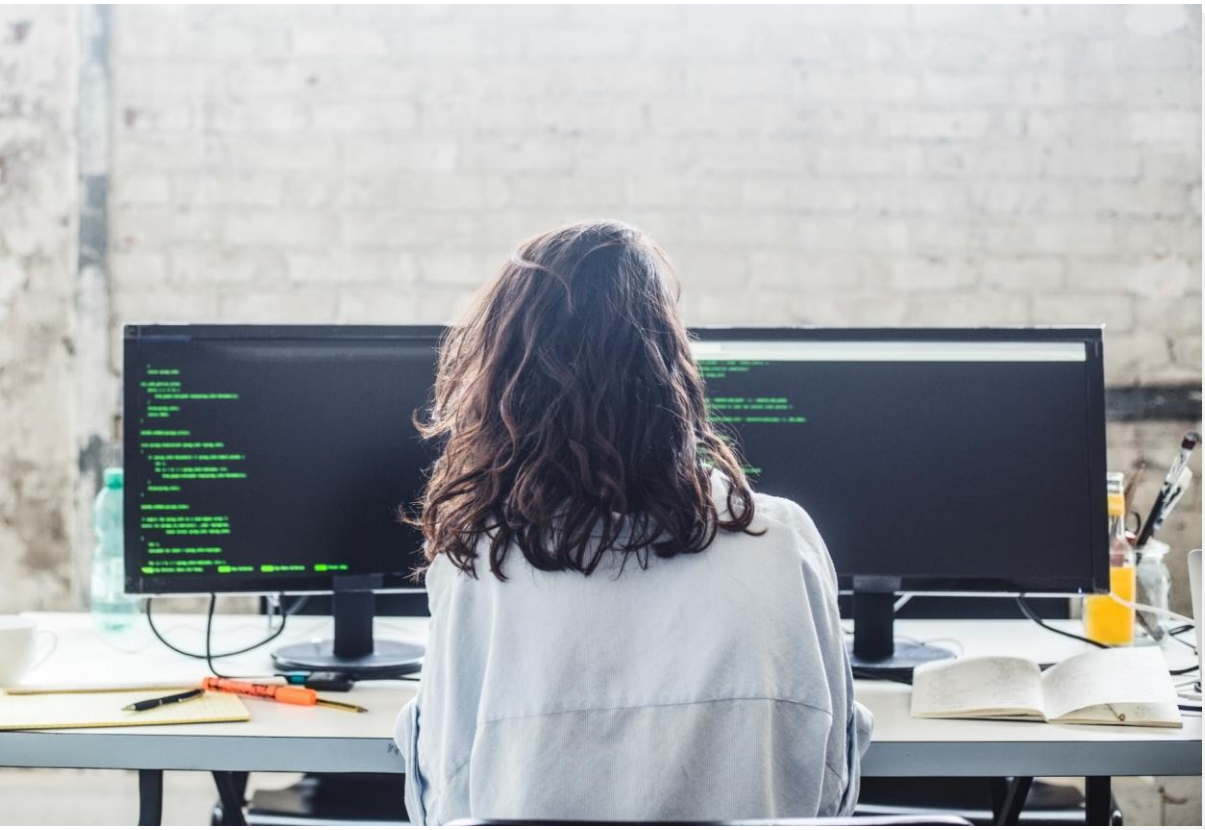


Information Security – FAQ's

Published Date: 24/01/2022

Version: 55.121

This electronic document supersedes all previous electronic and printed documents or oral statements regarding this policy. All company Standards are subject to change at the sole discretion of FISCAL management.

Prepared for:
Employees
Contractors
Partners and Customers

FISCAL TECHNOLOGIES

1. CONFIDENTIALITY

This document is the property of FISCAL Technologies. It may not be copied, distributed, or recorded on any electronic or other medium without the express written permission of the company.

All material contained in this document which is not readily available in the public domain is regarded as confidential to FISCAL Technologies and may not be divulged to any other parties without the express written permission of FISCAL Technologies.

2. PURPOSE

FISCAL Technologies is the leading provider of Supplier Risk Intelligence that provides finance teams with the controls and insights to continuously protect the bottom line. Our solutions have been designed in partnership with finance teams to empower them to eliminate supplier risk.

FISCAL Technologies handles key customer information to allow our software to provide reassuring, preventative solutions using Artificial Intelligence and advanced forensics to prevent errors and identify key risks.

Our software aims to improve the financial operational performance of the organisation by automatically and continuously analysing payments data (typically invoices and credit notes) prior to payment to determine the risk of error and/or fraud and for reporting compliance to payments processes; and automatically and continuously analysing the Master Supplier File for opportunities to reduce the risk of error and/or fraud caused by duplicated supplier records, supplier records that are not actively being used or changes.

This document lists details of the most commonly asked information security questions relating to FISCAL Technologies and our SaaS solutions.

Contents

3. COMPANY INFORMATION

3.1 BUSINESS ADDRESSES

EMEA Headquarters	North America Headquarters
FISCAL Technologies Ltd	FISCAL Technologies, Inc.
448 Basingstoke Road	One Copley Parkway, Suite #100
Reading, RG2 0LP	Morrisville, NC 27560
United Kingdom	United States

3.2 COMPANIES HOUSE REGISTRATION

FISCAL TECHNOLOGIES LTD.

Company number: 04801836

3.3 VAT REGISTRATION DETAILS

FISCAL Technologies Ltd is a VAT registered company.

UK VAT number: 815382334 or GB815382334

Registered business name: FISCAL TECHNOLOGIES LTD

3.4 ICO REGISTRATION DETAILS

ICO Registration Number: ZA115827

4. FISCAL'S PRODUCTS

4.1 NXG FORENSICS

4.1.1 Product Summary

The FISCAL NXG Forensics Software Service aims to improve the financial operational performance of the organisation by:

Automatically and continuously analysing payments data (typically invoices and credit notes) prior to payment to determine the risk of error and/or fraud and for reporting compliance to payments processes; more efficiently supporting audit recovery projects of previously enacted payments.

Automatically and continuously analysing the Master Supplier File for opportunities to reduce the risk of error and/or fraud caused by duplicated supplier records, supplier records that are not actively being used or changes.

NXG Forensics utilises a read-only extract from the organisation's ERP/accounting system. This will be collected, typically daily, and uploaded (automatically or manually) into the FISCAL NXG Forensics software service.

The extracted data will be encrypted both in transit and when stored within the NXG Forensics platform and it will remain in the same geo-regulatory region as specified during implementation. It will not be shared in an unencrypted form with anyone other than FISCAL.

The Artificial Intelligence enabled processing compares each payment and/or supplier record with stored historic and current records identifying potentially abnormal ('exception') characteristics with the payment

or supplier in question. A risk score is assigned to the record depending on the range of potential abnormalities discovered.

After processing, the analysis is presented back to the authorised user(s) to determine whether any risk avoidance action is required. The risk decision and actions of the user are recorded and may be used to moderate the risk profile of future similar instances.

The data is related to characteristics of the payment or supplier record. For example:

Payments:

System identifiers for ERP, transaction & user(s), dates, values, currency, supplier reference and name, description, internal purchasing organisation

Suppliers:

Supplier/site references, address(es), banking details, contact details

The data may contain details from international suppliers and may include payments intended for international recipients. The amount of data processed and stored is typically between 13 months and 36 months of payment transactions, as agreed contractually, and supplier data is dependent on the size of the Master Supplier File.

The Data Subjects whose data FISCAL may process may include:

(i) suppliers or prospective suppliers;

(ii) employees or prospective employees; or

(iii) other entities (including temporary employees, contractors and sub-contractors) of the organisation as applicable.

The types of Personal Data which FISCAL may process (only to the extent necessary to carry out the purpose) of those Data Subjects are:

(i) personal contact information (including names, addresses, email addresses, mobile and

telephone numbers);

(ii) employment details (including employee name, employee ID, system login IDs, bank details);

(iii) business contact details;

(iv) financial details; and

(v) other types of Personal Data which the organisation expressly informs FISCAL that FISCAL may process in order to fulfil the purpose.

No special category or criminal offence data is required to be processed by FISCAL and FISCAL specifically asks organisations to warrant that such data will not be provided to FISCAL for processing at any time.

4.1.2 NXG Forensics – Benefits

4.1.2.1 What will the benefits be to the organisation?

NXG Forensics Recovery Audit will identify any overpayments which have been made via Accounts Payable and the Customer will then be able to start a process to recover those overpayments, should they choose to.

NXG Forensics will enable the identification of potential duplicate or fraudulent payments prior to the payment being made. These can be assessed and if found to be incorrect, the payment will not be made ensuring Funds are not issued incorrectly.

4.1.2.2 *What will the benefits be to individuals and other parties?*

NXG Forensics identifies recoverable funds which have been paid in error to enable the customer to recover and increase their available funds for expenditure in the financial year and in future years, public funds are not reduced due to incorrect payments.

4.1.2.3 *Could individuals and other parties be affected negatively by the processing provide details (for example if we might make adverse decisions about them)?*

Yes. If over payments are identified and recovery action is taken, then those suppliers or individuals will be impacted negatively by having to repay funds even though they were not legally entitled to the payments initially.

