egress

How the Egress Platform can assist ISO 27001:2013 compliance

Product Alignment

April 2020

Contents

How the Egress Platform can assist ISO 27001:2013 compliance

The Egress Platform can be used, along with appropriate documented policies and procedures, to assist organisations in achieving their goal of compliance with the ISO 27001:2013 standard for an Information Security Management System.

Below is a table of the ISO 27001 Annex A controls and how the Egress Platform can aid compliance with those controls.

A.8 – Asset Management

A.8.2 – Information Classification

A.8.2 – Information Classification	
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation. The Egress platform is relevant to the following controls: • **A.8.2.1: Classification of information** ○ *Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.* • **A.8.2.2: Labelling of information** ○ *An appropriate set of procedures or information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.* • **A.8.2.3: Handling of assets** ○ *Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.*	**Egress Protect** and **Egress Prevent** enables administrators to configure a relevant digital information classification scheme for their organisation, dependant on the legal requirements, value, criticality and sensitivity of that information. Users can use **Egress Protect** and **Egress Prevent** swiftly and easily classify their documentation, mail and other unstructured data, with labels, overlays, watermarks and metadata, in accordance with the information classification scheme that the administrator has configured for the organisation. If **Egress Protect** and **Egress Prevent** is used in correlation with appropriate documentation, then the ISO 27001:2013 A.8.2 controls can be reached, and compliance with this control achieved.

A.8.3 – Media Handling

A.8.3 – Media Handling	
Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media. The Egress platform is relevant to the following controls: • **A.8.3.1: Management of Removable Media** ○ *Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.* • **A.8.3.3: Physical Media Transfer**	A feature of **Egress Protect** and **Egress Prevent** which aids compliance with A.8.3.3, is the ability to create encrypted packages on removable media, for example writing to USB sticks and burning onto disks. The software ensures confidentiality and integrity of information whilst being transported through this vector, via encryption, as well as access control to prevent unauthorised access, and audit logs of access and usage to combat misuse or corruption.

○ *Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.*	Information on removable media can also be classified using **Egress Protect** and **Egress Prevent**, which, along with appropriate procedures by the customer organisation, can achieve compliance with the A.8.3.1 control also.

A.9 – Access Control

A.9.1 – Business Requirements of Access Control

A.9.1 – Business Requirements of Access Control	
Objective: To limit access to information and information processing facilities. The Egress platform is relevant to the following controls: • **A.9.1.2: Access to Network and Network Services** ○ *Users shall only be provided with access to the network and network services that they have specifically authorised to use.*	The **Egress platform** is compatible with ADFS login which allows for role-based access control for Egress accounts (and other software). Additionally, **Egress Secure Workspace** is a cloud-hosted secure solution to file management and storage. Users can create document 'Zones' to store projects, create and edit files within them. They can then share those Zones with varying permission settings, providing appropriate access to their peers whilst still having control over potentially sensitive information, thereby aiding compliance with the control.

A.9.4 – System and Application Access Control

A.9.4 – System and Application Access Control	
Objective: To prevent unauthorised access to systems and applications. The Egress platform is relevant to the following controls: • **A.9.4.1: Information Access Restriction** ○ *Access to information and application system functions shall be restricted in accordance with the access control policy.*	One of the main reasons for using **Egress Protect** is to ensure that access to information is restricted to only those who require it. **Egress Protect** encrypts emails and files into Egress packages so that when emails are sent, they can still be controlled by the sender (package owner) to restrict access in accordance with policy, even if an email or file has been sent to individual(s) who should not have access. **Egress Secure Workspace** also aids compliance with the control, alongside appropriate documentation, as it can be used to segregate organisation users from company information that they should not have access to, without preventing users from collaborating on or sharing information and data that requires sharing.

A.10 – Cryptography

A.10.1 – Cryptographic Controls	
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. The Egress platform is relevant to the following controls: • **A.10.1.1: Policy on the use of Cryptographic Controls** ○ *A policy on the use of cryptographic controls for protection of information shall be developed and implemented.*	**Egress Protect** and **Egress Secure Workspace** are both 'cryptographic control' solutions which allow customers to enforce a higher level of security through cryptography, therefore, along with appropriate policy documentation, they can be used to aid in compliance with A.10. Both solutions can be used to secure files and unstructured data (as well as the information that are contained within these) in order to protect confidentiality and integrity.

