question mark

Security of Questionmark's European OnDemand Service

Questionmark has a policy of continual improvement. Information herein is provided in good faith and is accurate at time of writing. However, based on knowledge and experience, Questionmark may update its security at any time.

Authors:

John Kleeman

David Hunt

Sonata Ožemblauskaitė

Last updated: 11 May 2020

www.questionmark.com

This paper is intended for use by Chief Technology Officers (CTO), Chief Security Officers (CSOs), IT Architects (ITAs) and others who need to understand the security of the Questionmark OnDemand service. This paper covers Questionmark's European OnDemand service.

Table of Contents

1. Management Overview

Questionmark is an ISO 27001 certified company who takes security seriously and operates a trustable, scalable and robust OnDemand Service for managing and delivering assessments. Questionmark's OnDemand Service contains multiple layers of security, including physical safeguards, access control, environmental management and uninterruptible power supply, and is protected by firewalls to appropriately restrict access. This document describes the blanket of security protections in place for customers and prospective customers. Some of the key capabilities include:

- High availability and resilient service
- Trustworthy staff including criminal background checks and training
- Physical security of the data centre
- ISO 9001 and ISO 27001 data centre certification
- Support of SAML 2.0 for user authentication
- N+1 and 2N redundancy with various carrier independent links to internet
- Network security including TLSv 1.1, 1.2 and IPS
- Uninterruptable power supplies with multiple connections to the grid through various sub-stations
- Back-up power generators
- Disaster Recovery Processes to maintain service continuity including hourly offsite backups

The following diagram shows the layers of protection that surround your data when stored in the service. Each layer provides an obstacle for a potential hacker and thereby confidence that your data is secure.
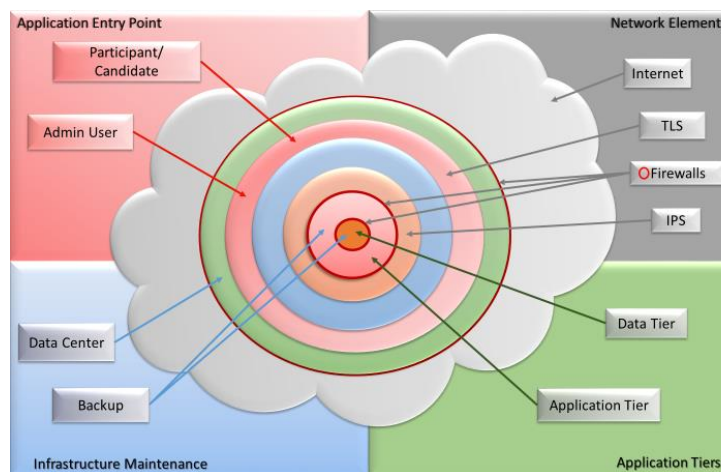
Using all the systems and security we have in place, we target a 99.9% uptime of Questionmark OnDemand. For more information on Questionmark security, see www.questionmark.com/trust.

2. Accreditations and Compliance

ISO 27001

ISO27001 (full name ISO/IEC 27001:2013) is the most widely recognized information security standard in the world. It recognizes organisations for establishing, implementing, maintaining and continually improving their Information Security Management System (ISMS).

Questionmark's Information Security Management System has been certified against ISO/IEC 27001:2013 by British Standards Institution (BSI).A copy of the ISO 27001 certificate is available from Questionmark's websiteat https://www.questionmark.com/trust. We can also share a copy of our statement of applicability, subject to NDA. You can confirm the status of our certification on the BSI website at https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory by entering the certificate number, 668255.

G-Cloud

The UK Government G-Cloud is an initiative aimed at streamlining the process by which public-sector bodies procure cloud-based applications and solutions. Organisations approved to host on G-Cloud are government vetted and enable government associations to dramatically reduce the time spent procuring services and connect with suppliers that fit their needs in a much more effective, time efficient way.

Questionmark's G-Cloud listing covers Questionmark OnDemand within the latest iteration of the UK Government G-Cloud Framework, G-Cloud 11. Questionmark's G-Cloud Service ID is 920078550113152, and more information is available at https://www.digitalmarketplace.service.gov.uk/g-cloud/services/920078550113152

Cyber Essentials

The Cyber Essentials scheme is a key deliverable of the UK's National Cyber Security Programme. Cyber Essentials is a government-backed cyber security certification scheme that sets out a good baseline of cyber security suitable for all organisations in all sectors. You can confirm the status of our certification at https://ces.apmg-certified.com/PublicOrgLogin/Certificate.aspx?g=f59b3b90-72ad-44c8-8715-e855c345f2d6

Other accreditations and compliance with regulations

Questionmark is a Gold Microsoft partner and an SAP Platinum partner. Questionmark's US company, Questionmark Corporation is a GSA contract holder and is able to provide contractual assurance to hold data under HIPAA and FERPA regulations. Questionmark Corporation is also certified under FedRAMP and is compliant with the EU-U.S. Privacy Shield and Swiss-U. S. Privacy Shield.