4.1.3 Environment Summary

NXG Forensics is written and developed by FISCAL Technologies and hosted in Microsoft Azure utilising a mix of PaaS and SaaS offerings to host our SaaS solution, taking inspiration from Microsoft Azure Architecture Center (Link) for our architectural design. Utilising Azures' offerings allows FISCAL to monitor trends in usage and harness the elastic nature of Azure to scale up quickly to increase capacity on demand where needed.

NXG Forensics is developed leveraging numerous languages and frameworks including: C#, Typescript, .Net core, react, terraform.

NXG Forensics utilises API's for elements of its structure, of which we allow customers to utilise them for uploading of data in to NXG Forensics. Documentation can be found here:

https://onboarding.apfnxg.com/uploads/why

4.2 AP FORENSICS

4.2.1 Product Summary

FISCAL AP Forensics is FISCAL Technologies legacy SaaS solution that aims to improve the financial operational performance of customers organisations by automatically and continuously analysing payments data (typically invoices and credit notes) and Master Supplier Files.

AP Forensics provides analysis prior to payment to determine the risk of error and/or fraud and protects against duplicated supplier records, inactive suppliers, or changes to reduce the risk of error and/or fraud.

The solution provides reporting to enable compliance to payment processes.

4.2.2 Environment Summary

TBC

5. ISMS & GOVERNANCE

Management direction for information security

Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall "information security policy" as specified in ISO/IEC 27001 section 5.2.

5.1 ORGANISATION OF INFORMATION SECURITY

FISCAL Technologies operates an ISMS program to protect the confidentiality, integrity, and availability of its data and information systems and the data provided by its customers, regardless of how its data is created, distributed, or stored. FISCAL Technologies implements security controls accordingly so that cost-effective controls can be applied with the risk and sensitivity of the data and information system in mind and in accordance with all legal / compliance obligations.

5.1.1 ISMS Scope & Certifications

FISCAL has taken the decision to implement an Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of its information assets. To meet legal and professional requirements and satisfy obligation to our customers FISCAL must use cost effective security measures to safeguard its and its customer's information resources. This Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The scope of the ISMS is as follows:

The provisioning and management of FISCAL's SaaS delivered financial software from the Reading, UK facility and the associated data centres.

The assets deemed to be within the scope of the ISMS are as follows:

- FISCAL internal interested parties - Desktop and Laptop computers
- FISCAL Reading corporate IT infrastructure
- FISCAL Reading Network and Internet Connection (Leased Line / DSL Backup)
- Cloud Platform Infrastructure (Microsoft Azure)
- Cloud Platform Infrastructure (The Bunker)

FISCAL Technologies is certified under the ISO27001:2013 standard and Cyber Essentials.

5.1.2 Roles & Responsibilities

The FISCAL Technologies Executive Leadership Team has the objective to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Ensuring the ISMS programme must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

The FISCAL Technologies Board has assigned the COO overall responsibility for:

- Ensuring that the ISMS conforms to the requirements of ISO27001:2013
- Development and dissemination of IS Standards within FISCAL Technologies
- Reporting on the performance of the ISMS
- Electing members of the IS Forum and chairing meetings

COO may choose to delegate some or all these responsibilities from time to time to the Chief Information Security Officer (CISO), Technical Information Security Officer (TISO) or to others as appropriate.

At current the role of COO is assuming all responsibilities comparable to those of CISO.

FISCAL Technologies allocates role of Technical Information Security Officer (TISO) to the Head of IT to ensure proper technology risk considerations are addressed at each phase and provide proactive solutions to correct exposures or mitigate risk. They are responsible for interpreting procedures, and guidelines for multiple platforms and environments in designing solutions, recommending enhancements, or defining mitigating controls to existing systems.

All employees of FISCAL Technologies are responsible for reviewing, understanding, and abiding by company policies.

Roles and Responsibilities are documented as part of FISCAL's ISMS policies and included in a governance document that is signed by all employees to confirm they have read and understand the security policies of FISCAL Technologies.

5.1.3 Policies

As part of FISCAL's ISMS programme, we have created information security policies that are reviewed and maintained on a yearly basis. All Staff are informed of any material changes to policies and are expected to review and understand current company policies.

The policies apply to all information whether spoken, written, printed or computer-based, which is owned, held in the custody of, or used by FISCAL Technologies.

The Policies also apply to all resources used in creating, processing, transmitting, storing, using or controlling that information.

The objectives of these policies are to ensure that:

- Information is protected from unauthorised access, disclosure, modification, or loss.
- Information is authentic.
- Information and equipment are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded, and managed.
- Safeguards to reduce risks are implemented at an acceptable cost.
- Audit records on the use of information are created and maintained as necessary.
- All legal, regulatory, and contractual requirements and standards of due care are met.
- All staff to receive Information Security training at their induction.
- All staff to receive Information Security training at least annually.

FISCAL's privacy policy can be found on our website: https://fiscaltec.com/privacy-policy/

5.1.4 CISO – Chief Information Security Officer

Name: Lesley Reeve

Title: Chief Operating Officer / Director of Customer Success

Email: lreeve@fiscaltec.com

Phone: 01344 988712

5.1.5 DPO – Data Protection Officer

FISCAL is currently not required by law to have a dedicated DPO however, to ensure FISCAL manages data protection appropriately; The review of incidents or disputes are managed by the CISO or TISO.

If you have any complaints regarding data privacy, you should first contact us at privacy@fiscaltec.com. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of your personal information in accordance with our policies and legal requirements.

5.2 COMPLIANCE WITH LEGAL & CONTRACTUAL REQUIREMENTS

FISCAL accepts its obligations to comply with the laws of the United Kingdom. All employees of FISCAL must be aware that there are legal requirements relating to information that must be met.

The principles of these are detailed below:

Commented [A1]: 1.1.1Mandatory appointment

Under the GDPR, appointing a DPO is mandatory under thr circumstances:

1.The organisation is a **public authority or body**.

2.The organisation's core activities consist of data proces operations that require regular and systematic **monitori of data subjects on a large scale**.

3.The organisation's core activities consist of large-scale processing of **special categories of data** (sensitive data such as personal information on health, religion, race or sexual orientation) and/or personal data relating to crimi convictions and offences.

SMEs (small and medium-sized enterprises) are not exempt from the DPO requirements, should any or all of the above apply to them.

What are the legal requirements for the DPO role?

Independence

The GDPR requires that the DPO operates independently and without instruction from their employer over the way they carry out their DPO tas This includes instructions on what result should be achieved, how to investigate a complaint or whethe consult the ICO. Organisations also cannot tell their DPO how to interpret data protection law.

No conflicts of interest

Although the GDPR allows DPOs to "fulfil other task and duties", organisations are obliged to ensure tha these do not result in a "conflict of interests" with th DPO duties. Most senior positions within an organisation are likely to cause a conflict (e.g. CEO, chief operating officer, chief financial officer, chief medical officer, head of marketing, head of HR and head of IT).

5.2.1 Data Protection Act 2018

This legislation updates the previous UK Data Protection Act and enshrines the General Data Protection Regulations (GDPR) into UK law. It places obligations on those who record and use personal data and the organisation for which the work.

CISO/SIRO is responsible for registration matters with the Office of the Data Protection Registrar, application of the Data Protection Principles and the briefing of all Data Users within the team.

5.2.2 Privacy & Electronic Communications Regulations (PECR)

The e-privacy Directive complements the general data protection regime and sets out more specific privacy rights on electronic communications. It adopts the GDPR definition of 'consent' and provides rights to individuals regarding the data stored about them for tracking or marketing purposes including the requirement for explicit consent for the data to be held and the right for the data to be deleted.

5.2.3 Software Copyright

Software is protected by the Copyright, Designs and Patents Act 1988, which state that 'the owner of the copyright has the exclusive right to copy the work'.

It is illegal to make copies of software without the owner's permission. Penalties include unlimited fines and up to two years in prison.

5.2.4 Computer Misuse Act

The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer.

The offences are:

- Unauthorised Access to Computer Material
- Unauthorised Access with intent to commit or facilitate the commission of further offences
- Unauthorised Modification of Computer Material

5.3 INFORMATION SECURITY REVIEWS

5.3.1 Employee Awareness Training

FISCAL provides security education and training to all staff as appropriate to their assessed needs.

FISCAL provides staff with education, notes and information on topical security trends e.g. Password Management, Phishing, Impersonation Prevention, etc through email, face to face or training sessions where applicable.

FISCAL Developers are educated on changes to each OWASP revision to ensure good coding practices.

FISCAL also utilises a learning and development platform that provides training on key security areas including ISO27001 and GDPR for all employee's yearly and all employees are tested to validate their knowledge. The learning and development platform is reviewed at the end of each contract renewal to review it's continued validity and allow FISCAL to have the most appropriate platform for security education.

5.3.2 Internal Audits

5.3.3 External Audits

The organisation's information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employees' and systems' compliance with security policies, procedures etc. and initiate corrective actions where necessary.

Does your organization maintain cyber liability insurance in addition to general liability insurance? Yes, $5 million aggregate

6. HUMAN RESOURCE SECURITY

6.1 PRIOR TO EMPLOYMENT

Information security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (e.g. through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements defining security roles and responsibilities, compliance obligations etc.).

