Autolomous Information Security Brochure

Document owner	Compliance Team
On this page	

Overview

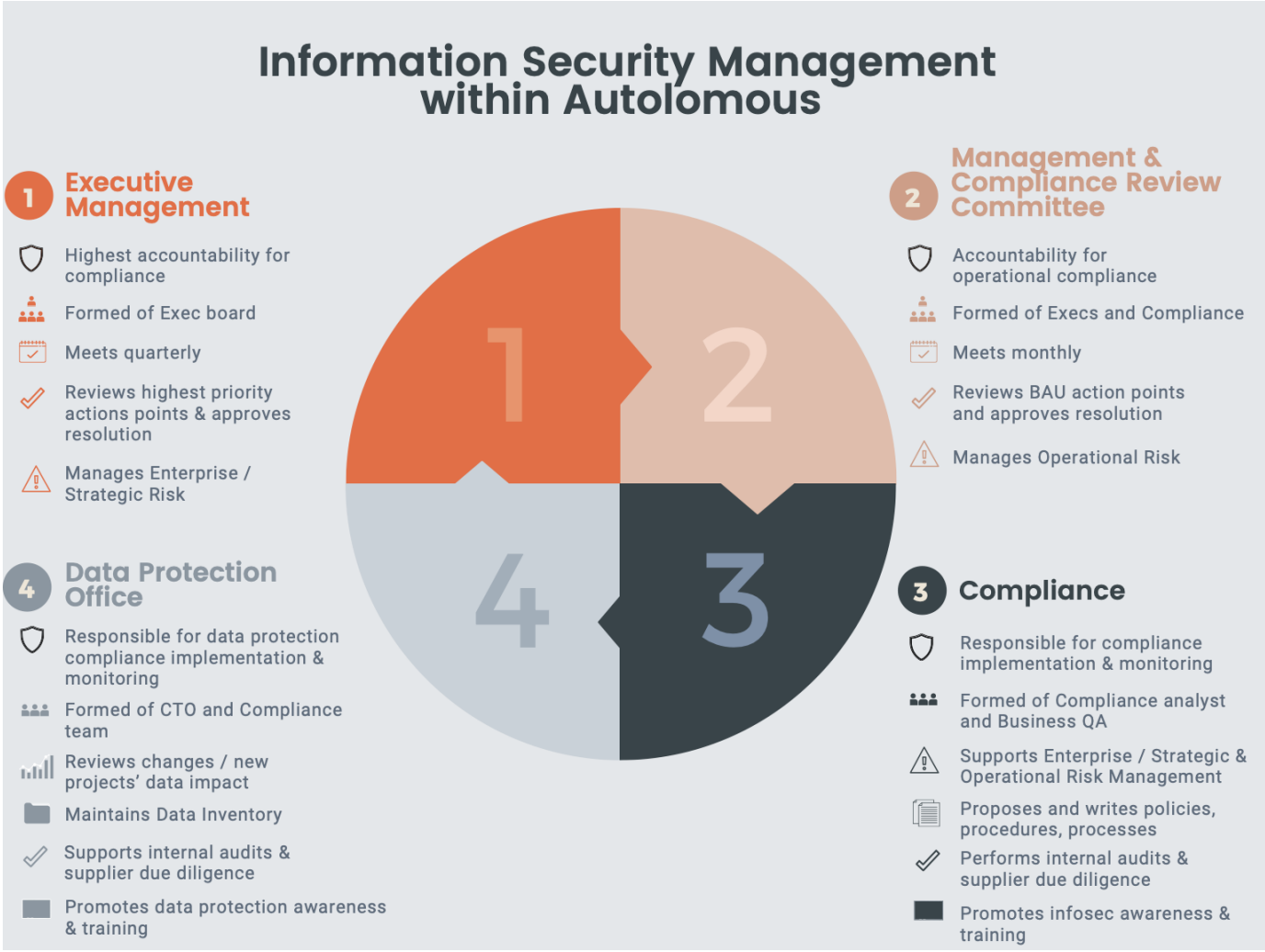
1. Information Security in Autolomous

Autolomous utilises a blend of people, processes, and technology along with a proven development methodology to build an information security programme that protects our organisation's assets and those of our customers.

Our information security management system (ISMS) has been certified against the ISO 27001:2013 standard. ISO 27001 is a framework of policies, processes, and controls used to manage information security in a structured, systematic manner

Autolomous is a Cyber Essentials certified organisation, thus reiterating our commitment to data protection and cyber security.

