IRIS Elements Platform

Information Security Assurance Statement

Document control
Version number:1.0
Owner: Tim Cropper-Williams
Date of last update: 17 April 2024
Document type:Information Security Assurance Statement
Replaces:N/A
Approved by:
Approval date:
Data protection impact screening:
Date of next formal review: April 2025

Contents

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS Accountancy, Education and HR & Payroll software by IRIS with transparency as to the security and personal data compliance of these products from all threats, whether internal or external, deliberate or accidental. Also this document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS Elements Platform

- IRIS Elements Platform is a SaaS web application, hosted with Amazon Web Services. It hosts multiple services that support the Cloud offering of IRIS Accountancy, Education, HR & Payroll, Reporting and analytics.
- If customers are also customers of the IRIS Elements Platform, customers' client and non-client data is safely and securely synchronised between the Elements cloud and IRIS Elements Platform.
- If customers are not customers of IRIS Elements Platform, customers' client and non-client data is not synchronised with any other environment.
- Personal data may be shared by clients from time to time with the IRIS Elements Platform Support team/service for software application support and product implementation.
- Personal data stored and processed by IRIS Elements Platform is sufficient for the purposes of carrying out anti-money laundering (and other regulatory) checks against customers' clients and employees where these are also clients. Practice managements, company secretarial and tax.
- Personal data stored includes, but is not limited to, name, address and contact details for individual clients and non-clients.
- Personal data is securely transmitted to a third-party (TransUnion) for the purposes of performing anti-money laundering checks.
- The postcodes of individuals are securely transmitted to a third-party (Ideal Postcodes) for the purposes of address disambiguation and completion. Data is not retained by Ideal Postcodes.
- Where a customers' client is a business, personal data pertaining to directors and other business officers may be downloaded and stored in IRIS Elements Platform.

Statement of assurance

IRIS Elements Platform will ensure that:

1 We will put in place measures to protect customer information from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
2 We will meet our regulatory and legislative requirements.
3 We will produce, maintain and test Business continuity plans.
4 We will provide information security training to all our staff
5 We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
6 We will monitor compliance with our Information Security Policy.

IRIS ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, passwords-authentication, communication and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

IRIS Elements Platform - Organisational Security

IRIS Elements Platform is part of the IRIS Software Group.

Organisational security at IRIS Group level

Data protection and information security at IRIS Software Group is controlled by the *IRIS Privacy, Security and Compliance Steering Group*. This group meets at least quarterly and includes:

- Members of the Executive Committee
- IRIS Group IT Director
- IRIS Group Data Protection Officer
- IRIS Group Compliance Manager
- Other key security leads within the company

The Privacy, Security and Compliance Steering Group approves IRIS Group level policies relating to information security and data protection, which IRIS products must comply with. There are three Group policies and a detailed Information Security Management System (ISMS). The three Group level policies are:

- IRIS Group Data Protection Policy – this sets out the roles and responsibilities for data protection compliance within the IRIS Group. It also sets out the requirement for risk assessment and data protection assessment for all projects and proposals that will change or impact on the handling or use of personal data.

- Information Security and Acceptable Use Policy Summary – this sets out the basic information security and acceptable use standards that all staff within the IRIS Group are required to adhere to.

- IRIS Personal data incident reporting and investigation procedure – this indicates the reporting and investigation procedure for all security incidents that become known or are reported to anyone within the IRIS Software Group.

The above policies are communicated to all staff and relevant external staff within the IRIS Group at least annually, using a dedicated training and policy management platform. Managers responsible for delivering IRIS products and services are required to ensure local arrangements are in place to comply with those policies and to evidence this.

- IRIS ISMS – This is the default security system for IRIS Software Group. All IRIS products must meet or be working towards meeting the standards of the IRIS ISMS except for those which already have their own certification under ISO27001 or any other standard relating to information security and data protection.

Organisational security for IRIS Elements Platform

At IRIS Elements Platform, the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering IRIS Elements Platform to ensure IRIS Elements Platform complies with the IRIS Group policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

For IRIS Elements Platform, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- Elements Product Management
- Elements Engineering
- IRIS Elements Platform Architecture
- IRIS Technical Support

The IRIS Elements Platform team keep your data secure by ensuring that appropriate measures are implemented to protect your data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to your data while being stored, transmitted, or otherwise processed by or on behalf of IRIS Elements Platform.

Measures are "appropriate" if they have been identified through risk assessment.

The IRIS Elements Platform team will ensure adequate records are created and maintained to support compliance verification and inspections and incident response (subject to any limitations set out in our Terms and Conditions).

