

## Appendix 2 to Annex A: Technical Response

	<p>Question One – ISO 27001 Accreditation</p> <p>Pass/Fail Question</p>
<p>The primary outcome of this contract is the development of a feed management information system that can be demonstrated to have been developed by a supplier which holds ISO 27001 accreditation or equivalent in relation to their operation and the delivery of this project.</p> <p>Please attach certificated evidence to show that you are ISO 27001 (or equivalent) accredited or will commit to be accredited before the commencement of the contract or will be able to demonstrate an equivalency with the underlying criteria of ISO 27001.</p>	
<p><b>Supplier Response</b></p> <p>Esri UK holds ISO 27001 certification. Please see the attached certificate.</p> <p>The proposed solution is ArcGIS Online, which is developed by Environmental Systems Research Institute Inc (Esri) and has been granted a FedRAMP Tailored Low Authority to Operate (ATO). The security controls for this authorisation align with US National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 4) which maps to ISO27001 and ISO15408 controls. The controls and the mapping to ISO27001 is comprehensively documented in the ArcGIS Online Cloud Controls Matrix.</p>	



Question Two – Adaptability and Future Proofing  
– 5%

A solution whose requirements are defined in the Schedule 2 of the Contract Document is planned that is adaptable enough to facilitate multiple points of integration with existing and new systems, not all of which will be hosted close to, or built on the same software stack, for example the ability to integrate with Outlook, Objective ECM, Sharepoint and GIS systems.

Browser Support

As a minimum, we would expect:

- Desktop Applications
  - Latest Chrome and Chromium
  - Latest Firefox
  - I.E. 11 and above
  - Safari 10.11 and above
  
- Mobile & Tablet
  - iOS 10 Safari
  - iOS 10 Third Party Browsers (Chrome and Firefox)
  - Android 7.0 Chrome and default browsers and above

Please indicate how any solution would meet these requirements.

## Supplier Response

To satisfy the FSS's requirements for an adaptable and future-proofed system, Esri UK proposes a Feed Audit Management System that is built using Environmental Systems Research Institute Inc's ("Esri") ArcGIS Commercial-off-the-Shelf (COTS) functionality. The COTS products will be delivered by ArcGIS Online and ArcGIS mobile applications deployed and configured to meet the requirements of the GIS systems components of the Feed Audit Management System.

This approach supports the requirement for adaptability and future-proofing in the following ways:

- Approximately 90% of the requirements can be met by the COTS products out-of-the-box functionality, including configuration of those COTS products.
- [Redacted]The proposed COTS products are maintained and supported through a structured product development programme funded by 30% of Esri's annual revenues. Product upgrades (patches and major and minor versions) are included in the maintenance charges. Upgrade content is informed from a range of user, partner and industry input.
- Esri is fully supportive of open standards both for data and document interoperability, and for software and application interoperability. In the UK, we follow the seven open standards principles adopted by the Cabinet Office in the Open Standards Principles publication on the GOV.UK web site.

ArcGIS is built on web services, which allows excellent interoperability. All interfaces to ArcGIS are based on open standards and are accompanied by publicly documented Application Programming Interfaces (APIs). Esri continually scrutinises changes in architectural policy and advice from the Cabinet Office and the Government Digital Service, released in blogs or in updates to the Government Service Design Manual. Esri UK has frequently integrated Esri software with third-party business systems including asset management, business intelligence and CRM systems, making the GIS system a fully integrated part of the enterprise IT landscape.

The versatility of the ArcGIS platform, and the breadth of the analysis available, is already the cornerstone of collaboration between government bodies in Scotland.

[Redacted]

## Browser support

The following summarises the browser support for the ArcGIS products defined above access via web applications on the desktop:

Browser	ArcGIS Online	Web AppBuilder for ArcGIS 2D	Web AppBuilder for ArcGIS 3D <sup>(1)</sup>	Operations Dashboard for ArcGIS	Workforce for ArcGIS	Survey123 for ArcGIS
Chrome	Yes	Yes	Yes	Yes	Yes <sup>(5)</sup>	Yes
Firefox	Yes	Yes	Yes	Yes	Yes <sup>(6)</sup>	Yes

Safari	Yes	Yes <sup>(2)</sup>	Yes <sup>(3)</sup>	Yes	Yes <sup>(7)</sup>	Yes
Edge	Yes	Yes	Yes	Yes	Yes <sup>(8)</sup>	Yes
Internet Explorer 11	Yes	Yes	Yes	Yes <sup>(4)</sup>	Yes	Yes

(1) 3D application in Web AppBuilder for ArcGIS requires a desktop web browser that supports WebGL. The latest versions of the most common desktop browsers have WebGL built in.