6.2 DURING EMPLOYMENT

Managers should ensure that employees and contractors are made aware of and motivated to comply with their information security obligations. A formal disciplinary process is necessary to handle information security incidents allegedly caused by workers.

Do you have a formal procedure for creating IT accounts?

Yes

FISCAL has a formal procedure for starters, leavers and change requests that follows the process of creation, change and removal of user accounts.

6.3 TERMINATION AND CHANGE OF EMPLOYMENT

Security aspects of a person's departure from the organization, or significant changes of roles within it, should be managed, such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy and intellectual property laws, contractual terms etc. plus ethical expectations.

Is there a formal de-registration procedure for user accounts to ensure they are disabled after a person has ceased employment?

FISCAL has a formal procedure for starters, leavers and change requests that follows the process of creation, change and removal of user accounts.

7. ASSET MANAGEMENT – DATA

7.1 RESPONSIBILITY FOR ASSETS

All information assets should be inventoried, and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization.

7.1.1 Example Questions

7.2 INFORMATION CLASSIFICATION

Information should be classified and labelled by its owners according to the security protection needed and handled appropriately.

7.3 DATA RESIDENCY

7.4 MEDIA HANDLING

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Inventory of assets Are all IT assets recorded in an up-to-date inventory? How? (e.g. a central database, excel spreadsheets etc.) Yes

Acceptable use Do you have any documented rules for the acceptable use of assets by staff? How are they communicated to staff? (e.g. rules for email and internet use, remote access, etc.) Yes

Information classification Do you classify information? (e.g. confidential, internal, public, etc. relating to the value of the information) Yes

Information classification Do you protect information based on its classification? (e.g. with encryption, secure disposal, etc.) Yes

Information labelling & handling Is there a documented procedure directing staff on the handling of information at different classification levels? (e.g. rules for information processing, storage, transmission, and destruction) Yes

Secure disposal Are IT assets and electronic media recycled or disposed of securely? (e.g. securely erased, physically destroyed) Yes

Secure disposal Do you ensure confidential paper waste is disposed of securely? (e.g. shredding) Yes

7.5 DATA PROTECTION

7.5.1 Scope

The scope of the data held by NXG Forensics is as follows:

- NXG Forensics processes invoices and supplier data held in ERP/accounting systems.
- NXG Forensics data is stored and used within the solution to identify patterns and find future potential risks.
- NXG Forensics will only require access to Employee data if the Employees module has been purchased.

- NXG Forensics does not require any personally identifiable data/ information (PII), but it is possible the supplier information will contain names, phone numbers and email addresses. It is also possible that some suppliers will be individuals and so recognisable by "supplier name" and address information. Except where the Employees or Sanctions/ ESG module has been selected.
- NXG Forensics does not store any Protected Health Information (PHI) data.
- NXG Forensics does not store any financial data considered to be "in-scope" for Payment Card Industry Data Security Standard (PCI-DSS) or Sarbanes-Oxley (SOX) regulations.

Direct access to customer data is on a least privilege basis and is restricted to those required to investigate specific customer issues and the Data Science team.

7.5.2 Encryption

NXG Forensics approach to encryption is as follows:

- NXG Forensics protects customer data by encrypting all data transfers and all data at rest.
- NXG Forensics data in transit is transmitted over HTTPS using TLS 1.2 (AES 256) encryption.
- NXG Forensics secures all data at rest using AES-256 encryption.
- NXG Forensics utilises a RESTful API connection secured with JWT bearer authentication and HTTPS/TLS 1.2 encryption when customer data is being imported.
- NXG Forensics publicly accessible endpoints all require authentication and authorisation and where applicable firewalls are deployed to further restrict access.

Additionally, backups are kept to enable data to be restored.

7.5.3 Customer Data Separation

transmissi

7.5.4 Additional Customer Data Usage

As per the contract, data may be used for development and test purposes, to improve the effectiveness of the solution and ensure that the most appropriate risks are presented to BHSF. When used for these purposes data is stored in restricted environments which are only available to a limited number of engineers that require access.

Data can be transferred to our dedicated data science environment to help improve the product.

7.5.5 Site & Data Destruction

NXG Forensics securely removes all associated data from a customer's site at the point the no longer wish to utilise the service. Custom scripts are used to remove platform elements and Microsoft Azures tooling is utilised to remove the data from their PaaS offerings.

The customer's NXG Forensics site will be deleted at the point they terminate their contract leading to the destruction of their data and backups within 30 days.

As NXG Forensics is hosted using Microsoft Azure's PaaS and IaaS offerings, destruction of data is managed in line with their security processes (https://servicetrust.microsoft.com/).

Details of Microsoft Azure's disposes of equipment can be found in the Equipment Disposal section in the attached link:

https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

7.5.6 Meta-data

NXG Forensics product usage metrics metadata is collected to help provide you the best service we can. This includes page visits, processing metrics & authentication attempts. All metadata is stored in the EEA region. It is not possible to opt out as without this information it is not possible to ensure that the service is running effectively.

It is not possible to opt-out of this data collection as this data is required to ensure that the services running effectively.

NXG Forensics login information, permissions and audit logs are stored centrally in the EU, but all their customer data is stored in their selected region.

When implementing NXG Forensics typically customers will provide between 1 and 3 years of historic data which is used to identify risks. This data is extended each time additional Transaction and Supplier data files are uploaded to NXG Forensics. Our algorithms use this data to understand the suppliers invoicing behaviours in order to understand whether they pose a risk to the customer. As such we retain historical data for the duration of the customer using NXG Forensics. If the customer chooses to stop using the service at a later date all associated data from the customer's site will be removed.

7.5.7 Miscellaneous

NXG Forensics does not provide an archiving capability.

7.5.8 Does the processing concern vulnerable individuals?

- Yes

7.5.9 Does the processing involve large amounts of personal data (for example, where many individuals are involved, or many categories of data)?

- Yes

Will the processing involve the consolidation or matching of data sets?

- Yes, data is consolidated and matched to identify potential risks

Does the project include systematic monitoring of a publicly accessible area on a large scale?

- No

Will the data transfer across borders outside the European Union? (UK/EU customers only)

- No

Will individuals have been compelled to provide personal or sensitive information about themselves?

- No

Will the processing result in you making decisions or taking action against individuals in ways which can have a significant impact on them? This includes evaluation and profiling activities.

- Yes

What is the key legislation that is associated with this processing?

- Data Protection Act 2018, UK GPDR 2021, Section 151 Local Government Act 1972

Commented [A2]: 'Processing' means any operation or set o operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptat or alteration, retrieval, consultation, use, disclosure by transmiss dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.Processor
'Processor' means a natural or legal person, public authority, ag or other body which processes personal data on behalf of the controller. Data processors are organisations or entities that pro personal information on behalf of a data controller. As noted ab 'processing' is essentially anything done to the data, including storage, archiving or just looking at it. It is normal for an organisation to be both a controller and a processor in respect o most personal data; it is only processing that is carried out by th parties on behalf of the controller that has to be addressed in lir with the requirements on processors.

2.Personal data
'Personal data' means any information relating to an identified o identifiable natural person ('data subject'); an identifiable natura person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to or more factors specific to the physical, physiological, genetic, men economic, cultural or social identity of that natural person. Perso data under the GDPR is a broad set of types of information abou "an identified or identifiable natural person". This means that th information is not personal data if there is no way to link it to a natural person. Personal data is anything that could be linked in way to the data subject, so organisations will need to be careful about how information is gathered and used, as it may be possib to accidentally gather sufficient information to remove the anonymity of the subject. Note that the definition specifically includes biometric, genetic and health information, as well as or identifiers, such as an IP address that can be used to identify a person. The GDPR does not extend any rights to deceased perso

Who are the data subjects?

- Any individual that has been paid through the ERP system

Does the processing involve innovative technologies?

Yes, Artificial Intelligence is used to find risk

Does the processing involve privacy invasive technologies?

- No

8. DEVICE MANAGEMENT

8.1 RESPONSIBILITY FOR ASSETS

All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization.

8.2 INFORMATION CLASSIFICATION

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

8.3 MEDIA HANDLING

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

8.4 MOBILE DEVICES AND TELEWORKING

There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other Boys' Toys) and teleworking (such as telecommuting, working-from home, road-warriors, and remote/virtual workplaces). [I don't know how this ended up under section 6, but here it is.]

If USB storage devices are allowed, is all data stored on such devices required be encrypted while at rest?

- USB storage devices are not allowed unless with explicit permission from TISO or CISO. Allowed devices are required to be encrypted.

Inventory of assets Are all IT assets recorded in an up-to-date inventory? How? (e.g. a central database, excel spreadsheets etc.) Yes

Acceptable use Do you have any documented rules for the acceptable use of assets by staff? How are they communicated to staff? (e.g. rules for email and internet use, remote access, etc.) Yes

Information classification Do you classify information? (e.g. confidential, internal, public, etc. relating to the value of the information) Yes

Information classification Do you protect information based on its classification? (e.g. with encryption, secure disposal, etc.) Yes

Information labelling & handling Is there a documented procedure directing staff on the handling of information at different classification levels? (e.g. rules for information processing, storage, transmission, and destruction) Yes

Secure disposal Are IT assets and electronic media recycled or disposed of securely? (e.g. securely erased, physically destroyed) Yes As NXG Forensics is hosted using Microsoft Azure's PaaS and IaaS (Infrastructure as a Service) offerings, destruction of data is managed in line with their security processes (https://servicetrust.microsoft.com/).

