Programme Management Planning Report

Rural Payments Agency

Rural Payments Agency

Assessment dates	24/10/2022 to 24/10/2022 (Please refer to Appendix for details)
Assessment Location(s)	Reading (000) - Remote
Report author	[redacted]
Assessment Standard(s)	ISO/IEC 27001:2013

making excellenc

Table of contents

Executive summary

The programme management has been completed and communicated with the client. It reviewed the durations and sampling plan. There were inconsistencies noted by the assessor (and the client) whereby sampling could be of any duration from 1 to 3 days and either annually, every 2, or every 3 years. The following should be noted:
- Centralised processes are sampled at the Reading office and should not be re-sampled at satellite offices.
- All satellite branch offices follow the same processes with the same output.

The sampling and associated visit plans have been changed accordingly. The 3-year plan redesigned to afford more clarity.

The visits for 2023 have been booked and include:
- Reading
- Exeter
- York
- Crewe

The programme management activity included:
- Meeting with the clients representative using MS Teams
- Review of data held by BSI relating to the client and locations
- Review of locations durations and sampling
- Review of client complexity and assessment duration calculations
- Confirm and communicate the updated audit duration with the client
- Review certification assessment programme
- Communication and working with the BSI Client Planning Advisors to adjust booked visits
- Submission of workflows to ensure that the new sampling cycle is implemented

Changes in the organization since last assessment

There is no significant change of the organization structure and key personnel involved in the audited management system.

No change in relation to the audited organization's activities, products or services covered by the scope of certification was identified.

There was no change to the reference or normative documents which is related to the scope of certification.

Assessment objective, scope and criteria

The objective was to produce a programme management plan for visits in 2023 and review the sampling of sites.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria:
- ISO 27001:2013
- Rural Payments ISO 27001:2013 information security management system documentation

Assessment participants

Name	Position	Opening meeting	Closing meeting	Interviewed (processes)
[redacted]	Compliance and Risk Lead	X	X	X
[redacted]	Compliance Analyst	X	X	X
[redacted]	Security Advisor	X	X	X

Assessment conclusion

BSI assessment team

Name	Position
[redacted]	Team Leader

Assessment conclusion and recommendation

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team concludes based on the results of this audit that the organization does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continues to achieve its intended outcomes.

The Rural Payments Agency are recommended for continued certification to ISO 27001:2013 and has been found in general compliance with the audit criteria as stated in the above-mentioned audit plan.

Use of certification documents, mark / logo or report

The use of the BSI certification documents and mark / logo is effectively controlled.

Findings from this assessment

Registration

Client details
The client contact details and assessor code requirements are confirmed to be correct.

Scope
Head office
- RURAL -0047532415-000 Reading

Satellite offices (Sampling)
- RURAL -0047532415-001 Carlisle:
- RURAL -0047532415-002 Newcastle Upon Tyne:
- RURAL -0047532415-003 Exeter
- RURAL -0047532415-004 Workington
- RURAL -0047532415-005 York
- RURAL -0047532415-006 Worcester
- RURAL -0047532415-007 Crewe
- RURAL -0047532415-008 Cambridge
- RURAL -0047532415-009 Leeds
- RURAL -0047532415-010 Nottingham

Client preference

The client prefers all audits to be preform remotely as there is a hybrid working system whereby home working is the normal practice..

Certificate
The receipt and administration of the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), including the detection and investigation of fraud under CAP schemes, and the provision of traceability of cattle and associated activities in accordance with the Statement of Applicability version SPOL V2.0 dated October 2021.The client is the paying agency for the EU's Common Agricultural Policy (CAP) schemes in England. Pays out over [redacted] each year to farmers, traders and land owners; makes payments on behalf of Natural England; and manages over 40 schemes.

Statement of Applicability
-All controls are applicable

Certificate details
- Original Issue date 05/08/2015
- Latest revision date: 03/11/2021
- Expiry date 04/08/2024

Risk profile

Review of ISO 27006 duration:
- Process complexity = 1
- Type of business = 1
- Information confidentiality= 2
- IT Infrastructure= 2
- Availability = 1
- Development: 2
- Total employees across 11 sites: circa ~2500

The 3-year cycle required:
- 5 days per annum continuing assessment visit
- 1 day programme management prior to recertification
- 9 days recertification (Recertification Option 2)

Continuing Assessment Visits
- Reading: 2 days per annum
- Branch offices: 3 sampled annually (1 day at each site)

Recertification
- Reading: 4 days
- Branch Offices: 5 sampled (1 day at each site)

Notes:
1. Above includes required planning and preparation time at 30% of audit duration.
2: Centralised services at Reading includes: IT, HR, Supplier Management, Overall delivery of services
2. Visit cycles may be subject to change as a result of organisational or scope changes and will be reconfirmed as necessary at each assessment visit.