(2) Safari 3 and later

(3) Safari 7.2 and later

(4) Compatibility View is not supported in IE11 by Operations Dashboard for ArcGIS

(5) Chrome 67.0 or later

(6) Firefox 60.0 or later

(7) Safari 11.0 or later

(8) Edge 42.0 or later

The following table summarises the browser support for the ArcGIS products defined above access via web applications on mobile devices.

Browser	Web AppBuilder for ArcGIS 2D	Operations Dashboard for ArcGIS	Workforce for ArcGIS
iOS Safari	Yes	Yes	Yes <sup>(1)</sup>
Chrome for Android	Yes	Yes	-
Android	-	Yes	Yes <sup>(2)</sup>

(1) iOS 6.0 or later running Safari

(2) Android 4.0 or later running Chrome 54.0 or later

The following summarises the mobile application support for the ArcGIS products defined above access via mobile applications on mobile devices:

Workforce for ArcGIS: The following operating systems (with minimum versions) are supported for the Workforce for ArcGIS mobile application:

- Android:
  - Android 4.2 (Jelly Bean) or later
  - Processor: ARMv7 or later, or x86
  - OpenGL ES 2.0 support
- iOS:
  - iOS 9 or later
  - iPhone and iPad

Survey123 for ArcGIS: The following operating systems (with minimum versions) are supported for the Survey123 for ArcGIS mobile application:

- Windows:
  - Windows 10 Pro and Windows 10 Enterprise (32 bit and 64 bit [EM64T])

- Windows 8.1, Windows 8.1 Pro, and Windows 8.1 Enterprise (32 bit and 64 bit [EM64T])
- Windows 7 Ultimate, Enterprise, Professional, and Home Premium (32 bit and 64 bit [EM64T]) SP1
- Windows Server 2012 Standard and Datacenter (64 bit [EM64T])
- Ubuntu:
  - 16.04 LTS (64 bit) or later
- Mac OSX
  - 10.12.6 (Sierra) or later
- Android:
  - 4.4 (KitKat) or later
- iOS
  - 10 or later (64 bit)

Survey123 Connect: The following operating systems (with minimum versions) are supported for Survey123 Connect:

- Windows:
  - Windows 10 Pro and Windows 10 Enterprise (32 bit and 64 bit [EM64T])
  - Windows 8.1, Windows 8.1 Pro, and Windows 8.1 Enterprise (32 bit and 64 bit [EM64T])
  - Windows 7 Ultimate, Enterprise, Professional, and Home Premium (32 bit and 64 bit [EM64T]) SP1
  - Windows Server 2012 Standard and Datacenter (64 bit [EM64T])
- Ubuntu:
  - 16.04 LTS (64 bit) or later
- Mac OS X:
  - 10.12.6 (Sierra) or later

Collector for ArcGIS: The following operating systems (with minimum versions) are supported for the Collector for ArcGIS mobile application:

- Android:
  - Android 4.2 (Jelly Bean) or later
  - Processor: ARMv7 or later, or x86
  - OpenGL ES 2.0 support
  - Precise location (GPS and network-based) support
- iOS:
  - iOS 8 or later
  - iPhone, iPad, iPod touch
- Windows 10 (tablet and PC):
  - Version 1511 or later
  - Long-Term Servicing Branch (LTSB) version 1607 or later



Question Three – SUPPORT AND MAINTENANCE  
– 10%

We will expect a minimum of 12 months support and maintenance for the delivered solution on a rolling basis commencing on the go live date.

This will include but not be limited to:

- Support on software upgrades throughout the period
- Support with work flow, GUI and reporting systems
- Technical advice to IT team

The core feed inspection hours shall be Monday – Friday 9am-5pm, and support shall be required during those hours through a variety of means, i.e. email, freephone telephone, instant message and web portal.

Please indicate how these requirements would be met.

### Supplier Response

With an Esri ArcGIS-based solution to the Feed Audit Management System, FSS will be using Commercial-off-the-Shelf (COTS) products from a leading software product company. Esri invests over 30% of its annual revenues on research and development giving the reassurance that the products stay robust, secure and contemporary.