Questionmark is committed to GDPR compliance across our OnDemand services and provides GDPR guidance and related assurances within contracts and documentation to help customers be compliant. Questionmark is also committed to compliance with U.S. privacy regulations, including the CCPA.

More detailed and the latest information on Questionmark's accreditations and compliance with regulations can be found at Questionmark's Trust Centre at https://www.questionmark.com/trust.

3. Data Centre

Questionmark hosts the OnDemand Service in a state-of-the-art Data Centre in Europe. The physical data security measures in place within Questionmark's Data Centre are certified to ISO 9001 Quality Management System and ISO 27001 Information Security Management System standards.

Questionmark uses a Data Centre that provides the following features and safeguards:

Physical security measures

The physical security of the building and servers are maintained by:

- 24-hour manned security & intruder/security breach alarms
- Smart Card access policies
- Internal and external CCTV systems

The data centre does not include signage that could identify it as a data centre.

Environmental monitoring

The Network Operation Centre (NOC) monitors alerts (visual, audible and via email) and engages the personnel at the data centre to resolve issues:

- 24 x 7 environmental monitoring systems
- Fire alarm status and FM200 fire suppression equipment
- N+1 redundant Heating Ventilation Air Conditioning (HVAC) system
- Controlled environment - room temperature 24°C +/- 2°C

Data Center Certifications

The Data Centre is compliant with:

- **ISO 9001 Quality Management System standard** – ISO 9001 is a widely implemented Quality Management System standard for providing assurance about an organization's ability to satisfy quality requirements. Certification against ISO 9001 provides independent third-party assurance by a licensed certification firm that the data centre meets specified requirements.
- **ISO 27001 Information Security Management System standard** – ISO 27001 is the recognized international standard for Information Security Management Systems, requiring that a company demonstrates a systematic approach to managing sensitive information and ensuring data security. Compliance with ISO 27001 provides independent third-party assurance by a licensed certification firm that the data centre meets specified information security requirements.

4. Network Security and Connections

Security on network

A summary of the security provided by the network infrastructure is:

- Internet traffic in and out of the Data Centre is encrypted using TLS v1.1 or higher.
- The service is protected by redundant firewalls
- Each server in the various tiers is protected by a host-level firewall
- A Bastion Host is used to allow system maintenance without damaging system security or integrity
- Antivirus technology is used, and is updated automatically as new signatures become available.

For a current report on the SSL/TLS configuration and certificate used by the OnDemand service, see https://www.ssllabs.com/ssldb/analyze.html?d=ondemand.questionmark.eu

Connections to the system

Participants/candidates and Administrators use a TLS 128- or 256-bit encrypted connection through their web browsers and enter the service via the firewall.

Questionmark Platform Administrators securely connect to the OnDemand service via RDP over VPN to a Bastion Host to perform platform maintenance.
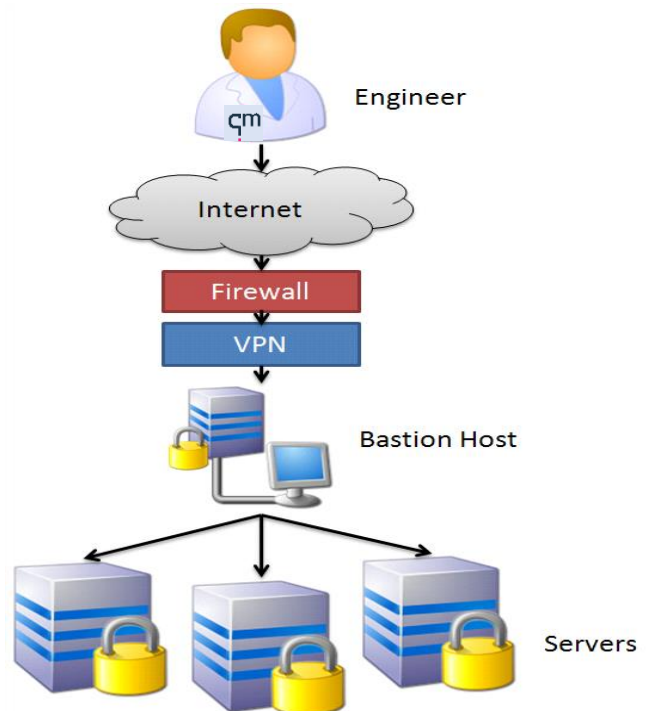
5. Access Control and Security within the OnDemand Application

The Questionmark™ OnDemand assessment management system enables trainers, educators and testing professionals to author, schedule, deliver, and report on surveys, quizzes, tests and exams.