Visits

RURAL - 0047532415	Location	No in Scope	Current Visit Frequency	New Visit Frequency	Last visit	Next Visit	Booked Y/N	Assessor	Recert Year	Assessor
000	Reading	215	2 days annually	2 days annually	11/05/2022	10/05/2023	Y	[redacted]	03/06/2022 (4 days)	[redacted]
001	Carlisle	283	3 days every 3 years	1 day every 3 years	20/05/2022	Due 2025	N			
002	Newcastle	542	2 days annually	1 day every 3 years	13/09/2022	Due 2025	N			
003	Exeter	235	1 day every 3 years	1 day every 3 years	23/06/2020	04/09/2023	Y	[redacted]		
004	Workington	450	1 day every 3 years	1 day every 3 years	04/06/2019	07/02/2024	Y	[redacted]		
005	York	277	1 day annually	1 day every 3 years	01/07/2020	10/10/2023	Y	[redacted]		
006	Worcester	180	1.5 days annually	1 day every 3 years	02/02/2021	Due 2024	N			
007	Crewe	138	3 days every 3 years	1 day every 3 years	22/02/2021	09/10/2023	Y	[redacted]		
008	Cambridge	48	1 day every 3 years	1 day every 3 years	03/10/2022	Due 2025	N			
009	Leeds	67	2 days every 3 years	1 day every 3 years	18/11/2021	Due 2024	N			
010	Nottingham	82	3 days every 3 years	1 day every 3 years	09/02/2022	Due 2025	N			
Total under scope		~2500								

Next visit objectives, scope and criteria

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to verify that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organization's management system; that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organization's specified objectives as applicable with regard to the scope of the management standard; to confirm the ongoing achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria:
- ISO 27001:2013
- Rural Payments Agency ISO 27001:2013 information security management system documentation

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organization within 30 days of an agreed visit date. It is a condition of registration that a deputy management representative be nominated. It is expected that the deputy would stand in should the management representative find themselves unavailable to attend an agreed visit within 30 days of its conduct.

Next visit plan

Date	Auditor	Time	Area/process
10/05/2023	[redacted]	09:00	Opening meeting: administration, business and ISMS changes, and previous report review
		09:30	Leadership: Top management interview, ISMS policy, objectives.
		10:00	Context: interested parties and scope
		10:30	Break from screen
		10:45	Planning/Operation: risk management, and Statement of Applicability
		11:30	Performance Evaluation and Improvement: Internal audit and corrective action, security incidents, monitoring and measurement, and management review (Clauses 9 & 10)
		12:30	Lunch
		13:15	IT (A.8 & A.9))
			IT (A.12, A.13)
		15:00	Interim Meeting
11/05/2023	[redacted]	09:00	Supplier relationships (A.15)
		10:00	Legislation (A.18)
		10:30	Break from screen
		10:45	Security incident management (A.16)
		11:30	Security awareness sampling: CPAT/GIS
		12:30	Lunch
		13:15	Security awareness sampling: RDT/Farm Inspections
		14:15	Contingency and review ISO 27001:2022 progress
		1500	Closing meeting followed by report production

Site Sampling 2023			
Date	**Auditor**	**Time**	**Area/process**
04/09/2023	[redacted]		Exeter
09/10/2023	[redacted]		Crewe
10/10/2023	[redacted]		York
This agenda to be implemented at all sites.		09:00	Opening meeting: administration, business and ISMS changes, and previous report review
		09:30	Local management system: context, risk assessment, internal audit, corrective action, feed in to management review
		11:00	Break from screen
		11:15	Security aspects of business continuity security
		12:15	Lunch
		13:00	RDT
		13:30	Farm Inspections
		14:00	CS Applications and Claims
		14:30	Data & Analysis
		15:00	Closing meeting followed by report production

Appendix: Your certification structure & ongoing assessment programme

Scope of certification

IS 619358 (ISO/IEC 27001:2013)

Scope: The receipt and administration of the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), including the detection and investigation of fraud under CAP schemes, and the provision of traceability of cattle and associated activities in accordance with the Statement of Applicability version SPOL V2.0 dated October 2021.

Assessed location(s)

The audit has been performed at Central Office.