A.12 Operational Security

A.12.2 – Protection from Malware

A.12.2 – Protection from Malware	
Objective: To ensure that information and information processing facilities are protected against malware. The Egress platform is relevant to the following controls: • **A.12.2.1: Controls against malware** ○ *Detection, prevention and recovery controls to protect against malware shall be implemented, combined with user awareness.*	As a file management system, **Egress Secure Workspace** provides a multitude of security features which benefits end users. Features such as automatically scanning all uploaded content for anything malicious; white and blacklist-filtering of uploaded content which is done by inspecting file content not just the extension or filename; preventing macros from running when using both the Egress and Microsoft Office online editors; and segregating files away from user devices all help to avoid any malware infections that can be transferred through files.

A.12.4 – Logging and Monitoring

A.12.4 – Logging and Monitoring	
Objective: To record events and generate evidence. The Egress platform is relevant to the following controls: • **A.12.4.1: Event Logging** ○ *Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.*	The **Egress platform** is designed with event logging in mind. When packages are created with **Egress Protect**, every single access attempt that is made to the package (successful or unsuccessful) is logged and can be viewed using the application, thereby complying with the control when coupled with regular review. **Egress Secure Workspace** also has event logging; the event logging shows the different users who have accessed content within **Egress Secure Workspace**, as well as whether they have edited any content and, if so, what editor they used to do so.

	Egress Investigate allows even deeper review of user event logs. It shows user email activity and can then also highlight the types of information that users are sending, how they are sending it, who they are sending it to and whether they are operating against business policy.

A.13 – Communications Security

A.13.2 – Information Transfer	
Objective: To maintain the security of information transferred within an organisation and with any external entity. The Egress platform is relevant to the following controls: • **A.13.2.3: Electronic Messaging** ○ *Information involved in electronic messaging shall be appropriately protected.*	Egress' flagship product**, Egress Protect**, allows users to have control of their emails even after they are sent, granting assurance and protection. Emails, depending on their classification (chosen by the user), are encrypted over a TLS connection with an RSA 2048 bit (SHA256 with RSA) certificate and sent to the recipient in the form of an Egress '.switch' package, which the sender has full control of. They can remotely revoke access, allow others to access packages, as well as see who has and has not tried to access the packages.

A.14 – System Acquisition, Development and Maintenance

A.14.1 – Security Requirements of Information Systems	
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. The Egress platform is relevant to the following controls: • **A.14.1.2: Securing Application Services on Public Networks** ○ *Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.*	**Egress Protect** will secure information contained within Egress '.switch' packages as they make their way to their destination across the internet (a public network). The encryption that Egress packages are secured with will protect the mail and file content from fraudulent activity as well as from unauthorised disclosure (using audit logging and the ability to change package access) and modification (unique package IDs and using audit logging). **Egress Secure Workspace** provides a secure service for users to work and collaborate on documents and files over the internet (a public network). The information sent between the user and the **Egress Secure Workspace** is encrypted.

A.18 – Compliance

A.18.1 – Compliance with Legal and Contractual Requirements	
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. The Egress platform is relevant to the following controls: • **A.18.1.3: Protection of records.** ○ *Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislator, regulatory, contractual and business requirements.* • **A.18.1.4: Privacy and Protection of Personally Identifiable Information** *Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.*	**Egress Protect** can help meet some of the compliance requirements of ISO 27001:2013 by ensuring that data is protected while at rest and in transit. This means information is appropriately secured, integrity maintained and only accessible to authorised personnel. Additionally, when **Egress Protect** used in conjunction with **Egress Prevent**, they can help to prevent unauthorised access and unauthorised release of information by alerting the user of any conflicts. For example, A spreadsheet which has been classified as “Internal” would raise a warning message if a user was attempting to send it to an external recipient.

Egress Software Technologies Ltd

Egress provides human layer security – helping users receive, manage and share sensitive data to meet compliance requirements and drive business productivity.

Egress' award-winning platform makes sure emails and files are delivered to the correct recipient, encrypts and protects sensitive data, and provides compliance auditing and reporting.

www.egress.com

✉ info@egress.com

☎ 0844 800 0172

@EgressSoftware

egress