Questionmark technologies have been designed from the ground up to be multi-tiered and scalable solutions. They include:

- Storing data (personally identifiable information, assessment content and results) safely and securely
- Minimizing possible attack surfaces

OnDemand uses authentication and authorization to control access and rights to/in the system. This includes:

- Administrators – they need to be registered on the system and will have to supply a username and password to enter
- Participants - they need to be registered in the system and scheduled to an assessment. Before they take an assessment, they will be asked to enter their username and password

Customer user management

Questionmark OnDemand allows you to define roles, each of which contains privileges into the system and to allocate people to one or more roles. These roles can have granular levels of access permission, based on role. As you can see by the screenshot below, new roles can be created with defined levels of access to topics and assessment content. Customers also have the option of using predefined roles if they choose too. This allows our customers to manage their users by the rule of least privilege and need to know.
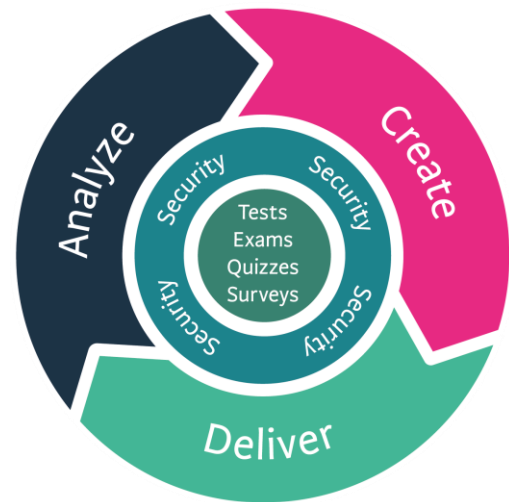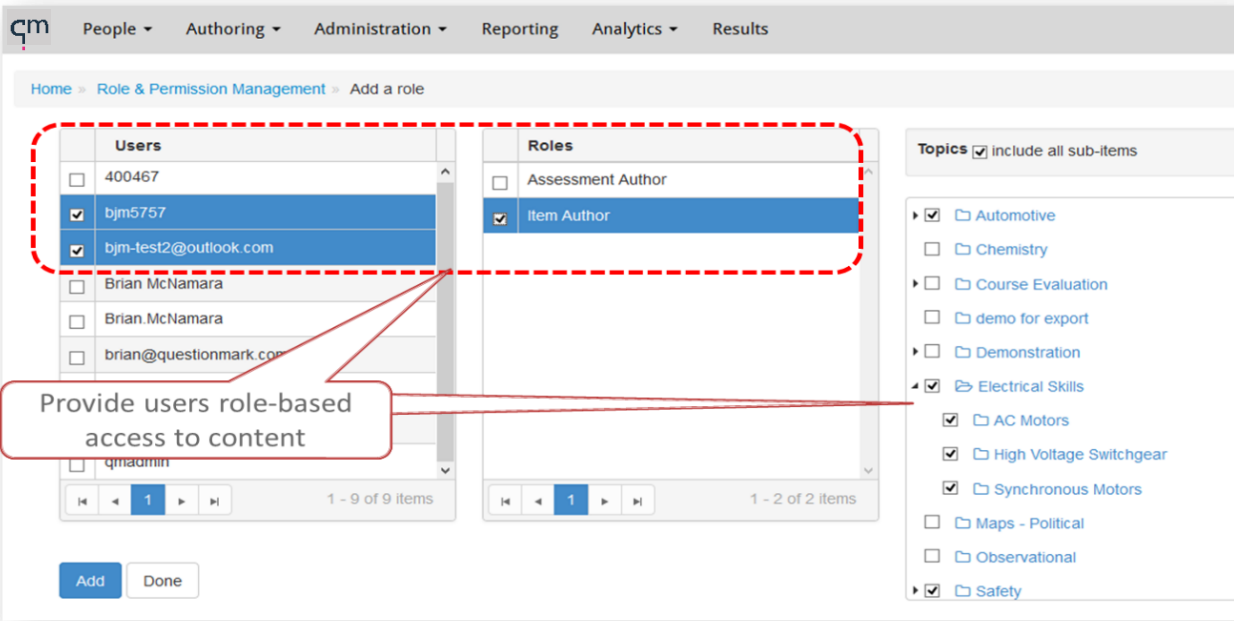
Questionmark OnDemand is provisioned with default roles including Assessment author, Item bank administrator, Item author, Monitor, Publisher, Reporter, Reviewer, Role manager, Scheduler, Test centre administrator and Translation manager and users can add and modify roles.

Authentication within Questionmark OnDemand Portal

When logging into the Questionmark portal directly, each customer defines a password policy including making settings for length and complexity of passwords, when they expire, how much delay is required before changing a password and how many previous passwords are checked to ensure a password is not re-used when changed. See below for screenshots of default password policy. Each field can be customized by role.
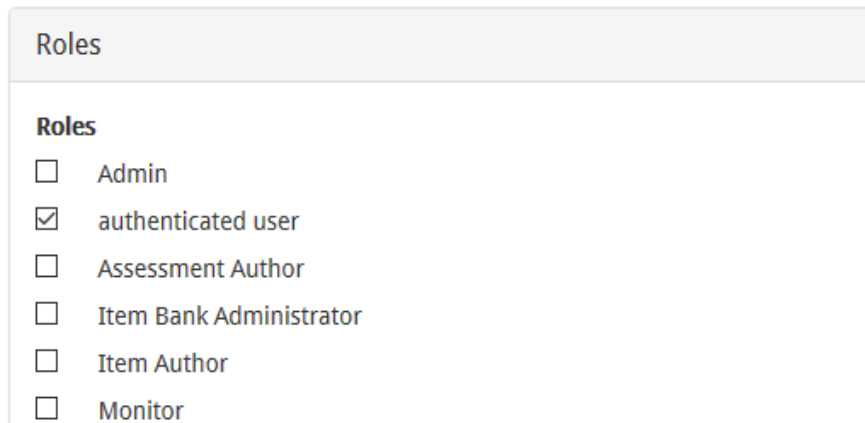
Expiration