The IRIS Group Data Protection officer is responsible for providing advice and guidance to the IRIS Elements Platform team and for monitoring our compliance on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner's Office.

The IRIS Elements Platform Dev Ops team are responsible for the operation and integrity of IRIS Elements Platform AML's IT systems and for keeping systems reasonably up to date.

IRIS Elements Platform development systems are managed by IRIS Group IT, supported by the local development team.

Asset register: Group IT and IRIS Elements Platform Dev Ops teams record and maintain a register of all assets, relevant to IRIS Elements Platform (including acquired software licences) in a fixed assets system.

Client defined classifications: Client information and materials processed, stored, or transmitted by IRIS Elements Platform shall be handled strictly in line with the customer's prior advised classification policies and standards, subject only to legal compliance.

IRIS Elements Platform human resource security

IRIS Elements Platform Dev Ops and Support staff will have controlled and restricted access to your customer's client data only for the purposes of servicing technical support requests. Records of data access are maintained by the Elements Dev Ops team.

Prior to employment

- Staff and contractors are subject to background checks and verifiable references to ensure suitability for any given job role.

- All staff are required to accept our Group Data Protection Policy, Incident Reporting Procedure and Information Security & Acceptable Use Policy.

During employment

- Corporate policies, procedures and training are administered via the IRIS KnowBe4 portal.

- A formal and communicated disciplinary process is implemented to handle IRIS Elements Platform employees who have committed a security breach. This process is owned by HR.

Termination and change of employment.

- Upon instruction from HR of a person leaving IRIS, that person's access to confidential areas shall be restricted immediately, culminating in:
- Full removal of access to any part of the corporate network
- All corporate assets in that person's possession having been returned and or been collected by the relevant Department manager or the Information asset Owner as appropriate.

In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

IRIS Elements Platform Access Control

At IRIS Elements Platform, there is a stringent password policy, Your password must:

be at least 10 characters long

have at least 1 uppercase letter

contain at least one number

not contain any invalid characters (such as " or £)

Which is enforced through the software. The password can be changed as regularly as the users internal staff policy dictates, via the password settings page found in the users profile section.

Change your IRIS Elements Platform password (help-iris.co.uk)

At IRIS Elements Platform, MFA is available for all users to use at their own discretion. The software can mandate MFA enrolment on given user journeys where there is a requirement set by 3rd party integrations. However is does not mandate by default.

Turning on multi-factor authentication (help-iris.co.uk)

At IRIS Elements Platform, Role Based Access controls are in place and are enforced on all users that use IRIS Elements Platform. The RBAC service allows users to control what features users can access from a basic level of access to full administrative control. Invited users on to the platform are given the least privileged role until their permissions are adjusted by the system administrator.

Roles and permissions (help-iris.co.uk)

Support can currently only direct the customer by giving instructions on where to go and how to locate the correct user that can elevate a user's permissions by assigning another role. Support does not have a method to do this on behalf of the customer.

Customer can make changes to user roles if they have the required role that allows them to modify a users role. Where an action is not permitted by the restrictions placed on the user by RBAC controls the user is notified with a hover over tool tip that informs them that they do not have access to this feature and that it should be requested if needed from the system administrator. An audit log is retained, capturing:

- The tenant id
- The id of the user that made the change
- The id of the user that had the change applied to them
- The date and time the change occurred (in UTC as per usual)
- Whether the action was to assign or remove a role
- The role name involved
- The IP number the user used

The audit trail extends to all user on Elements regardless of privilege level.

Support does not have the ability to modify user permissions.

For the avoidance of doubt, IRIS Elements Platform warrants to Clients that it will not seek to circumvent, compromise or change the Client's security controls, and IRIS Elements Platform will not change the Client's software configurations (without proper authorisation); and no 'back door' password or other method of remote access into IRIS Elements Platform's software shall exist.

Encryption (cryptology)

- Client to server connections, and internal communication between services is over TLS. Data at rest is encrypted according to Amazon guidelines.:
  https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
  https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html

IRIS Elements Platform physical and environmental security

IRIS does not maintain physical servers or other infrastructure for any IRIS Elements Platform product. All infrastructure is hosted by Amazon AWS, and as such, IRIS Elements Platform inherits the physical and environmental controls implemented by Amazon.

Details may be found on the Amazon AWS website: https://aws.amazon.com/security/

Access to IRIS resources and equipment is subject to Group IT Policies.

Operations security

Environmental and application monitors and alerts are in place and are documented here:
https://ngiris.atlassian.net/wiki/spaces/IELMHP/pages/2071233248/Monitoring+and+Alerting

Datadog is the services used to monitor the state of the system and AWS autoscaling and serverless frameworks are used to ensure we can meet future capacity requirements. We also use Snyk and SonarQube for security and source quality scanning in the CI/CD pipelines. SLA's are in place for critical and high vulnerabilities.