We have a policy internally for how media is sanitized.

Secure disposal Do you ensure confidential paper waste is disposed of securely? (e.g. shredding) Yes

Do you utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices? All company devices have Microsoft Bitlocker which encrypts the hard drives.

All staff operate daily work devices for their day to day activities. Management of the cloud service is split in two ways. Delivery and service configuration is automated through a CI/CD pipeline process where engineers do not have any privilege to access or modify the production environment. Changes to production require code to be amended into source control, peer reviewed and released via a release CAB to minimise risk of impact from malicious actors be that internal, external or programmatic. Other Management is done via a web browser through the similar portals that our customers access to access the product. All users do not have administrator access with the exception of the engineering team and domain administrators. Engineers require administrator privileges to enable them to run a native NXG environment on their device for development purposes.

Personal devices are allowed within FISCAL following restrictions based on our BYOD policy. Development of product and access to customer data is not allowed from a personal device by policy. Access to the management plane requires access from a FISCAL IP address restricting access from personal devices. All personal devices accessing email or collaboration tools must be on the latest version of the OS and patched inline with policy before accessing any data. No customer data is to be viewed or stored on personal devices.

All devices are part of a domain and controlled and hardened centrally via policy. We utilise device management solutions to ensure compliance of devices and delivery of software, configuration, patches to end user devices. All devices have an always on VPN solution on them to ensure they are controlled and data between them and the business is encrypted and controlled. All devices are part of update rings to ensure they are patched against vulnerabilities and exploits. All devices are encrypted by default and USB devices are restricted by policy and device management policy. All approved USB devices must be approved by the Head of IT and encrypted prior to use. All devices are protected with endpoint protection solutions that receive daily updates, always on scanning and full scans weekly, with protections for email and web. We also have email protection policies applied to our mail services to reduce risk related to potential email exploits. The FISCAL network utilises DNS protection to reduce risk with web access from end users. All delivered software goes through a risk review process prior to selection or installation to further reduce risk and ensure that all utilised software packages meet the business, security and compliance requirements.

We utilise KnowBe4 for training of all end users on a regular basis ensuring we have focus on key topics following trends we see in our environment and in the industry. Engineers undergo extra training related to privilege and OWASP. All new starters undergo an extensive NCSC certified training package to ensure all team members have a comprehensive understanding of security. We also run biweekly phishing testing at all employees.

9. ACCESS CONTROL

9.1 BUSINESS REQUIREMENTS OF ACCESS CONTROL

The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted.

9.2 USER ACCESS MANAGEMENT

The allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (now called "secret authentication information") plus regular reviews and updates of access rights.

9.2.1 Password Management – General

Are passwords allocated using a secure process? (e.g. identity checks of users, new/reset passwords are forced to change after use, new/reset passwords are random) Yes

Do passwords and authentication processes conform to a secure, standardised format? What is the format, e.g. mixed case, letters and numbers, minimum characters? Yes Minimum 14 characters with complexity requirements. Passwords have a maximum age of 180 days and minimum of 1 days. Passwords cannot be reused remembering the last 24 passwords. Account lockouts are in place with a 15 minute lockout duration following 10 invalid attempts in a 15 minute window. We also require MFA be used where possible.

Are passwords for key applications stored securely? (i.e. salted and hashed, salted and encrypted, etc.) Yes Passwords for key applications are stored in secure key vaults.

Exceptions to these defined rules are detailed below in their associated areas.

9.2.2 Password Management – Internal

Minimum 14 characters with complexity requirements. Passwords have a maximum age of 180 days and minimum of 1 days. Passwords cannot be reused remembering the last 24 passwords. Account lockouts are in place with a 15 minute lockout duration following 10 invalid attempts in a 15 minute window. We also require MFA be used where possible. Multi-factor authentication is required by to access the live production administration tools. By default MFA is required for all user accounts, regardless of privilege level.

Uses b2c…

9.2.3 Password Management – NXG

Are passwords allocated using a secure process? (e.g. identity checks of users, new/reset passwords are forced to change after use, new/reset passwords are random) Yes

Do passwords and authentication processes conform to a secure, standardised format? What is the format, e.g. mixed case, letters and numbers, minimum characters? Yes NXG's password policy follows the "Strong" complexity requirements provided by Azure B2C. This currently requires a password that is at least 8 to 64 characters and requires 3 out of 4 of the following types of characters: lowercase, uppercase, numbers, or symbols. B2C also utilises smart lock out functionality to block accounts after 10 failed logon attempt for 60 seconds increasing in time each failed attempt.

NXG Forensics provides an option to integrate with the customers own SSO solution. This option allows the customer to manage items such as password expiry, reset and the number of invalid attempts before lockout using their own authentication policies. The SSO integration also supports MFA.

The list of currently supported SSO providers can be found on the NXG Forensics on-boarding pages, by following the link below:

https://onboarding-uswest.apfnxg.com/sso/overview

NXG supports OAUTH/ OpenId for Single Sign-on

Are passwords for key applications stored securely? (i.e. salted and hashed, salted and encrypted, etc.)
Yes Passwords for key applications are stored in secure key vaults.

9.3 USER RESPONSIBILITIES

Users should be made aware of their responsibilities towards maintaining effective access controls e.g. choosing strong passwords and keeping them confidential.

Are users educated to not share passwords or store them insecurely? Yes FISCAL's security policies advise how to safely handle secrets and how to appropriately store them.

9.4 SYSTEM & APPLICATION ACCESS CONTROL

Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities and restricted access to program source code.

9.4.1 Application Connectivity

NXG Forensics is hosted in the Microsoft Azure cloud service and does not require application servers to be hosted at the customer's site.

NXG Forensics will not initiate any connectivity to the customer's network and does not require a dedicated network connection.

Customer's will need to push data files (transaction, suppliers, employees) via an API to NXG Forensics for processing and analysis, to provide insights into potential risks and anomalies. This data transfer is secured by…

All website certificates use SHA256 with either 2048-bit RSA or 256-bit ECDSA keys.

Documentation on the uploads API can be found here:

https://onboarding.apfnxg.com/uploads/why

User's access to NXG Forensics is via a supported browser (Google Chrome, Microsoft Edge & Mozilla Firefox). Access is secured either by username/password or SSO.

NXG Forensics supports current versions of Chrome, Edge and Firefox.

NXG Forensics does not support mobile devices.

Is access to IT systems approved by an approval authority, with access granted according to user roles, based on the principle of least privilege to a level that allows them to carry out their duties?

Yes

FISCAL gifts privilege to its users based on the users role utilising the least privilege model to ensure they only have the required level of privilege to carry out their duties.

Is end user and privileged access to critical systems and applications reviewed at least annually?

Yes

FISCALs policies state that Asset owners should audit atleast yearly associated privileges and report requirements for change.

Do IT systems have screensavers which lock after a short period of inactivity? Yes FISCAL's computers have an inactivity timeout policy applied that will automatically lock the screen after 10 minutes of inactivity.

Do you implement a clear desk policy for paper media and removable media (i.e. USB sticks, CDs, etc.)? Yes FISCAL has a policy that defines the requirements for clear desks and screens.

Does all remote access to your network require strong (e.g. two-factor) authentication? Partial "For internal access we require the device to be a member of our domain and a valid AD username and password.

For our production environments these are segregated and limited administrators are allowed access from RBAC roles, VPN which requires 2 factors of authentication."

Do you segregate the network? (e.g. externally facing services are in DMZs) Partial "Internal Services are not segregated.

All production environments are segregated away from the internet network and secured using network / resource / environment segmentation."

Is access to IT systems controlled by an authentication mechanism which permits authorised users and denies access to unauthorised users? (i.e. unique ID and password) Yes

Is encryption used to protect sensitive information stored on all portable media devices (e.g. laptops, smartphones, tablets) Yes Two-Factor Authentication

Do you have a formal policy for remote working that includes security? Yes

9.4.2 Application Session Management

NXG Forensics maintains user sessions state and manages them using Microsoft Azure B2C. Microsoft Azure B2C determines when the session identifier is no longer valid.

NXG Forensics user sessions currently timeout after one hour. This timeout is not customer configurable.

Microsoft Azure B2C has inbuilt defences to defend against session replay and man-in-the-middle attacks. Further information can be found at here:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

Identity & Access Management (IAM)

Do you review access rights?

- Yes, access rights are reviewed quarterly

Do you have dedicated zones for controlling access?

- Yes, Microsoft Azure is made up of a data and management layers

Is access to audit logs restricted?

- Yes, only authorised personnel are allowed to review audit logs

Do you, on a regular basis, review logs?

- NXG Forensics logs are not routinely monitored but are reviewed for the purposes of troubleshooting and diagnostics.