Password Expiration

180

Password Expiration Warning

14

Additional access control features:

- Administrators can be forced to change password when they first login.
- Administrators can be locked out of the system with too many false attempts.
- All administrator interactions with the system can be logged.

Authentication via Single Sign-on

Questionmark OnDemand supports multiple methods for authentication of participants and administrators via Questionmark's APIs as illustrated below.

The following authentication methods are supported:

- Product-specific connectors including SAP LSO and LTI- compliant learning
- management systems such as Moodle and Blackboard
- Custom-built applications using web services API
- Standards-based integrations with authentication handled by 3rd-party applications using AICC and SCORM
- SAML 2.0

SAML 2.0

SAML permits secure authentication of Questionmark OnDemand users via your own identity provider and if your identity provider supports it can be configured to provide additional security, for example:

- Directory and discovery
- User/Group Management
- User-based provisioning
- Device registration
- Device access control
  - o Username and password
  - o Access Key
  - o Access Card

- o Fingerprint recognition
- o Retina recognition
- o Gesture recognition
- Single Sign-On (SSO) including Questionmark
- Self-Service Password Reset/Change/Unlock
- Sync to other data sources
- Security / Usage Reports
- Group-based access management / provisioning
- Application Proxy
- Self-Service Group and app Management/Self-Service application additions/ Dynamic Groups
- Multi-Factor Authentication system access
  - o Username and password
  - o Trusted device (Certificates)
  - o Phone Call to trusted number
  - o Text message to trusted number
  - o Application receives temporary code
  - o Geolocation of device

Device Access
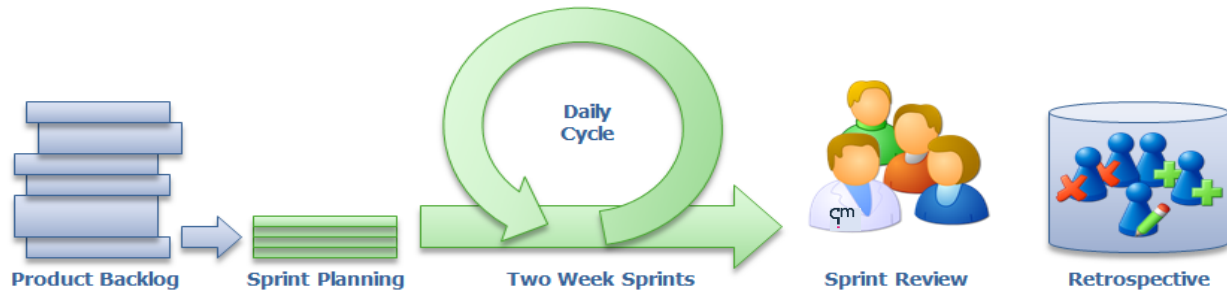
System Access via an Identity Provider (IDP)
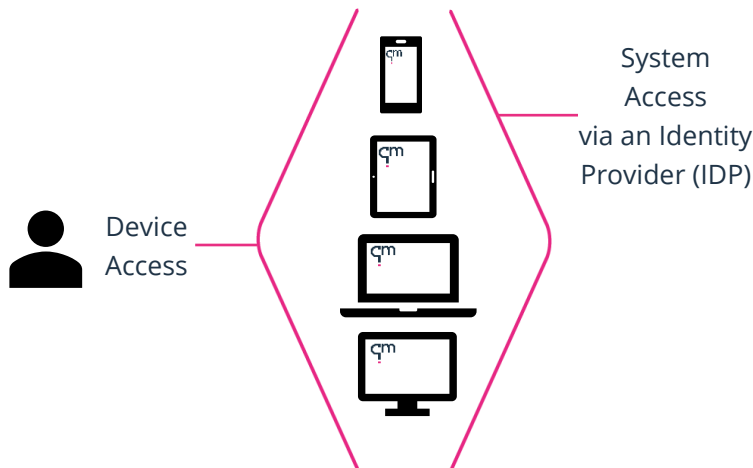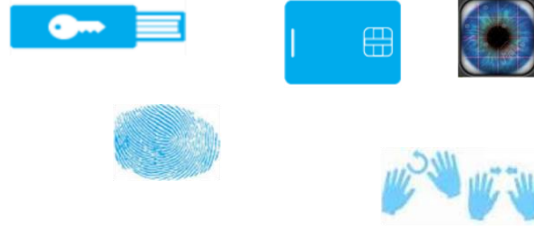
SSO to Questionmark