Certificate
No:369092021



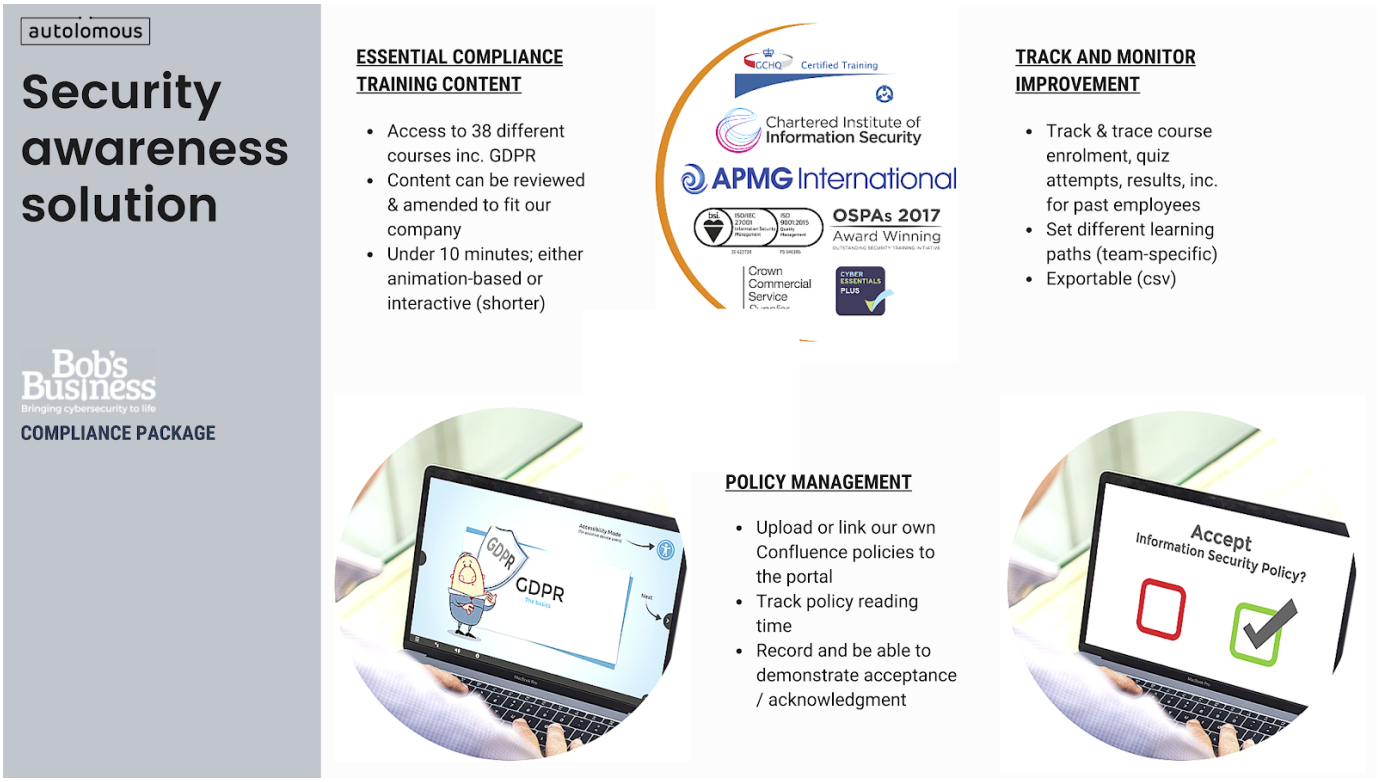
1.1 Programme foundation

As foundational components, we have devised a **policy set** aimed at outlining how to protect the organisation from threats, including computer security threats, and how to handle situations when they do occur, along with supporting processes and frameworks.

Executive Management has the ultimate responsibility for information security within Autolomous. Operational responsibility for information security is delegated to the **Compliance team**, which works to the standards set out in this framework, and the risk assessments agreed by the Executive Management. Within teams, accountability for security rests with team leads / managers.

In regards to **personal and sensitive data**, while our processing of such information is extremely limited, we are committed to maintaining the privacy and security of the data we hold. We actively monitor our compliance against the EU GDPR and the UK Data Protection Act 2018, and have appointed an internal team to oversee this - the Data Protection Office. Detailed roles and responsibilities are defined in Autolomous' Global Data Protection Policy. All types of data processed, alongside protective measures and lawful basis are monitored through our internal Data Inventory. It is important to note that any personal data that is to be recorded in our AutoloMATE eBMR configurations is encrypted.