Elements is deployed across four isolated environments – Development, Testing, Staging and Production, each running on a different AWS account. All networks are separate and organized around subnets:
https://ngiris.atlassian.net/wiki/spaces/IELMHP/pages/2885779617/06+Deployment+View
https://ngiris.atlassian.net/wiki/spaces/IELMHP/pages/2506589038/Target+Deployment+View

Security Groups (SGs) and Network Access Control List (NACLs) prevent access to AWS resources on an IP level, protecting from unauthorised access.

All Elements data and infrastructure is hosted on AWS. RDS instances are configured to create automated daily backups that are stored for 7 days. The backups are stored in AWS.

Application and infrastructure logs are aggregated in AWS CloudWatch:

https://ngiris.atlassian.net/wiki/spaces/IELMHP/pages/2614428534/Logging+-+services+log+aggregation+in+CloudWatch.

Logs are retained in CloudWatch for 90 days and then migrated to S3 for warm storage for 1 year.

After one year all logs are moved to S3 Glacier for 3 years.

AWS CloudTrail is used for logging of the AWS account activity - https://aws.amazon.com/cloudtrail

Only nominated administrative accounts have non-read-only permissions to CloudWatch, S3 logs storage accounts and CloudTrail.

All server clocks are configured to synchronize time to UTC using authoritative Internet time servers.

Automated security vulnerability scanning is integrated in the CI/CD pipelines of the application. Veracode, SonarCloud and Trivy are in place to facilitate this scanning. All identified vulnerabilities are analysed, and fixes and mitigations are prioritized depending on the criticality of the vulnerability.

Code with critical vulnerabilities blocked from deployment.

Communications security

Security groups and network access control lists are used to control the access to all Elements networks:

https://ngiris.atlassian.net/wiki/spaces/IELMHP/pages/2947088608/Security+Groups.

VPN connection and SSH tunnelling is required to access to some special network segments – networks with RDS stores, control servers, etc.

Elements application networks are segregated by subnets. There are public and private subnets, subnets for compute instances and lambda and data storage. See https://ngiris.atlassian.net/wiki/spaces/IELMHP/pages/2885779617/06+Deployment+View

Summary of Sub-processors

Sub-processor	Purpose
Amazon Web Services (AWS)	Hosting, storage and all other associated services with running the platform
Cybage	India based development organisation (see page 12 "Supplier Relations" for more detail
Okta	Identity and authentication provider. Used to enable users to log into the Elements Platform. Storage and management of usernames, passwords and MFA. Okta security statement
App Direct	Used as the IRIS Marketplace to enable IRIS users to browse and purchase IRIS software digitally. App Direct security statement

System acquisition, development, and maintenance

Information security requirements analysis and specification - Before features are developed, or changed, an Architecture Review Board reviews and approves the technical architecture being proposed. If changes are required these are fed back to the teams. This process includes a full security review including, but not limited to attack surface & vector analysis and encryption requirements.

Securing application services on public networks – All data transfer within the Elements application infrastructure is secured and encrypted using the latest industry accepted standards. Similarly, all access to the Elements platform across public networks is secured and encrypted using the latest industry accepted standards.

Security in development and support processes

Secure development policy

IRIS' Secure SDLC (Software Development Life Cycle) is based on the Microsoft Secure Development Lifecycle. The framework is designed to lead IRIS development teams through the phases of a software change, indicating the various artefacts that should be produced and quality gates that should be met to ensure the software is high-quality and secure.

System change control procedures

We have an Architecture Review Board where major changes are documented, reviewed and decided upon to ensure the solution meet our Architectural principles. We also have a Change Advisory Board that reviews major changes prior to them being deployed into Production environments to ensure the right quality processes have been applied and we can support the changes effectively.

Technical review of applications after operating platform changes

Changes are made programmatically to lower environments first where we test changes before applying them with the same code to Production environments.

Restrictions on changes to software packages

Changes to our software are controlled through the Product backlog under the stewardship of the Product Owner. All changes are prioritised by the Product Owner and approved by them before deployment into the Production environment.

Secure system engineering principles

Our Architectural principles place heavy emphasis on security and we bake security into our engineering delivery practices. We use tooling for detecting security issues early and have gates to prevent security risks entering our environments.

All work is carried following the same processes, using the same tooling, and adhering to the same principles. The architecture and operating environments are standard IRIS Elements Platforms for all teams, internal or external.

We have a test strategy that covers all types of testing and defines the tools we use. Security testing forms part of this and we have tooling in place that runs security tests in the delivery pipelines.