6. Application Development and Monitoring Security

Questionmark uses the Secure Development Lifecycle for Agile:

Questionmark uses the SCRUM/Agile software development methodology:

- The team pursues assigned tasks during two-week 'sprints'
- Tasks are prioritized and assigned by the Product Owner
- Quality Assurance teams test the development work on the OnDemand integration area (using automated, service layer, and black-and-white box testing) and do security testing.
- Once the QA team approves the system for release, it is passed to the Staging area where customers can test the environment before it goes into production.
- Once approved, the application is released to the production area for general use.
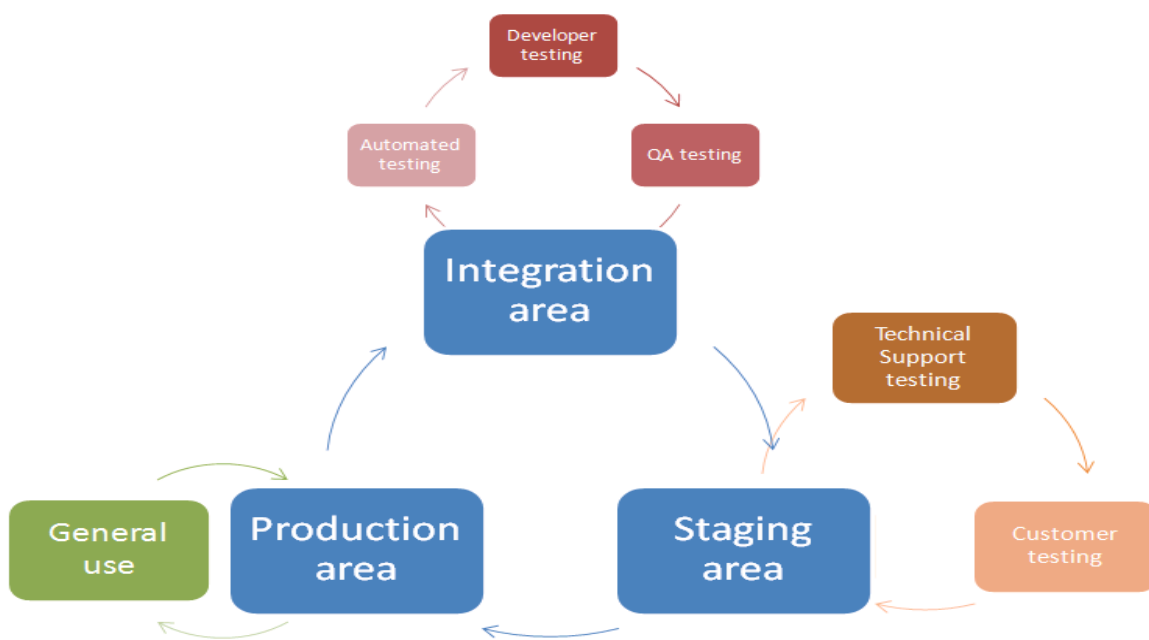
All developers are trained and coached to ensure coding follows best practice. This ensures the developers:

- Are up-to-date with the latest techniques
- Understand how to mitigate known issues
- Provide feedback to others about new/additional issues they have found

The development teams follow Agile SDL best practices with regards to building functionality and features. Common threats are mitigated through secure coding practices based on the work of the Open Web Application Security Project (http://www.owasp.org/).

The Quality Assurance teams utilize industry best practices to deliver thoroughly-tested applications at the end of each sprint. Questionmark believes in quality from the outset and because of this we use automated:

- Regression testing
- Build and deployment testing
- UI testing
- Service-level testing
- Unit tests

Application performance

Questionmark always tries to improve system performance to ensure that it continues to meet the requirements of our customers. We actively work with our customers to improve performance where we can. We hold quarterly performance reviews of our application to determine if and how performance can be improved.

Our performance testing is focused upon the delivery engine of the technology, where the greatest load on the system occurs with the ability to deliver hundreds of thousands of assessments to participants.

JMeter is used for our automated performance testing. It is used to benchmark performance tests daily and ensure changes do not negatively affect performance.

Our performance testing is focused upon simulating high load against a test system that closely matches our deployed infrastructure, combined with, a strategy of monitoring load on our live systems to validate our results.

Application monitoring

Servers are continuously monitored for downtime and designed to notify the Network Operations Centre for action to be taken immediately. The service is monitored from around the world to track performance and connect, processing and transfer times. For up-to-date details about the status of the OnDemand Service, please refer to: http://status.questionmark.com.