What authentication factors are supported?

- For Customers username and password are available, additionally SSO is offered for enhanced security

What SSO Providers are supported?

- For the latest list of 1st party support SSO providers please check here:

https://onboarding.apfnxg.com/sso/overview

What protocols are supported for SSO?

- OpenId Connect

Do you support Active Directory?

- No, NXG Forensics is a cloud based solution, if required Microsoft's Azure Active Directory may be an alternative solution

Can the software features be controlled via RBAC?

- Yes, roles are available and can be managed by a user administrator or FISCALs support team

Are all default passwords changed?

- Yes, where possible Microsoft Azure Managed Identity is used to limit password use

Do you support account lockout?

- Microsoft's Azure B2C is used to partially support this requirement, information on how threats are managed is documented here:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

Can the customer change the authentication policies?

- Yes if they use SSO integration

Can the users reset their own Passwords?

- Yes, password reset is available from the home page of the solution

NXG Password Policy

- "Strong" complexity requirements provided by Azure B2C currently: A password that is at least 8 to 64 characters. It requires 3 out of 4 of lowercase, uppercase, numbers, or symbols.

What is FISCAL Technologies internal password policy?

- Minimum 15 characters with complexity requirements.
- Passwords have a maximum age of 180 days and minimum of 1 day.
- Passwords cannot be reused remembering the last 24 passwords.
- Account lockouts are in place with a 15 minute lockout duration following 10 invalid attempts in a 15 minute window.
- MFA be used where possible.

List of non-supported auth

- LDAP, Active Directory, Kerberos

10. CRYPTOGRAPHY

10.1 CRYPTOGRAPHIC CONTROLS

There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

Cryptography

Can we generate customer specific keys ?

- No, all keys are managed at a platform level

Are keys stored in the cloud?

- Yes, the platform is built upon the Microsoft Azure service

What software is used for key management?

- All keys are stored in a Microsoft Azure Key Vault

What encryption standards and algorithms are used for key storage?

- Information around how keys are generated can be found here:

https://docs.microsoft.com/en-us/azure/key-vault/keys/about-keys#software-protected-keys

What TLS level is used?

- We use a minimum of TLS 1.2 across all services

Questions on the use of http and https

- HTTPS is always used throughout the NXG Forensics service

What encryption algorithms are used for data at rest?

- 256-bit AES encryption is used for data at rest

Is data anonymised or is pseudonymisation used?

- No, data is used in its original format in order to process it and identify risks

Is data encrypted?

- Yes, all data is encrypted at rest and in transit

11. PHYSICAL AND ENVIRONMENTAL SECURITY

11.1 SECURE AREAS

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas etc. against unauthorized access. Specialist advice should be sought regarding protection against fires, floods, earthquakes, bombs etc.

11.2 EQUIPMENT

"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and air conditioning) and cabling should be secured and maintained. Equipment and information should not be taken off-site unless authorised and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

11.3 PHYSICAL SECURITY

NXG Forensics physical security policy is as follows:

- The physical security of the NXG Forensics servers is managed by the Microsoft Azure service team. Details of which can be found here:

  https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security#physical-security

- NXG Forensics is SaaS solution hosted by Microsoft's Azure cloud solution, see attached link for further details:

  https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Microsoft Azure meets the following security standards; ISO 27001/27002, SOC1, SOC2

https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

Physical Security

Is wireless used on the network holding customer data?

- No, wireless networks are not used on a network that holds customer data

List the data centres Security standards

- Data centre security standards are managed by the Microsoft Azure team, details of these standards can be found here:

https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

Is wireless access on client machines configured to only allow access only to authorized wireless networks and to restrict access to other wireless networks?

- We do not restrict access to wireless environments. However we do enforce an always on VPN solution whenever the device is not in the corporate environment.

12. OPERATIONS SECURITY

12.1 OPERATIONAL PROCEDURES & RESPONSIBILITIES

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

Operational Security

NXG Forensics is primarily deployed on the Microsoft Azure platform which provides a secure environment to host the application. Microsoft Defender for the Cloud is reviewed on a regular basis to ensure that the latest security recommendations are reviewed and implemented as appropriate to ensure the platform is secure.

NXG Forensics is SaaS solution deployed within the Microsoft Azure cloud service and takes advantage of the security features provided by this platform.

https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Transactions and Supplier data can be uploaded to NXG Forensics via an API. NXG Forensics only accepts valid files of a specific type and size limits are enforced. The files are parsed as text files and are not executed. Once uploaded the files are not available for download.

Cloudflare and Microsoft Azure DDoS Protection provide protection to NXG Forensics from Denial of Service attacks.

NXG Forensics is hosted on Microsoft's Azure platform which manages the solutions network and infrastructure redundancy.

Yes, the NXG Forensics processor is the only know single point of failure. The processor is used when uploading files and therefore does not affect the daily reviewing of risks and suppliers. In the rare event of the processor failing, the Engineering team receives an alert allowing them to investigate and restart the service.

NXG Forensics application logs are used for diagnostic purposes when an issue is encountered. Monitoring and alerting is used to identify issues which are handled by a dedicated Engineering team.

As NXG Forensics is deployed on the Microsoft Azure platform the majority of these controls are provided by this platform. Microsoft Defender for Cloud is regularly monitored and security of the platform is updated based on these recommendations. Additionally, internal vulnerability scans are run against the software packages used by NXG Forensics so that issues can be identified and addressed. Finally external penetration tests assist in identifying potential weak points in NXG Forensics security.

An individual incident for a customer will be provided a support ticket, with ticket ID number for reference, communication is primarily through email however also through direct calls to the customer affected (when possible), customer is informed up to the point of resolution and a final satisfaction email is sent upon closure.

Prior to each NXG Forensics release, a release readiness meeting is held by the Change Advisory Board (CAB). The CAB consists of the Head of Operations, the Head of Development, Product Owners and senior members of the development team. During this meeting the CAB reviews a pre-list checklist and the release is only approved if the list is successfully completed.

Once the release is approved, it is deployed via an automated CI/CD pipeline.

Vulnerability scans are run against NXG Forensics on a weekly basis. When issues are identified they are evaluated and resolutions are scheduled based on severity. Normally, issues will be resolved during NXG Forensics 2 weekly release cycle, but high priority issues can be deployed as hot fixes.

Open vulnerabilities will be accepted in rare circumstances if it can be demonstrated to the satisfaction of the Head of Operations and Head of Software Development that it cannot be exploited within NXG Forensics.

NXG Forensics is hosted on Microsoft's Azure platform. Members of FISCAL Technologies support team are authorised to directly access customer sites via the User Interface once the customer has granted them permissions and there is an open support ticket.

The NXG Forensics service is monitored on a regular basis. Azure monitor allows us to monitor trends and increase capacity where needed. We also utilise the elastic nature of Azure to scale up when needed. When consistent platform issues are identified the resources allocated to the platform are adjusted appropriately.

Customer data is logical separated, while the physical security of the servers is managed by the Microsoft Azure service team. Details of which can be found here:

https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security#physical-security

Specific developers are granted access to live production systems on a limited basis only to assist with deployments or to diagnose issues.

Network ports are limited and controlled, and additional network restrictions implemented to limit network intrusion.

NXG Forensics uses a multitude of different technologies to protect customer data, these include, but is not limited to, the use of the following additional technologies: Azure’s SQL Transparent Data Encryption (TDE), Azure managed identities, HTTPS, Azure Key Vault.

FISCAL Technologies does not currently deploy an Intrusion Detection System (IDS) for NXG Forensics.

FISCAL Technologies has adopted the principle of least privilege to ensure that access to NXG Forensics live production environments is only available to those that require it.

Access to NXG Forensics live production environments will be granted to senior members of the development team in the case of an emergency to investigate the issue. In the majority of cases any modifications required to address the issue will be delivered by the automated deployment pipeline rather than manually. Escalated privileges will be removed once the issue has been diagnosed and addressed.

NXG Forensics sites are monitored on a regular basis, but no specific SIEM tools are deployed.

The live production NXG Forensics solution is deployed to a separate environment, segregated from all development and test environments. Access is restricted to only those employees that require it on a least privilege basis and the solution is update via a secure deployment pipeline.

It is FISCAL Technologies policy that all operational administration is undertaken from FISCAL supplied equipment.

NXG Forensics uses an Azure VPN Gateway to administrate the service. The supported cipher suites are documented by Microsoft on the link below under the "What IKE/IPsec policies are configured on VPN gateways for P2S?" and "What TLS policies are configured on VPN gateways for P2S?" sections.

https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#what-ikeipsec-policies-are-configured-on-vpn-gateways-for-p2s

Customer data is logically separated to prevent customers from accidently or maliciously accessing each other's data.

Development & Testing environments are deployed to separate sites that the live production environments and are therefore logically and most likely physically segregated from customer sites.

NXG Forensics sites are monitored to ensure that resources are available to prevent individual customers impacting the performance of other customers in that pool.

NXG Forensics user passwords are managed by Azure AD B2C, unless customers have selected the SSO integration option.

Access to the live production sites is restricted on a least privilege basis.

Multi-factor authentication is required by to access the live production administration tools.

