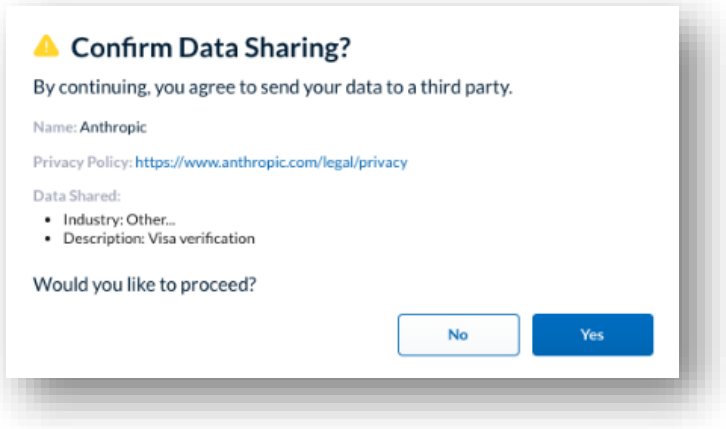

Figure 4 – AI Data Share Warning

AI generated output is not marked as such. The output generated by AI and postprocessed by iControl is presented via the user interface. Beyond the template contents (Flow, KPI, Business Controls, Steps), there is no summarization or documentation generated. All the output provided should be consumable by a trained user of the tool.

There is no mechanism to report problematic outputs from AI. If the bad output is suspected of being fouled by iControl's interpretation of AI output, you may contact HCL Support. For organizational transparency the Nominated Owner (Accountable) and Nominated Operator (Responsible) users exist with contact information in iControl user interface.

11.7 Performance

Template generation times, echoed by existing customers, are usually under one minute. Time of day can impact performance. It is extremely rare to get an inaccurate or non-reliable answer.

The AI is typically not concerned with incomplete inputs as iControl composes the input prompt and will ensure the user has provided reasonable and complete answers. In situations where the AI returns unusable output, the generation will error out and the user will be informed.

11.8 Limitations

Depending on the body of data the Anthropic LLM has been trained on, there might be industries or business process flows that have limited representation. Even in these cases, the AI should return a reasonable attempt to satisfy the prompt. It is at this point that the user (SME) may have more industry knowledge in the niche and can modify the prompting text with more context to arrive at a better generated answer or fall back to manual template creation.

11.9 Ethical Considerations

iControl does not filter potentially harmful or sensitive prompt input, it is pre-processed before submitting to Anthropic LLM for template generation.

Anthropic has been put in guardrails to ensure no harmful content is generated. This is a cat-and-mouse game of ever evolving guardrails when the guardrails are broken. For the content requested by iControl, it is difficult to imagine experiencing typical harmful content. However, it is possible that generated assets could be counter to the user's intent and harmful to the operation of the user's organization. This is where HITL becomes essential.

Sensitive content would be equally unlikely due to the limited use case for AI that is required by iControl. Anthropic APIs are instructed to assume legitimate intent, however if a user's prompt has "red flags," AI is told not to interpret them charitably.

For the iControl use case there is no assumption of "fit-for-purpose" from the AI generated assets nor the manually created assets. The assumption is the user is operating in good faith for the benefit of their organization. It is the responsibility of the customer's process to ensure the templates, flows and controls are fit for purpose. Users are expected to verify AI generated assets before implementation. The user can use AI to refine an existing Flow, Control or Template, including narrowing the focus of the prompt to a specific step in a Flow.

The bottom line for all ethical considerations is that a human is the arbiter of what is ethical and correct for their organization.

12 Conclusion

HCL is committed to providing a secure and reliable product. HCL iControl is built with security in mind, leveraging strong encryption and relying on the robust security features of the platforms it runs on. Through the shared responsibility model, a partnership between HCL and the customer ensures that the application and the data it processes are protected according to industry best practices. By following the recommendations in this document, customers can ensure a secure and compliant deployment of HCL iControl.

HCLSoftware

hcltechsw.com