7. Data Security Policy

Questionmark has a comprehensive Data Security Policy in place that applies to all employees and a small number of authorized contractors (quasi-employees). Here is a summary of the policy regarding employees:

- Background checks are carried out on all new employees.
- Employees are required to:
  - Sign a confidentiality agreement
  - Commit to Questionmark's Data Security Policy
- Data Security training is given to each new employee.
- Data security and information security awareness briefings are given to all employees regularly.
- Questionmark's Information Security Officer is responsible for compliance and recording breaches if and when they occur.
- A password policy for all employees includes using 8+ characters, capitalization and numbers.
- All employees must pass annual tests on Questionmark's Data Security Policy.

As employees leave, procedures to remove access (including physical) to company data and equipment are carried out.

Accessing stored data:

- A limited number of employees in technical support and related areas can request access to customer areas to assist customers with modifying their installation of the application or troubleshooting issues. Any access to your account by an employee is logged and monitored.
- Questionmark keeps customer data strictly confidential and does not share it with third parties, nor use it for its own marketing purposes
- Questionmark uses a small number of sub-processors in the delivery of its service, including our ISO 27001 certified data centre. These sub-processors are bound by confidentiality restrictions including the EU Model Clauses and are carefully monitored by Questionmark.
- Unless required by law, Questionmark will not release customer data to government bodies. If a request is placed by a government body for access to customer data, Questionmark will only provide this data if its lawyers advise that it is mandatory to do so. Unless prohibited by law, Questionmark will consult or inform the customer prior to releasing data based on a government request.

8. Service Continuity

Continued running of the Questionmark OnDemand Service is important for us and our customers. We target a 99.9% uptime of our data centre. For up-to-date details about the uptime, please refer to: http://status.questionmark.com

Maintaining service continuity is a process of assessing threats, risks, and vulnerabilities and then managing these to maintain uptime and ensure continuation during minor and major events. Many of Questionmark's processes, procedures and redundant systems are maintained to achieve the highest uptime possible.

Redundancy

To ensure improved uptime and connectivity the Data Centre has:

- Carrier-neutrality
- On-site power generators
- Diesel-powered back-up generators in case of a power failure
- Dual independent power feeds, backed up by dual battery string Uninterrupted Power Supplies (UPS) systems (deployed as standard)
- Scalable architecture including multiple redundant core switches and routers
- All tiers load balanced. If a particular node fails, the other nodes will continue to function, taking up the extra processes without interrupting service.
- Virtual Dedicated Servers to run the tiers independently. The virtualization allows Questionmark to deploy rapidly in the case of a disaster or if the need to increase capacity arises.
- A self-healing fully redundant, high-speed local area network infrastructure (Fast Ethernet/Gigabit Ethernet) and wide area network.

Routine Maintenance - This is performed at low volume periods while the system is up, without disrupting service. Routine maintenance can cause slight reductions in service speed as we switch individual servers in the cluster in and out of the system, and we announce routine maintenance timings on our RSS feed to alert customers who might be concerned of this.

Scheduled downtime maintenance - Using redundancy features, most updates can be made without downtime. Very rarely, Questionmark will need to perform scheduled maintenance which requires the system to be offline for a short period of time. We target that this will happen no more than 4 times per year. We reserve a monthly window of the 3rd Saturday of each month from 10am GMT to 10pm GMT for such scheduled maintenance. Where

possible, Questionmark will provide notice several weeks in advance of a pending maintenance requiring downtime.

Emergency maintenance – Additionally, in the unforeseen case where Questionmark becomes aware of a serious event requiring immediate action, an emergency maintenance session may be scheduled. Questionmark will provide notice as soon as it becomes aware of the need for such a window.

Downtime

Using redundancy features, most updates can be made without downtime. However, users are notified of scheduled downtime several weeks in advance via email and RSS feeds. Further updates reminding customers of the scheduled downtime are also sent closer to the time. While Questionmark will not postpone updates, we are sensitive to our customers' needs and where possible we will minimize any potentially disruptive work.

Questionmark monitors the services globally 24 hours a day. Any unplanned downtime is recorded and analysed to understand why it occurred and if mitigation steps can be taken to limit the disruption. Questionmark will follow through with risk management planning to ensure that this type of unplanned downtime will not happen again.

Depending on the nature of the downtime, it is possible to offer customers the ability to indicate to participants that the service is unavailable. This is a feature within the application

To deal with the unlikely event of a service disruption, a Disaster Recovery Plan is in place to cover:

- **Data Backups**
  Questionmark makes hourly database backups.

- **Communications during a disruption**
  Questionmark maintains several geographically disperse systems to maintain communications with customers and employees, providing confidence that communications will still flow during a major outage. Communication systems that are not housed within Questionmark's OnDemand Data Centre include:
  - Questionmark's email system and Customer relationship management system
  - Questionmark's blog at http://questionmark.com/resources/blog/
  - Questionmark's twitter feeds http://twitter.com/questionmark/
  - Questionmark's OnDemand status at http://status.questionmark.com/

In the event of a significant business disruption, employees will be able to use third-party systems (such as Microsoft Teams, instant messenger, mobile phones, internal twitter feeds, etc.) and calling trees to cascade information down to customers and employees.

During a significant service disruption, employees will assess the best method to use and will keep customers informed as to the projected time to recover.