Access to the live production administration tools is restricted on a least privilege basis.

Ensure an adequate patching regime is in place to apply updates within 3-14 days. General industry guidance is to deploy Critical patches within 7 days, High within 30 days, and others with 90 days

NXG Forensics is a SaaS solution, which is continuously updated as part of our development cycle. NXG Forensics receives an update to the product, its functionality, and any patches / updates / packages every 2 weeks or more frequently if urgent changes are required. Due the nature of the service, customers are unable to either accept or postpone updates. All updates are managed and applied to the solution automatically without customer intervention.

As part of each development cycle, we check for updates for all packages used in used in and supporting NXG Forensics, these go through an update ring cycle, where they are applied to our test environment and used through the 2-week sprint to ensure that they do not cause negative impact to the product from security, vulnerability, performance, stability or user experience perspectives. We utilise vulnerability management tools that scan our environments for vulnerabilities, security patches, and good practice configuration. NXG Forensics base images and environments are scanned multiple times a week and all supported packages are scanned at least once every 2 weeks. These tools highlight any risks or immediate remediations that need to occur before implementing our new release. These same tools scan our live environment to highlight new vulnerabilities. Where Critical or High vulnerabilities are found we will implement a Hotfix / remediation within at most 14 days from resolution of the vulnerability. If no resolution is planned, we review requirements for implementing a mitigation or potential changes required to resolve the vulnerability.

NXG Forensics is a SaaS solution deployed in Microsoft Azure. Where NXG Forensics utilises Microsoft SaaS offerings Microsoft are responsible for the patching and security of these products in line with their compliance requirements and service agreements. For all other areas of NXG Forensics, FISCAL manages the patching and update as described above. Details of Microsoft's compliance's and audit reports can be found here: https://servicetrust.microsoft.com/

As part of the development cycle all changes are peer reviewed, verified and approved prior to release, with the final release subject to review by the Change Advisory Board (CAB). The CAB works through a pre-release checklist covering numerous areas including (security, compliance, performance, stability, user experience), confirming all conditions are met before the release is approved. Releases are approved by Change Management Board (CAB) which consists of the Head of Operations, Head of Software Development, Chief Architect, Product Owners, and Software Engineers. Once approved, the release is deployed via a secure CI/CD pipeline. This is an automated process which overseen by an engineer who will ensure that the process runs smoothly and will approve a number of key stages as required. Once the release is complete final checks are performed to ensure that it has been successful. Where Critical or High vulnerabilities are identified, ADHOC releases can be authorised and expedited to minimalise the risk of vulnerability to the product and customers data.

12.2 PROTECTION FROM MALWARE

Malware controls are required, including user Leness.

Is anti-malware software in use?

- We utilize ESET cloud protect for all Fiscal end user computers.

  NXG Forensics is a SaaS solution hosted within Microsoft's Azure platform and is therefore able to take advantage of all the security measures provided by this service. We utilize Azure Defender for all of our cloud environment.

Is anti-malware software configured to get updates and run scans frequently?

- NXG Forensics is a SaaS solution hosted within Microsoft's Azure platform and is therefore able to take advantage of all the security measures provided by this service. Anti-malware software is therefore not currently used on the NXG Forensics platform.

  Devices scan at least weekly, we have constant scanning on end user devices and checks for updates every hour.

12.3 BACKUP

Appropriate backups should be taken and retained in accordance with a backup policy.

12.4 FISCAL TECHNOLOGIES BACKUP POLICY

12.5 NXG FORENSICS BACKUP POLICY

Is system data backed up?

- Customer backups are created nightly as part of the Microsoft Azure cloud solution and can be restored to a new site should NXG Forensics encounter a catastrophic failure.

  Backups are stored on a separate site in the same geographical location as the customer's main site.

Do you test restoration of systems from the back up?

- Due to the way we develop our solution, we run full rebuilds of our product in an automated fashion once every 2 weeks to prove continuity in a disaster event and we do a full backup hardened test at least once a year. With the next full test due to be run in Q3 2022.

  Internal infrastructure backups are automatically tested at least once a month through our backup solution.

12.6 LOGGING AND MONITORING

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

Do you monitor capacity and performance?

- Microsoft Azure provides mechanisms to monitor trends and increase capacity where needed. Microsoft Azure is also utilised to scale up quickly when required.

Do you use common time synchronisation?

- Yes, time management is synchronised across all services and is provided by Microsoft Azure

12.7 CONTROL OF OPERATIONAL SOFTWARE

Software installation on operational systems should be controlled.

12.8 TECHNICAL VULNERABILITY MANAGEMENT

Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

Vulnerability Prevention & Remediation

Do you use code analysis tools?

- Yes, source code is scanned weekly to identify potential issues

Do you review all software releases for vulnerabilities?

- Yes, part of the CAB process includes a review of all known vulnerabilities

Do you ensure software is running fully supported versions?

- Yes, dependant packages are updated frequently and as soon as possible for high or critical vulnerabilities

How is patch management of the platform handled?

- As we use PaaS Software, platform patch management is handled by the Microsoft Azure team

Threat Management

Do you monitor for network based attacks?

- Yes, a combination of Microsoft's Azure Monitor and Azure Security Centre are used to protect the platform

Are your systems and applications scanned for vulnerabilities prior to new releases?

- Vulnerability scans of NXG Forensics are performed weekly. Critical and High issues are resolved in the next sprint after discovery. The resolution of medium and low issues is scheduled in the short term roadmap.

Are audit logs collected centrally?

- Yes, all logs are collected centrally in Microsoft's Azure monitor

Do you have a SEIM?

- No, currently the combination of Microsoft's Azure monitor and Azure security centre is used in this space

Can logs be provided to the customer?

- No, logs are used for internal support and monitoring of the platform only

Do you have the ability to generate system or service alerts?

- Yes, Microsoft's Azure Security Centre provides alerts of all high incidents and custom alerts can be setup in Azure monitor

Do you perform platform level security scanning?

- No

Do you perform external pentests?

- Yes, pentests are performed annually

Can we perform our own pentests?

- Yes, please provide 1 weeks' notice

Are non-company devices allowed to access NXG?

- As a SaaS platform customers can connect to NXG Forensics via the devices of choice. FISCAL has policies that restrict the usage of employee's personal devices.

Are secure code training sessions provided to the members of the development team?

- Yes, courses based on OWASP are conducted at least annually

12.9 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

13. COMMUNICATIONS SECURITY

13.1 NETWORK SECURITY MANAGEMENT

Networks and network services should be secured, for example by segregation.

13.2 INFORMATION TRANSFER

There should be policies, procedures and agreements (e.g. non-disclosure agreements) concerning information transfer to/from third parties, including electronic messaging.

14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

14.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

Security control requirements should be analysed and specified, including web applications and transactions.

14.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled. Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled. System security should be tested, and acceptance criteria defined to include security aspects.

14.2.1 Application Development

NXG Forensics is developed on the Microsoft .NET platform.

FISCAL Technologies engineering team have adopted an Agile approach to development utilising techniques such as Scrum, Pair Programming, Continuous Integration and Continuous Delivery.

NXG Forensics is developed using Agile software development techniques, specifically Scrum, Continuous Integration and Continuous Delivery.

Application development currently takes place in Reading in the UK.

All NXG Forensics source code is held in a source repository. Code changes are initially developed in a private branch, which are peer reviewed and required a suite of unit tests to have successfully completed before merged to the main branch.

At the end of each two-week sprint, all verified changes will be moved to a release branch. A pre-release meeting will be held were the change advisory board (CAB) who will approve the release.

The release is then deployed via an automated process which updates the production environment.

Security is considered throughout the development process of NXG Forensics. All tasks are evaluated on creation, to determine whether they will have a potential impact on the security of the solution.

Once a task has been identified as having a potential security impact, any required mitigation will be addressed during the design phase and checked during the peer review.

Finally, all tasks flagged as having a security impact are reviewed by the CAB in the pre-release meeting to ensure that any issues have been addressed prior to deployment.

We use an in-house development team for the creation of NXG, at this time no work is outsourced to third parties.

Security is considered throughout development, from the design stage through to final sign off for the release

GDPR, ISO 27001 & OWASP awareness training is provided to developers.

All code goes through code reviews, it is also deployed to a test environment prior to release

Currently all development is undertaken by permanent employees located in the United Kingdom

An extensive set of unit and integration tests are maintained for all code

Microsoft Azure subscriptions are used to keep test and production environments apart

Data may be moved to our performance or data science environments, but these are considered production environments

All changes to the code base must have a work item assigned to them

Each task is assessed for any potential security risks at the design stage. Engineers develop the code against the OWASP principles, and a final review is conducted prior to release by the Change Advisory Board before the release is signed off.

Yes, duties are segregated within the development, testing and infrastructure support teams, although FISCAL Technologies is a small organisation resulting in some overlap between these roles.

For example, there is a single development team responsible for development and verification and senior engineers may be required to assist with operational support.

NXG Forensics is developed using the principle of "security by design". The software development team is familiar with the current OWASP top ten and receive an annual training to refresh their knowledge.