#### Support and Maintenance including hours and access

FSS can rely on Esri UK’s Standard Support Service for efficient problem management and resolution when using ArcGIS COTS products. Our standard service is available for all software products with a current maintenance contract from the point of delivery.

The service is subject to the full Esri UK Standard Support Policy, which describes the support process in detail. We have summarised the policy below and attach the full policy with our proposal.

The service will allow FSS to log cases through their ‘My Esri’ account or to notify our Technical Support team of software or service faults via email at any time. FSS may also log cases by telephone Monday to Friday 09:00 to 17:30 UK time excluding English Bank Holidays. Cases will be logged and handled by our technical support team between 09:00 and 17:30.

For each case, a technical support analyst logs a standard set of information including a unique reference number. We use a Customer Relationship Management (CRM) system to log and monitor the status of all support cases. This enables us to monitor progress effectively on all outstanding cases.

The technical support analyst will review each new support case with FSS to assess its relative priority (using the definitions in the table below) and agree next steps for resolution. Our target response times and service levels are also shown in the table below.

Priority Level	Target Response Time	Symptom
P1	2 hours	The system is inoperable. No users can run the application.
P2	2 hours	A critical component of the system is inoperable, preventing use of the system for “full production”. However, other areas of the system can be used.
P3	4 hours	Elements of the system are not providing the functionality as expected, or there are Intermittent failures in system processing. In all cases, the system can be used for “full production” at that point in time.
P4	8 hours	Problem does not impact upon the use or productivity of the system but is frustrating to use, or there is an error in the documentation.

The technical support analyst will confirm the outcome of the case by email. Once logged, the CRM system places all support cases in a queue according to the agreed priority and assigns each case to the next available technical support analyst with the requisite area of expertise. The allocated analyst will use in-house systems to replicate the problem or access other technical resources to identify known problems and recommend workarounds.

To ensure FSS is kept fully informed of progress, the analyst will provide regular updates throughout the analysis and resolution period. FSS can also use their ‘My Esri’ account to view support cases, view old case histories and resolutions, request new cases and see the progress of bugs associated with their cases.

FSS will have a nominated Esri UK Customer Success Manager (CSM), who has overall responsibility for the relationship with Esri UK. The CSM will be notified of support cases and will oversee their successful resolution.

We resolve cases by:

- Assisting with the operation of the product
- Developing a workaround or working practices to avoid a problem
- Helping and enabling customers to develop their own workaround
- Logging enhancement requests for products or services.

If the analyst cannot resolve the case, it will be escalated (according to documented escalation procedures) to the Technical Support Manager who can draw in additional assistance from Esri UK product teams or Professional Services. If the problem still cannot be resolved, Esri UK will escalate the case to the Esri product teams.

Once FSS agrees the advice and guidance has resolved the problem, or the resolution is deferred to a future release, the analyst closes the case.

### Scope of support

The solution comprises ArcGIS COTS products either out-of-the-box or configured. All upgrades (patches, new releases and versions) are included in the annual support and

maintenance fee for all COTS products. This scope will cover workflows, GUIs and reporting components.

As a leading software vendor, Esri is in a strong position to maintain alignment with third party software vendors' new product versions even though this activity involves factors outside Esri's control. Esri has top-level relationships with industry software vendors, for example a global alliance partnership with Microsoft. This means Esri gains early sight of roadmaps and new software releases, often whilst they are still in beta testing. In turn, this allows Esri to schedule upgrade work into its own roadmap and development schedules. This typically results in product alignment and certification within months of the third-party software release.

If the solution evolves to include any customised elements, these can be supported using a Technical Support Agreement (TSA), which carries a fixed price for the period of the contract, provides 3rd line support for assistance, bug-fixes and enhancements and is delivered via the Technical Support team with an agreed SLA for response times.





Question Four – DATA UPLOAD, VERIFICATION AND MANAGEMENT – 10%

The Contractor must ensure that feed premises and inspection data provided by FSS is appropriately uploaded and maintained.

An example of the data held for a registered premises is contained within the file below:



Premises Record  
Example.xlsx

Please provide evidence that any solution can accommodate the following:

- Have the FSS master list of feed premises uploaded into a suitable premises database.
- Allow the officers to have access to historical inspection reports and records of actions taken for non-farm premises, currently stored by Local Authorities, and which will be extracted from current Local Authority systems and uploaded into appropriate shared document storage.