Our **Security Awareness Programme** consists of monthly e-learning courses, complementary learning tools such as security articles, and the dissipation of relevant security policies and procedures. We also have an integrated QMS-ISMS portal where all employees can search for documentation and an internal communications channel where questions can be raised to the Compliance team. All new joiners go through a Compliance induction session.



1.2 Technical controls

In terms of technical controls, we have focused our efforts on access and vulnerability management and robust security architecture.

1.2.1 Application security

Autolomous' internal application development is supported by guidance during the systems development life cycle (SDLC) and by following base security principles, including confidentiality, integrity, and availability. Our development is reviewed and evaluated in accordance with best practices.

1.2.2 Third-party security

Autolomous suppliers are selected based on the quality services and security guarantees provided and must be aligned with our own standards and vision. Our suppliers are to be periodically assessed and monitored according to quality and information security expectations; upon entering any agreement, we will share with third parties our Supplier Security Requirements Policy which they must acknowledge and adhere to.

1.2.3 Infrastructure security

Autolomous' core systems and applications are hosted in several secure and certified data centres across the globe. Client deployments will be hosted at data centres in specified regions in line with the client's location and managed in accordance with local regulations. These data centres are layered with operational and security controls, ISO/IEC 27001 certified and not only - among the other certifications included are ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27018, SOC 1/2/3, PCI / DSS and HITRUST CSF.

The AutoloMATE backend is mostly composed of Google Firebase Services. The Google Firebase Services employed are using a Google Cloud Platform project that encompasses the initial configuration, security, and setup of the Google Firebase project, including authentication, database, storage, and hosting. More details on the provider's certifications can be found here https://cloud.google.com/security/compliance.

The AutoloMATE platform uses blockchain to immutably store data and ensure provenance; this is hosted on the Amazon Quantum Ledger Database (AWS QLDB), which offers service with 99.9% SLA with enhanced security, built-in high availability and embedded ledger backups for continuous operations.

1.2.4 Incident management

Autolomous' Security Incident Response Team (SIRT) responds and proactively monitors information security incidents. High-level guidelines have been defined in the Information Security Incident Response (IS IR) Policy. Incidents can be reported to us either via email - compliance@autolomous.com, or via our internal QMS-ISMS portal, hosted on Confluence (Atlassian tool).

2. Why AutoloMATE is a secure solution

Security is paramount to Autolomous and we aim to use best in class account security practices where this is practically possible.

2.1 Passwords

To this end, we have implemented a password security system that is practical, secure, and future-proof. Autolomous aligns its password security measures with Google's 'Modern Password Security for System Designers' whitepaper, as well as established scholarship in data system security.

Autolomous uses a passphrase system that requires users to define a phrase of any length but with minimum requirements for the number of words and total character length - good passphrases are generally easier to remember than complex passwords.

The system enforces passphrase strength based on two measures:

1. The number of words in the passphrase (X)
2. The number of characters in total in the passphrase (Y)

These values are configurable by administrators but Autolomous strongly recommends against values lower than the defaults.

2.2 Two-factor authentication

The app supports two-factor authentication (2FA), configurable at either platform or individual account level. The 2FA is email-based, in order to work with clean room environments where computers are shared and mobile phones are disallowed.

2.3 Enforced timeout

Users are automatically logged out of the application after a period of inactivity as and if configured in the customer configuration.

2.4 Encryption

Personal or sensitive data in eBMRs can be encrypted using the secured AES-256 encryption standard. This is configurable at the field level. All data is encrypted at rest and in transit. For web browsers, we enforce the use of TLS 1.3.

2.5 Audit trail

Our platform uses distributed ledger technology to immutably store data and ensure provenance. As such, our solution allows users to access a reliable, complete, and searchable audit log of all events in a product eBMR. Quality Assurance personnel can regularly review and approve product eBMR audit logs. A system audit functionality is available to our clients' system administrators providing an overall useful tool for investigative and record-keeping purposes.

2.6 e-Signatures

Users are required to sign using a unique 6-digit passcode generated by the platform.

2.7 Segregated user permissions

Roles can be defined by the customer and permissions enabled / disabled per role.

2.8 Secure exports

No possibility to email content from the app, only to export on the device. Note that emails sent are enforced with TLS encryption (TLS 1.3).

2.9 Regular pen-testing

Regular penetration testing is conducted for the AutoloMATE platform. This is done on an annual basis, unless major upgrades / infrastructure changes occur and justify earlier testing.