Software changes are coded, tested and hosted on different environments. Development takes place on a branch, once reviewed, verified and approved, updates are deployed to the verification/staging server. The final approved release is then deployed to the live production environment via an automated pipeline.

NXG Forensics development/test environments are also deployed to the Microsoft Azure cloud, but to separate sites. So, while they are certainly logically separated from customer sites they are also most likely also physically separated.

Risk assessments are performed on third-party packages and libraries, which include reviewing the justification for using the package and the results of a vulnerability scan security assessment.

NXG Forensics uses open-source packages/libraries to transmit, process and store data.

NXG Forensics is developed using the principle of "security by design".

The software engineering team develop the code against the OWASP principles and receive annual training to keep their knowledge up to date.

NXG Forensics is developed using the latest technologies to take advantage of built-in protection against a number of common vulnerabilities, including amongst others SQL injection, XSS attacks, CSRF, HTTP Response attacks.

All NXG Forensics infrastructure changes are made via Infrastructure as code and reviewed prior to release by the CAB which consists of the Head of Operations, Head of Software Development, Chief Architect, Product Owners and members of the Senior Development team.

NXG Forensics is primarily deployed on the Microsoft Azure platform which provides a secure environment to host the application.

Microsoft Defender for the Cloud is reviewed on a regular basis to ensure that the latest security recommendations are reviewed and implemented as appropriate to ensure the platform is secure.

The live production NXG Forensics solution is deployed to a separate environment, segregated from all development and test environments. Access to NXG Forensics live production environments is restricted to only those employees that require it on a least privilege basis and the solution is updated via a secure deployment pipeline.

Azure monitor is utilised to monitor trends and increase capacity where needed.

Vulnerability scanning is performed weekly on the third-party packages that are used within the solution.

NXG Forensics is subject to an annual Penetration test performed by an external CREST accredited agency.

Software Development Life Cycle

Do you have security controls in place?

- Yes, security is considered throughout development, from the design stage through to final sign off for the release

How do you verify the quality of you code before release?

- All code goes through code reviews, it is also deployed to a test environment prior to release

Are 3rd Party development teams used?

- No, currently all development is undertaken by permanent employees located in the United Kingdom

How are data input routines verified?

- An extensive set of unit and integration tests are maintained for all code

How are test environments separated from production?

- Microsoft Azure subscriptions are used to keep test and production environments apart

Will the customer's data be used in non-production environments?

- No, data may be moved to our performance or data science environments but these are considered production environments

Is Formal ticketing used?

- Yes, all changes to the code base must have a work item assigned to them

Is there separation of build and release?

- Yes, see the section on Change Management

Are information security principles designed into the product lifecycle?

- Yes, each task is assessed for any potential security risks at the design stage. Engineers develop the code against the OWASP principles and a final review is conducted prior to release by the Change Advisory Board before the release is signed off.

14.2.2 Verification Approach

FISCAL Technologies believes that product quality is the responsibility of the whole team and therefore does not have a dedicated QA team. Instead, the team relies heavily on automated testing and has invested in developing a suite of unit tests, automated integration, User Interface, and performance tests to ensure the overall quality of NXG Forensics.

NXG Forensics test strategy relies heavily on automated testing. Unit tests are created for each code change which are run automatically every time the source is built. Testing is further supported by a suite of Selenium tests which run each night. Changes are peer reviewed, before check-in and all changes are manually checked on a test system before being approved.

Load testing is performed on NXG Forensics once a week using a historical data file of 3 million transactions. Additional load testing is performed when research is required into specific performance issues or when changes are required to improve the scalability of the solution.

Functional and automated testing must be completed successfully prior to the NXG Forensics release.

14.2.3 Change Management Process

NXG Forensics is a SaaS solution, which is continuously updated (currently every two weeks, but more frequently if urgent changes are required). Due the nature of the service, customers are unable to either accept or postpone updates.

All updates are managed and automatically applied to the solution with the need for customer intervention.

All changes are peer reviewed, verified and approved prior to release, with the final release subject to review by the Change Advisory Board (CAB). The CAB works through a pre-release checklist, confirming all conditions are met before the release is approved.

Releases are approved by Change Management Board (CAB) which consists of the Head of Operations, Head of Software Development, Chief Architect, Product Owners, and Software Engineers.

Once approved, the release is deployed via a secure CI/CD pipeline. This is an automated process which overseen by an engineer who will ensure that the process runs smoothly and will approve a number key stages as required. Once the release is complete final checks are performed to ensure that it has been successful.

Routine releases are approved by the Change Advisory Board (CAB) which includes the Head of Development, the Head of Operations and Chief Software Architect. While minor urgent fixes can be approved by any two of the previously mentioned individuals.

The CAB is made up of the head of IT, Head of development and Development architects

All NXG Forensics infrastructure changes are made via Infrastructure as code and reviewed prior to release by the CAB which consists of the Head of Operations, Head of Development and the Senior Development team

All changes are deployed to an internal test environment for final verification prior to release to production

Component versions and patch levels are monitored on a regular basis, updated as required and deployed using Infrastructure as code techniques

The platform is deployed through a service account using Infrastructure as code to prevent un-authorised software being installed on any production systems

Software updates are currently deployed on a regularly two weekly basis and customers are informed of new features via the "What's New" notifications which appear in the product.

FISCAL Technologies operates a roll-forward policy should an issue be encountered during deployment, rather than rolling-back.

NXG Forensics is updated on a regular basis (currently every two weeks) and customers are notified of new features via the "What's New" text within the product.

Emergency changes can be signed off by a reduced subset of the CAB.

FISCAL Technologies operates a roll-forward approach when patching, where issues are fixed rather than updates rolled-back.

All changes are tracked in Azure DevOps which links the change request directly to the committed modified code.

The majority of patches are deployed at any time with minimal impact on customers. Patches that will potentially impact customers are deployed outside of standard working hours.

NXG Forensics is a SaaS solution deployed in Microsoft Azure cloud computing service, therefore the Azure team take responsibility for ensuring that the platform is up-to-date and secure.

Are infrastructure changes approved by the CAB?

- Yes, all NXG Forensics infrastructure changes are made via Infrastructure as code and reviewed prior to release by the CAB which consists of the Head of Operations, Head of Development, and the Senior Development team

Do you test infrastructure changes?

- Yes, all changes are deployed to an internal test environment for final verification prior to release to production

Do you monitor component versions and patch levels?

- Yes, component versions and patch levels are monitored on a regular basis, updated as required and deployed using Infrastructure as code techniques

Do you have controls in place to monitor unauthorised software?

- Yes, the platform is deployed through a service account using Infrastructure as code to prevent un-authorised software being installed on any production systems

Will you inform the customer of changes prior to release?

- No, software updates are currently deployed on a regularly two weekly basis and customers are informed of new features via the "What's New" notifications which appear in the product

14.2.4 Source Control Strategy

NXG Forensics source code is stored in a source repository. All changes are made in separate branches and need to be peer-reviewed before they can be committed to the main branch. As part of the commit process a suite of unit tests are run and the commit fails if any of the tests fail. Once the change has been manually checked and approved it is ready for release.

At the end of each development sprint (currently 2 weeks) all approved changes in the main branch are merged into the release branch ready for deployment.

Once approved, the release is deployed via a CI/CD pipeline. This is an automated process which overseen by an engineer who will ensure that the process runs without any issues and approves key stages as required. Once the release is complete final checks are performed to ensure that it has been successful.

14.2.5 Application Security

Security is considered throughout NXG Forensics development process, from design, through development and verification to release.

Packages used by NXG Forensics are reviewed and updated on a regular basis to reduce the opportunity of running against outdated components.

Microsoft Defender for the Cloud is reviewed on a regular basis to ensure that latest security recommendations are reviewed and implemented as appropriate so that the platform is secure.

NXG Forensics is developed following OWASP security principles to minimise the impact of security vulnerabilities.

NXG Forensics uses a combination of Entity Framework and parameterised queries for data access to protect against SQL injection attacks.

NXG Forensics UI is created using React, which comes with built-in mechanisms to protect against XSS attacks.

NXG Forensics API uses bearer tokens for authentication. This prevents CSRF from being an applicable attack vector.

NXG Forensics API uses ASP .NET core which has built-in protection against HTTP Response Splitting attacks. It makes minimal use of HTTP response headers and no user untrusted values are use in HTTP response headers.

NXG Forensics utilises React route templating to ensure URLs follow a certain pattern. If the URL is manipulated, the user will either be redirected back a valid page which they are authorised to access or an error page.

The NXG Forensics API uses ASP .NET core authentication, with authentication middleware running for all requests to enforce authentication. The API is also configured so that by default endpoints will return a forbidden response until the endpoint explicitly specifies what permissions are required to access that resource.

NXG Forensics API has a top-level exception handler which returns no detail in the event of an unhandled exception when running in production.

NXG Forensics is a SaaS solution hosted within Microsoft's Azure platform and is therefore able to take advantage of all of the security measures provided by this service.

NXG Forensics is subject to an annual Penetration test performed by an external CREST accredited agency. Additionally, a weekly vulnerability scan is performed on the third-party packages that are used within the solution.

The penetration test is an external test performed against a test account created on the production environment. This test does not include a source code review, but the external testers are granted access to a user account.