**Supplier Response**

[Redacted]



Question Five – MANAGEMENT AND REPORTING OF PREMISES RECORDS – 15%

FSS requires assurance that the solution has sufficient capacity and configuration for the effective management and reporting of registered feed premises information.

Please provide evidence that any system can accommodate the following as detailed in Schedule 2 of the Contract Document:

- Use the premises registration number as a unique identifier
- Record and amend the premises main feed activity code, and any additional codes in use by the premises.
- Record and amend the name of the feed business, address, postcode and contact detail fields including email.
- Where available, record and amend the holding number (the County Parish Holding number a premises may hold from Scottish Government, which is separate from the feed registration number) and grid reference of the premises.
- Record and amend if required the Local Authority area where the premises is located.
- Record and amend the industry assurance scheme membership details for the premises, including the name of the scheme, reference number, status and expiry date.
- Record and amend risk rating information, with a component based on the premises type, and a component to be determined during an inspection based upon the level of compliance.
- Change the allocation of Local Authority areas into regional groupings if necessary.
- Record and amend the details of authorised officers.
- Be able to create a new premises record.
- Perform batch deletion/ updating of old or unused records.
- Be able to search for personal details, including in free text and attachments.
- Maintain own parameters and data items.
- To be able to link business owners to different businesses.
- To be able to include intelligence-based links and additional information.
- Use a mapping function to display the location of premises and associated premises information

**Supplier Response**

[Redacted]



Question Six – MANAGEMENT AND REPORTING OF TASKS AND WORKFORCE – 15%

Please provide evidence that any solution can accommodate the following as detailed in Schedule 2 of the Contract Document:

- Allocate inspections to inspection staff, and have inspection staff notified of their allocated inspections
- Use the risk rating total under a set of defined rules to allocate an inspection frequency, and use this frequency to allocate a date of next inspection.
- Identify which officer has carried out an inspection, and which organisation that officer belongs to.
- Allow the spatial representation and interpretation of premises and inspection data.

**Supplier Response**

[Redacted]



Question Seven – INSPECTION ACTIVITY RECORDING AND REPORTING – 20%

Please provide evidence that any solution can accommodate the following as detailed in Schedule 2 of the Contract Document:

- Allocate categories to actions, to cover feed inspection visits, follow-up visits and sample only visits.
- Have a system of data entry that can be accessed in the field by users, on a variety of mobile devices, or at the office, which can store data offline in the event of having no connectivity.
- Create an inspection record with a unique reference for an official control visit
- Link the inspection record to the premises record and any other relevant documentation or information, such as location maps.
- Use preloaded templates for the recording of inspection results, which shows the areas to be inspected, and which can associate those activities under inspection with relevant legislation.
- Identify the areas of non-compliance identified during an inspection - for example pest control, cleaning and disinfection, storage, waste and hazardous substances, production, facilities, records. Fields to be determined, based upon the draft inspection form.
- Record if any representatives of other organisations accompany a visit.
- To be able to upload supporting documentation relating to an inspection visit
- Record the outcome of the inspection visit, in line with the reporting requirements for annual returns: revisits, advice given, sampling, other active interventions, voluntary closures, seizure or detention of product, suspension or revocation of approval/ registration, emergency prohibition, cautions, written warnings, improvement notices and prosecutions
- Give completion dates for follow-up actions and have prompts if these dates are not met.
- Be able to access records while away from the office where connectivity is available, if those records have not been assigned by a coordinator.
- To be able to add data fields to enable the recording of additional information such as the feed products used at a premises, animal species if relevant, and the approximate quantities.
- Be able to record if a sample has been taken, and the type of sample.
- Be able to record comments as free text.
- Produce pre-defined letter/ email templates, and link to Outlook to send.
- Be able to generate user defined reporting and management information dashboards to display current data.
- Be able to store generated documents (for example, pdf, jpeg, word) within the system, or to enable linking to those documents stored elsewhere in Sharepoint or Objective ECM.
- To have a reporting function that can view premises information and associated data on a graphical/map-based interface.

