

Data in Transit

Please provide evidence of how data is managed in transit

Axon maintains controls to protect and monitor boundaries of Evidence.com. These include firewalls, network segmentation, proxies, and intrusion detection systems. Evidence data transiting networks is [redacted] or stronger keys. [redacted] Additionally, [redacted] is enabled. Axon maintains policies and practices for Evidence.com for encryption key and certificate management.

Asset Protection & Resilience

Please provide evidence of how the assets are protected and made resilient

Axon Evidence.com data centres are located [redacted]. Customer data is not stored outside of the UK. Axon commits in contract that data will not be stored outside the UK. Axon Evidence.com data centres provide world-class physical protections and are ISO 27001 certified. When hard disks are taken out of service they are demagnetised and destroyed on site. Additionally, Axon Evidence.com is deployed in [redacted] to provide high levels of availability. This availability is backed by the Axon Evidence.com Service Level Agreement (SLA).

Segregation

Please evidence how data is segregated between consumers of the cloud environment

Axon Evidence.com customers are logically separated at the application layer. The application and underlying infrastructure undergo at least [redacted] that include in scope the separation between consumers. One of the [redacted]

Governance Framework

Please provide evidence that you align to a Governance Framework ISO27001 etc

Axon Evidence.com Is ISO 27001 certified by a United Kingdom Accreditation Service (UKAS) recognized audit body. The Vice President of Information Security coordinates the information security governance program.

Operational Security

Please provide evidence that you carry out operational security i.e. protective monitoring, incident reporting, notifications, audit

Configuration and change management, vulnerability management, protective monitoring, and incident management are demonstrated by Axon Evidence.com's compliance with the ISO 27001 information security standard. Additional detail can be reviewed in Axon's Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) response:

Personnel Security

Please provide evidence and assurance that you have carried out the necessary BPSS checks or will carry out NPPV

Axon personnel do not have access to a customer's evidence data without the explicit authorization from the customer. The only exception to this is for a small team of administrators who would only access evidence data in the event of a system emergency. All Axon personnel that may encounter customer evidence data as part of their job responsibilities are subject to the appropriate local adjudication processes. Many personnel have completed the UK BPSS or are SC cleared. Contractors are subject to the same personnel security screening and security education as Axon personnel. Axon conducts security education training on at least an annual basis. Additional security education training for personnel is align to job responsibilities.

Secure Development

Axon includes security as part of the product development process and ongoing application maintenance. This is demonstrated by the ISO 27001 certification and technically validated during the periodic penetration tests against Axon Evidence.com. Additional detail can be reviewed in

Supply Chain Security

Please provide assurance of any third party suppliers involved in this contract

Axon leverages Infrastructure as a Service providers to deliver the Evidence.com service. Service providers must be at least ISO 27001 certified and maintain their own OFFICIAL Accreditation. Axon periodically reviews the security practices of the infrastructure providers to ensure Axon's security expectations are met.

Secure Consumer Management

Please provide assurances of user access controls, rights, privileges and access to the cloud, who manages and controls these access rights

Within Axon Evidence.com, a force maintains full control over the administration and provisioning of user accounts within the service. Role-based access control can be utilized to define roles and permissions to evidence data and features of the service.

Identity and authentication

Axon Evidence.com allows for forces to securely manage their usage of the service commensurate with their security risk profile. Features of Evidence.com include: Customizable password length and complex password requirements Customizable failed login limit and lockout duration Enforced session timeout settings Mandatory challenge questions when authenticating from new locations Multi-factor authentication options for user login and prior to administrative actions Role-based permission management Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) Restrict access to defined IP ranges (limit access to approved office locations) Integration with a force's identity service for single sign-on capabilities.

External interface assurance

Please provide assurance and evidence of the protection of your external interfaces

The Axon Evidence.com application and underlying infrastructure undergo at least [REDACTED] One of the [REDACTED]

Secure Service Administration

Please provide assurances around your service administration processes and procedures

Axon administers the Axon Evidence.com service through secure interfaces that require at least [REDACTED] for authentication. The administrative interfaces are included in scope for the ISO 27001 certification. End-user devices used to manage the service are managed and controlled by Axon and configured with a hardened OS, an anti-malware solution and full disk encryption.

Audit information provision to consumers

Please provide assurances around your audit information

Axon Evidence.com maintains and provides to forces tamper-proof evidence audit records that log the when, who, and what for each evidence file. These records cannot be edited or changed, even by account administrators. User activity logging is available within the service to monitor users actions and authentication activity. Additionally, the service includes evidence deletion protection to monitor and recover evidence that may have been accidentally deleted. These deletion protection features include deletion approval workflows, deletions notification emails, and a deletion remorse period.

Secure use of the service by the consumer

Please provide evidence on how you support the consumer in using the cloud platform and measures to ensure secure use.

Axon Evidence.com provides detail of the security implications when using the service with the Evidence.com Service RMADS. Axon Evidence.com has many guides available to customers to educate and assist in administrating the service in a safe and secure manner. Additionally, Axon has a professional services and customer support team that can provide onsite or remote assistance related to the Axon Evidence.com service.