The last penetration test was performed against NXG Forensics in June 2021 by BlackBerry Cybersecurity Consulting.

Additionally Microsoft Azure Defender is utilised to constantly monitor the solution and identify potential vulnerabilities and identify security recommendations which can be utilised to improve the security of the platform.

NXG Forensics file integrity monitoring is managed by Microsoft Azure platform.

NXG Forensics secrets are secured in Microsoft Azure Key Vault.

NXG Forensics is a multi-tenant solution who keys are managed by Microsoft Azure's SQL Transparent Data Encryption (TDE).

NXG Forensics does not support the concept of user roles, but customers can restrict the permissions of individual users.

NXG Forensics supports role-based access controls. The following access restrictions are currently supported: file upload, create access token, user administrator, actions, employees, and unit access.

The NXG Forensics administrator will have the capability to manage users, while the user permission feature allows the customer to restrict access to the solution, based on the activities they are allowed to perform within their organisation's role.

NXG Forensics allows user access to be restricted. The following access restrictions are supported; file upload, create access token, user administrator, actions, employees, and unit access.

NXG Forensics currently allows multiple users sessions for the same user.

To prevent data leakage via error messages, NXG Forensics standard error handler only returns HTTP status codes.

NXG Forensics is completely segregated from FISCAL Technologies networks. IT utilises Microsoft Azure technologies to host and segment the PaaS, IaaS and SaaS services that make up our solution.

15. TEST DATA

Test data should be carefully selected/generated and controlled.

16. SUPPLIER RELATIONSHIPS

16.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS

There should be policies, procedures, awareness etc. to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

16.2 SUPPLIER SERVICE DELIVERY MANAGEMENT

Service delivery by external suppliers should be monitored and reviewed/audited against the contracts/agreements. Service changes should be controlled. [Exactly the same point applies to services delivered by internal suppliers, by the way!]

16.3 PROCESSORS AND SUB-PROCESSORS

16.3.1 Supplier Chain Security

NXG Forensics utilises the following external services as part of its solution:

Microsoft Azure Cloud Computing Services

1 Microsoft Way, Redmond, WA, United Stats

NXG Forensics is hosted by Microsoft Azure Cloud Computing Services. This service provides data storage and the resources for the solution to process data.

Compliance and Security Information:

https://servicetrust.microsoft.com/

https://azure.microsoft.com/en-gb/support/legal/

Cloudflare

101 Townsend Street, San Francisco, CA 94107, United States

Cloudflare is used by NXG Forensics to provide the service with DNS and DDOS protection.

Compliance and Security Information:

https://www.cloudflare.com/en-gb/trust-hub/compliance-resources/

FISCAL Technologies have an ongoing persistent contract with each of these providers.

Customer data is not available to these providers as it is encrypted during transit and at rest and is not visible.

Both parties were assessed prior to implementation and the security assurances provided on their websites were deemed to be acceptable for the purposes required of them.

FISCAL Technologies regularly reviews its solutions, identifying potential risks and either mitigating or accepting them depending on their severity.

NXG Forensics utilises the following external third-party services as part of its solution: Microsoft Azure Cloud Computing Services, Cloudflare and LexisNexis.

NXG Forensics is hosted by Microsoft Azure Cloud Computing Services. This service provides data storage and the resources for the solution to process data.

Cloudflare provides the NXG Forensics solution with DNS and DDOS protection.

NXG Forensics uses Lexus Nexus to identify Sanctions and ESG matches if these modules have been selected.

Customer data is not accessible by Microsoft Azure and Cloudflare as it is encrypted during transit and while at rest.

FISCAL Technologies assess its suppliers prior to implementation and the security assurances provided were deemed to be acceptable. All three services are ISO 27001 certified and Azure is certified with SOC1, 2, 3 and other certifications.

All suppliers provide appropriate cover based on our risk review processes and the data they handle

17. INFORMATION SECURITY INCIDENT MANAGEMENT

17.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS & IMPROVEMENTS

There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.

18. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

18.1 INFORMATION SECURITY CONTINUITY

The continuity of information security should be planned, implemented, and reviewed as an integral part of the organization's business continuity management systems.

Business Continuity Policy	Do you have a Business Continuity Policy?	Yes
Business Continuity Policy	Is your Business Continuity Policy reviewed and updated at least annually?	Yes
Business Continuity Policy	Do staff receive initial and ongoing awareness training of Business Continuity Policy and Procedures? (explain how)	Yes During onboarding and annual review of ISMS practices
Roles and responsibilities	Are Business Continuity Roles and Responsibilities clearly defined and documented?	Yes
Roles and responsibilities	Do you have an individual with the responsibilities comparable with those of a Business Continuity Manager? If no, what role are Business Continuity responsibilities part of?	Yes COO
Business Continuity Plans	Do you have a Business Continuity Plan(s)?	Yes
Exercising	Do you test your business continuity plans regularly to ensure that they are up to date and effective? How often?	Yes Annually

18.2 REDUNDANCIES

IT facilities should have sufficient redundancy to satisfy availability requirements.

Availability

Do you have an SLA?

- Yes, 99% within core business hours

DR

IT Disaster Recovery Policy	Do you have an IT Disaster Recovery Policy?	Yes
IT Disaster Recovery Policy	Is your IT Disaster Recovery Policy reviewed and updated at least annually?	Yes

IT Disaster teny Plans	Do you have detailed EADisaster Recovery plans?	Yes
IT Disaster Recovery	Do you test your IT Disaster Recovery plans regularly to ensure that they are up to date and effective? How often?	Yes FISCAL tests its disaster recovery plan yearly as part of an internal review process.

19. APPENDIX

19.1 GCLOUD

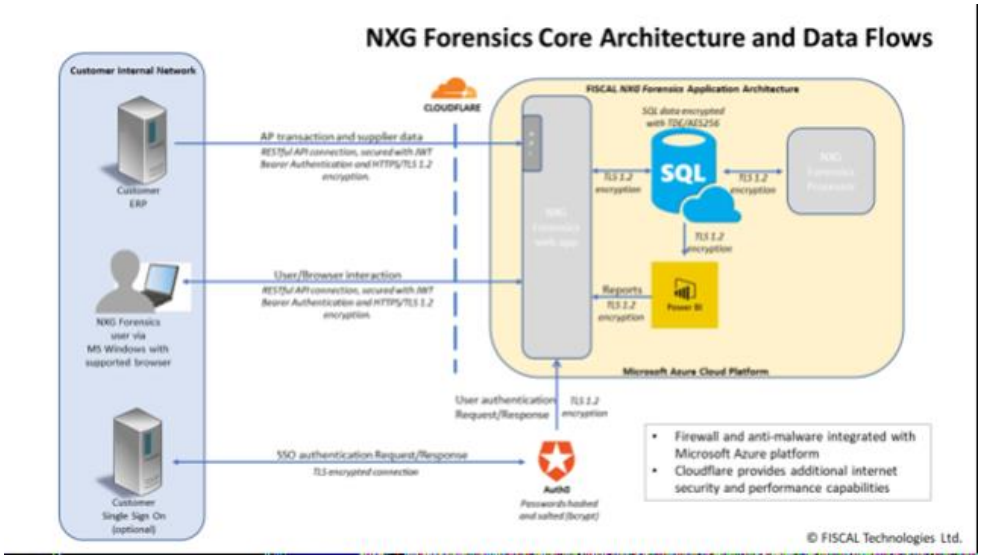
https://www.digitalmarketplace.service.gov.uk/g-cloud/services/785066254911746

19.2 ENVIRONMENT OVERVIEWS

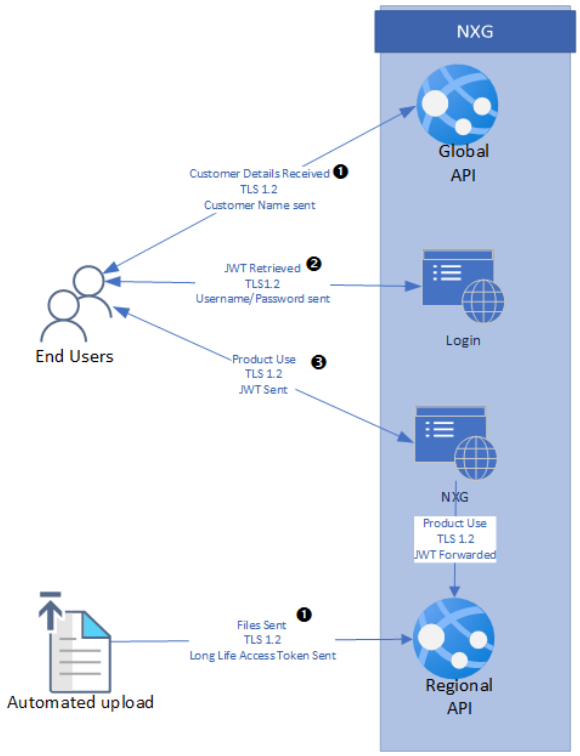
19.2.1 AP Forensics

19.2.2 NXG Forensics

19.2.2.1 Data Flows - High Level



19.2.2.2 End User Data Flow – High Level



19.2.2.3 Full Layout – Overview