**Supplier Response**

[Redacted]



Question Eight – AUDITING AND SECURITY  
– 10%

Please provide evidence that any solution can accommodate the following as detailed in Schedule 2 of the Contract Document:

- To have configuration programs restricted to administrators.
- To be able to identify all entries/alterations by time, date and user.
- To be able to use codes within the database either individually or in groups to provide statistical and performance information.
- To be able to allow individual users to be set up to allow access to programs and specific fields as appropriate to their role and training.
- To be able to use the system with appropriate search parameters and report formats to enable extraction of any information that has been entered into the system.
- To be able to restrict permission for deletion of records.
- To have daily back-ups of the database, and sufficient back-ups are available to allow restoration if required.
- Be able to undertake audits of any amendments to the database entries.
- Identify records beyond retention period for enforcement information.
- Conforms to the National Cyber Security Centre principles  
<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

**Supplier Response**

ArcGIS Online is a secured, reliable geographic information system (GIS) delivered using the software-as-a-service (SaaS) model. ArcGIS Online services are elastic, available on demand, managed by Esri, and accessed by a client running on a wide range of platforms. They can be shared and used by many customers and offer security benefits.

The following features are engineered by Esri as part of the core ArcGIS Online software platform:

- Roles: Four ArcGIS Online organisation roles exist - user, publisher, custom and administrator.
- Users can add items, create web maps, share content, and participate in groups.
- Publishers are users that can publish hosted services from feature or tiled map data.
- Custom roles provide greater flexibility and granularity in assigning privileges to members of an organisation.
- Administrators use a web-based administration interface to manage users, groups, permissions, and organisation-wide security features:

- Easily configure TLS (Transport Layer Security) and HTTPS to enforce confidentiality of all information as it crosses the Internet.
- Restrict anonymous access to organisation data.
- Enterprise Logins: For authentication, enterprise logins are now supported via SAML 2.0 providing federated identity management. Developers can utilise OAuth 2-based APIs to manage user and app logins.
- Sharing: User-added content is only accessible by users and groups that users explicitly share content with. By default, items are private and only accessible by the user adding content.

ArcGIS Online administrators can use the organisation page to set up their ArcGIS Online organisation and website in the required way. The organisation page is divided into tabs to help the user perform a variety of administrative tasks:


- The Overview tab provides key information about an organisation such as subscription details, credit status, and messages about upcoming system maintenance.
- The Members tab is used to invite or add members to join an organisation, manage member accounts and information, and manage content in an organisation.
- Assign premium application licenses to specific members using the Licenses tab.
- Generate reports about site usage via the Status tab.
- The Settings tab is used to configure settings for the organisation, including map and scene settings, roles and privileges, and security settings.

[Redacted]

The ArcGIS Online portal application, Survey123 for ArcGIS web application, Web AppBuilder for ArcGIS, ArcGIS for Desktop and ArcGIS Pro can all be used to perform queries to understand who has created and changes data. These applications can also be used to query the hosted feature layers and related information and, where configured to do so, allow information to be extracted and downloaded. Depending upon the data model and attribute being maintained, domains on hosted feature services and calculated question types within surveys can be used to record codes against features. These codes can be used by the query tools in Web AppBuilder for ArcGIS, Operations Dashboard for ArcGIS, ArcGIS for Desktop and ArcGIS Pro to generate queries and reports to support statistics and performance information and to identify data that has been stored beyond retention periods (where date and time information has been recorded).

[Redacted]

	<p>Question Nine – TRAINING AND SUPPORTING DOCUMENTATION – 10%</p>
<p>The contractor will be required to provide the following:</p> <ul style="list-style-type: none"> <li>• Full project documentation, including database and entity relationship diagrams;</li> <li>• Full training manual, bespoke to the project configuration;</li> <li>• Full training manual, bespoke for the end user (not IT staff to include videos where required);</li> <li>• Full on-site training at our Aberdeen office for multiple end users;</li> <li>• Full on-site training at our Aberdeen office for a ‘train the trainer’ session;</li> <li>• Full on-site technical overview, training and handover for our IT team;</li> <li>• Detailed functional and technical specifications detailing the configuration of the project deliverables.</li> </ul> <p>Please indicate how these requirements would be met and provide FSS assurance that that the training will be of a sufficient standard to enable users to have the necessary skills to utilise the system.</p>	
<p><b>Supplier Response</b></p> <p>[Redacted]</p>	

 <p><b>Food Standards Scotland</b> For safe food and healthy eating</p>	<p>Question Ten – DISASTER RECOVERY AND BUSINESS CONTINUITY – 5%</p>
<p>The Contractor must ensure that suitable arrangements are in place for continued provision of service.</p> <p>The Contractor shall have robust and tested Business Continuity and Disaster Recovery plans, policies and procedures in place in respect to any applicable Services offered under this Framework Agreement. These plans and procedures must be auditable and available upon request by FSS. The contractor should describe their BCDR process in relation to the delivery of this exercise.</p>	



ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP –LOW IMPACT–
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP security control requirements.  ArcGIS Online cloud Infrastructure providers ensure their business continuity plans align with ISO 27001 standards.	X	X	Clause 5.1(h) A.17.1.2 A.17.1.2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	ArcGIS Online does contingency plan and incident response plan testing at a minimum of annually in alignment with FedRAMP Tailored Low requirements.  ArcGIS Online's cloud infrastructure providers business continuity policies, plans, and processes are developed and tested in alignment with ISO 27001 standards.	X	X	A17.3.1	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	ArcGIS Online uses cloud infrastructure providers whose datacenters comply with industry standards (such as ISO 27001) for physical security and availability.	X		A11.2.2, A11.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)
Business Continuity Management & Operational Resilience Documentation	BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Information system documentation is made available internal to ArcGIS Online personnel through the use of Esri's Intranet site. For security and operational reasons, Esri does not provide internal operations documentation to customers. For best practice security implementation guidance for customer organizations in ArcGIS Online, see: <a href="https://doc.arcgis.com/en/trust/security/arcgis-online-best-practices.htm">https://doc.arcgis.com/en/trust/security/arcgis-online-best-practices.htm</a> . There are also detailed user guides available in the online help section for ArcGIS Online: <a href="http://doc.arcgis.com/en/arcgis-online/">http://doc.arcgis.com/en/arcgis-online/</a>	X		Clause 9.2(g) A12.1.1	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 SA-5
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Cloud infrastructure provider environmental controls have been implemented to protect the data center (complying with ISO 27001) including:  -Temperature control -Heating, Ventilation and Air Conditioning (HVAC) -Fire detection and suppression systems -Power Management systems	X		A11.1.4, A11.2.1 A11.2.2	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Windows Azure services' equipment is placed in environments which have been engineered to be protected from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquakes, and electrical interference.  AWS data centers incorporate physical protection against environmental risks. AWS services provide customers the flexibility to store data within multiple geographical regions as well as across multiple Availability Zones. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones.	X		A11.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Cloud infrastructure providers ensure continuity of operations during equipment maintenance. If an upgrade of ArcGIS Online requires an outage window, customers will be notified ahead of time.	X		A11.2.4	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	The cloud infrastructure providers' data centers have 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery.	X		A.11.2.2, A.11.2.3, A.11.2.4	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: <ul style="list-style-type: none"> <li>- Identify critical products and services</li> <li>- Identify all dependencies, including processes, applications, business partners, and third party service providers</li> <li>- Understand threats to critical products and services</li> <li>- Determine impacts resulting from planned or unplanned disruptions and how these vary over time</li> <li>- Establish the maximum tolerable period for disruption</li> <li>- Establish priorities for recovery</li> <li>- Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption</li> <li>- Estimate the resources required for resumption</li> </ul>	ArcGIS Online cloud infrastructure providers perform business impact analysis (BIA) meeting ISO 27001 standards requirements. Customers may view infrastructure and application status information on the following dashboards:  AWS: <a href="http://status.aws.amazon.com">http://status.aws.amazon.com</a> MS Azure: <a href="http://www.windowsazure.com/en-us/support/service-dashboard/">http://www.windowsazure.com/en-us/support/service-dashboard/</a> ArcGIS Online: <a href="http://status.arcgis.com">http://status.arcgis.com</a>	X	X	A.17.1.1 A.17.1.2	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3

ArcGIS Online Cloud Controls Matrix (CCM) Answers

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	Supplier Relationship		Scope Applicability	
				Service Provider	Tenant / Consumer	ISO/IEC 27001:2013	FedRAMP --LOW IMPACT--
Business Continuity Management & Operational Resilience Policy	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	ArcGIS Online's cloud infrastructure providers have developed Business Continuity documentation that align with ISO 27001 and FedRAMP Moderate Requirements.	X		Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure. ArcGIS Online provides customers with the ability to delete their data; however it is the customer's responsibility to manage data retention to their own requirements. A KBA describing backing up customer data is available at: <a href="https://support.esri.com/en/technical-article/000011795">https://support.esri.com/en/technical-article/000011795</a>	X	X	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1 A.8.2.3	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-9

[Redacted]