Recovery

Questionmark has developed high-availability models to ensure downtime/recovery time is minimized. Questionmark ensures that relevant staff and partners are engaged in a readiness plan for any disaster recovery event that is necessary. This is brought into effect as part of the Disaster Recovery Plans.

9. Customer Service and Notifications

Questionmark's goal is to provide a first-class customer experience. We provide extensive online documentation, including quick-start guides, manuals, white papers, best practice guides and communications from our customer support teams. Commercial and "how-to" information is provided by Questionmark's Customer Care teams and more detailed technical information is provided by Technical Support.

Prospective customers may call during working hours or email at any time to: support@questionmark.com . Questions are usually answered the same day.

A list of services available from Questionmark can be found on the following page.

Service Name	Description	Service Offering
Questionmark OnDemand	All of the services provided by people 24 x 7 to maintain the OnDemand service uptime.	Provided by Questionmark and/or its sub-contractors 24 x 7.
"Chat" Technical Support	Assistance provided to designated contacts using 24 x 7 browser text chat sessions and VoIP connectivity when helping to resolve issues.	Provided by Questionmark during regular working hours as standard and 24x7 for an additional fee.
1st Line Technical Support	Assistance provided by phone, email and chat to designated contacts to resolve technical issues that might result in resetting services, keeping people informed of service status, and answering questions as to where the answers could be found in the Questionmark manuals or knowledge base items.	Provided by Questionmark during regular working hours as standard and 24x7 for an additional fee.
2nd Line Technical Support	Assistance provided by phone, email and chat to designated contacts to resolve technical issues where answers could not be found in the manuals or knowledge base items.	Provided by Questionmark during regular working hours as standard and 24x7 for an additional fee.
3rd Line Technical Support	Fix technical issues with the OnDemand Services	Provided by Questionmark during regular working hours.
Participant Support	Any assistance provided by phone, email, chat sessions, etc. to the Participant to help them use any part of the Questionmark OnDemand Services and/or Products.	Available from Questionmark at an additional charge.
Proctor/Invigilator Support	Any assistance provided by phone, email, chat sessions, etc. to proctor/invigilators to help them with the proctoring/invigilation process including but not limited to the use of Questionmark OnDemand Service.	Available from Questionmark for an additional charge.
Consulting Support	Assistance with template creation and modification to change the look-and-feel of an assessment, assessment content import, content transformations, custom development, support of custom development, consulting services, training services, data format changes, etc.	Defined within a Statement of Work and delivered for a fee that depends on the scale of the work required.

Service Notifications	Questionmark uses several methods to keep customers informed of the OnDemand Service status. Service notifications available:
	• Service Status: http://status.questionmark.com/
	• Email notifications for:
	   ○ Maintenance windows
	   ○ Service outages
	• Twitter
	   ○ Service outages
		Provided by Questionmark 24 hours a day and 7 days a week.

Alert Systems

Questionmark has in place four alert systems:

- **Network Operations Centre**
  This team monitors and provides alerts related to:
    - Power issues and network connectivity
    - Resource/Processor/Disk utilization and Critical Errors (system alerts)

- **Worldwide Monitoring**
  Information from these monitoring stations is available from
  http://status.questionmark.com/. This is a worldwide system of monitoring devices
  that start assessments to check and provides alerts related to:
    - Resolve, connect, processing and transfer times

- **User reports**
  The Questionmark Technical Support team monitors anything related to the
  OnDemand service performance.
    - Email, phone, chat, etc.

- **Questionmark CERT**
  Questionmark has a Computer Emergency Response Team that monitors and
  provides alerts related to:
    - Security vulnerabilities reports from any source

Incident Response Procedures

An issue severity rating system determines how incidents are treated

Severity Level	Description of Impact	Response Level
Severity 1	An error isolated to the OnDemand service that renders the service inoperative or causes the service to fail catastrophically, e.g. major system impact, system outage or a data security issue. This issue must be resolved before the customer can use the service. All Severity 1 Issues have no workaround; the customer and Questionmark work closely together to resolve the error as soon as possible. Severity 1 issues are extremely rare and Questionmark escalates these issues to its highest priority.	• Initial Response Time (by email or callback) is within four (4) hours. • Maximum Time Between Updates (by email or callback or implementation in System) is four (4) hours during Normal Business Hours. • Email an alert to customers on Severity 1 alert list if widespread

Severity 2	An error isolated to the OnDemand service which causes a serious impairment to a critical feature of the service, but where overall functionality is not interrupted. Usually a workaround is available for this type of issue, but such is not always the case. Questionmark will resolve all Severity 2 issues as soon as possible.	- Initial Response Time (by email or callback) is within eight (8) hours. - Maximum Time Between Updates (by email or callback or implementation in System) is four (4) Hours during Normal Business Hours during the first three (3) business days and then updated as needed thereafter. - Email an alert to customers on Severity 2 alert list if widespread
Severity 3	An issue that causes the failure of a non-critical aspect of the Questionmark service and for which a satisfactory work-around already exists, but the presence of this issue will result in user dissatisfaction.	- Initial Response Time (by email or callback) is within two (2) business days during Normal Business Hours. - Maximum Time Between Updates (by email or callback or implementation in System) is two (2) business days for the first week and as needed thereafter. Solution is provided as part of a future release
Severity 4	An issue of minor significance. A slight variance exists between the product documentation and how the application actually performs.	- Initial Response Time (by email or callback) is within two (2) business days during Normal Business Hours. - Customer update is every five (5) business days, during the first month, and as needed thereafter. - Solution is provided as part of a future release at Questionmark's discretion.