System acceptance testing

All changes go through acceptance testing with our Product Owners and other key stakeholders. We also employ a feature toggling capability so new applications and features are tested in Production per tenant before we switch on for the larger customer base.

Test data

Protection of test data

Test data is typically created in house by the QA teams and our development teams do not have access to customer data. Customer sourced data may be used if the need arises but this is only available after a data access request has been submitted to our Operations team and the data obfuscated before being passed to the testers. Any copies of the data will be destroyed as soon as they are no longer needed.

Processing locations and international data transfers

On occasion, IRIS may use engineers and third parties located in India and Romania for production environment support, deployment activities, access management and security & vulnerability management. In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it. All relevant security requirements have been addressed and further information is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

Supplementary measures for personal data processed in India

IRIS and its engineers in India adhere to the standards of ISO 27001 and uses privileged access management controls to audit activity of engineers. VPNs and Bastions are used where appropriate and all communications are over encrypted channels. IRIS has an international data transfer agreement in place with all sub-processors used that are based in India. This requires them to comply with IRIS data protection and security policies and standards, particularly in relation to handling requests from official sources.

Supplier relationships

Development, bug fixing and enhancements to the IRIS Elements Platform product are sometimes carried out by a team in Cybage. All Cybage employees have the same checks and follow the same compliance procedures as FTE employees. Any customer data shared with Cybage for purpose of bug fixing is scrambled unless specific authorisation from the customer is attained first.

Supplier service delivery management

Managing changes to supplier services –If a new supplier needs to be selected for any reason, IRIS follows a Supplier due diligence process which assesses any potential supplier data protection and security arrangements.

Information security incident management

Management of information security incidents and improvements

In all instances, any IRIS Elements Platform critical incidents (whether relating to information security or not) are managed through the "Critical Incident Management Process", handled, and coordinated by the IRIS Critical Incident Manager. Incidents are prioritised and classified as part of this process. The process outlines stakeholder communication with a focus on customer communication during an incident resolution. A post incident review is then drawn up by the software manager and / or product manager and corrective actions are logged and tracked to execution.

Information security incidents must follow this process, but in addition will be triaged by the Group Data Protection Officer. The IRIS Group Data Protection Officer will report a summary of all data protection incidents to the IRIS Information & Security Governance Group and maintain a list of learning outcomes and actions arising from incidents with the aim of ensuring Information Asset Owners follow through on those actions. This process will also be used internally for any issues discovered during development, and training is provided for staff to promote awareness of this process.

Business continuity – Information security aspects

Information security continuity

No business-critical data is held on IRIS servers for IRIS Elements Platform applications. See appropriate documentation for our hosted service.

For application updates including legislation changes, code configuration is controlled within version control. In the highly unlikely event of disaster recovery being required, environments can be created through recreating replicable stored environments.

Data Protection – quick reference

IRIS Group Data Protection Officer – *Vincenzo Ardilio* - dataprotection@iris.co.uk

Data protection owner for IRIS Elements Platform – *Jenny Strudwick – jenny.strudwick@iris.co.uk*

Location of personal data processing

All customer data is held on local customer machines. For any customer data collected by support or engineering, it is held in the UK.

Retention of data

We will retain records of our dealings with our customers in line with our legal and taxation record-keeping obligations, such as details of invoices and payment details. The information we retain is reviewed regularly in line with our retention policies and removed at the earliest opportunity.

Data subject rights

Customers have a right to access personal data held by IRIS. Customers should direct their request to access data to the Support desk.

Right to Accuracy, Rectification and Erasure (Right to be Forgotten)

Data protection law imposes obligations on users to ensure the accuracy of the personal data that is processed, and it must be kept up to date where necessary.

Data Accuracy

IRIS Elements Platform allows the self-service of data accuracy.

- A single client record for each client within IRIS Elements Platform eliminates the need to duplicate data entry and improves data accuracy.
- IRIS Elements Platform is enhanced throughout the year to ensure that the legislative compliance and validation rules are up to date.
- Online filing validation is carried out within IRIS Elements Platform before submission to Companies House / HMRC, reducing the risk of the Accounts / Tax Return being rejected.
- Pre-population of client data made available via Making Tax Digital (MTD) can be imported directly into the return.
- Data can be rectified and resubmitted to Companies House and HMRC (within the limits of what is defined / regulated by Companies House and HMRC). To rectify information with either government body, it is recommended you consult with them on their processes around rectification of any data submitted and accepted by them.

Data Deletion

IRIS Elements Platform allows the self-service of data deletion.

- User profiles
- Customers
- Data within a customer (accounts, tax returns, tax notes)