Escalation and Information Flows

Questionmark's Technical Support team monitors incoming flows of information, the OnDemand service performance, and, if multiple issues are evident, prioritizes and escalates to resolve the most severe issues first. Questionmark's Technical Support team notifies customers and employees to keep them informed during any system degradation or outage. The information flow is as follows:
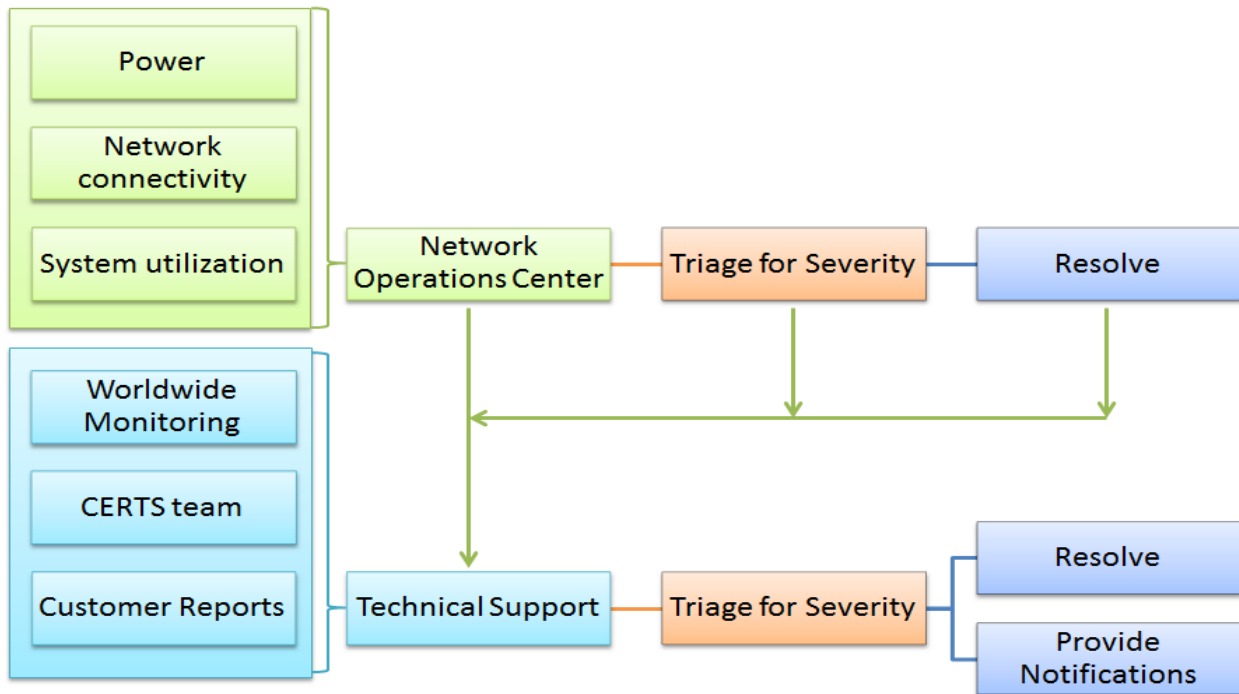
question mark

About Questionmark:

Questionmark provides a secure enterprise-grade assessment platform and professional services to leading organizations around the world, delivered with care and unequalled expertise. Its full-service online assessment tool and professional services help customers to improve their performance and meet their compliance requirements. Questionmark enables organizations to unlock their potential by delivering assessments which are valid, reliable, fair and defensible. Questionmark offers secure powerful integration with other LMS, LRS and proctoring services making it easy to bring everything together in one place. Questionmark's cloud-based assessment management platform offers rapid deployment, scalability for high-volume test delivery, 24/7 support, and the peace-of-mind of secure, audited U.S., Australian and European-based data centers.

Complete details are available at https://www.questionmark.com

Questionmark
United States
35 Nutmeg Drive
Trumbull, CT 06611
Tel: (800) 863-3950
Fax: (800) 339-3944
info@questionmark.com

Questionmark
United Kingdom
Moor Place, 1 Fore Street
London, EC2Y 9DT
Tel: +44 (0)20 7263 7575
Fax: +44 (0)20 7263 7555
info@questionmark.co.uk

Questionmark GmbH
Germany
Hopfenstr. 8,
80335 Munchen
Tel: + 49 (0) 89 220 61272
info@questionmark.de