Reading / IS 619358 (ISO/IEC 27001:2013)

Location reference	**0047532415-000**
Address	Rural Payments Agency 21-23 Valpy Street Reading RG1 1AF United Kingdom
Visit type	Programme Management
Assessment number	3449241
Assessment dates	24/10/2022
Deviation from audit plan	No
Total number persons within scope of certification across ALL locations	2500
Total number of persons within scope of certification at THIS location	2500
Scope of activities at the site	Main certificate scope applies.
Assessment duration	1 day(s)

Certification assessment programme

Certificate number - IS 619358
Location reference - 0047532415-000

		Audit1	**Audit2**	**Audit3**
Business area/location	**Date (mm/yy):**	05/2022	05/2023	05/2024
	Duration (days):	5	5	9
Opening meeting: administration, business and ISMS changes, and previous report review		X	X	X
Context: interested parties and scope		X	X	X
Leadership: Top management interview, ISMS policy, objectives.		X	X	X
Planning/Operation: risk management, and Statement of Applicability		X	X	X
Performance Evaluation and Improvement: Internal audit and corrective action, security incidents, monitoring and measurement, and management review (Clauses 9 & 10)		X	X	X
Support: resource and competence, roles and responsibilities, training and awareness, and communication and Documented Information (Clause 7)				X
Human Resources (A.7)		X		X
IT (A.8 & A.9))		X	X	X
IT (A.10)				X
IT (A.12, A.13)		X	X	X
Development (A.14)		X		X
Site tour: physical and environmental security (A.11				X
Supplier relationships (A.15)			X	X
Security incident management (A.16)			X	X
Information Aspects of Business Continuity Management (A.17)		X		X
Legislation (A.18)			X	X
Security awareness sampling: CPAT/GIS		X	X	X
Security awareness sampling: RDT/Farm Inspections		X		X
Security awareness sampling: CS Apps & Claims/Data & Analysis			X	X
Recertification: Reading 4 days				X
Programme management (1 day off-site)				X

		Audit1	Audit2	Audit3
Business area/location	**Date (mm/yy):**	05/2022	05/2023	05/2024
Site sampling (1 day at each site)		X	X	X
Carlisle		X		X
Newcastle		X		
Exeter			X	
Workington				X
Crewe			X	
York			X	
Cambridge		X		
Leeds				X
Nottingham		X		X
Opening meeting: administration, business and ISMS changes, and previous report review		X	X	X
Local management system: context, risk assessment, internal audit, corrective action, feed in to management review		X	X	X
Physical security: virtual				X
Security aspects of business continuity security		X	X	X
RDT		X	X	X
Security awareness sampling		X	X	X
Farm Inspections		X	X	X
CS Applications and Claims		X	X	X
Data & Analysis		X	X	X

ISO 27001:2022 – Summary of Changes

Number of controls

The number of controls in the new version 2022 has been reduced from 114 controls in 14 clauses in the 2013 edition to 93 controls in 4 clauses in the 2022 edition.

Areas of controls

The controls are now categorised into four areas
- Organisational controls
- People controls
- Physical controls
- Technological controls.

Control guidance

The Guidance on controls has improved and each control now has a Purpose: Statement explaining the control (Attributes).

Attributes

The controls now also have five types of ‘attribute’ to make them easier to categorise:
- Control type (preventive, detective, corrective).
- Information security properties (confidentiality, integrity, availability)
- Cybersecurity concepts (identify, protect, detect, respond, recover)
- Operational capabilities (governance, asset management, etc.)
- Security domains (governance and ecosystem, protection, defence, resilience)

Which controls have changed?

The control objective for a group of controls has been replaced by a “purpose” element and to enhance the risk mitigation, assessment and treatment process, the concept of “attributes to controls” has been introduced.
There are now only 93 controls with:
- 11 new controls reflecting the current information security, physical security and cyber security categories
- 24 merged controls,
- 58 controls updated for clarification.

New controls

The scope of ISO/IEC 27002:2022 now lists 11 new controls. These are:

- Threat intelligence – understanding attackers and their methods in the context of your IT landscape.
- Information security for the use of cloud services – the introduction through operation to exit strategy regarding cloud initiatives now needs to be considered comprehensively.
- ICT readiness for business continuity – the requirements for the IT landscape should be derived from the overall business processes and the ability to recover operational capabilities.
- Physical security monitoring – the use of alarm and monitoring systems to prevent unauthorised physical access has gained more emphasis.
- Configuration management – hardening and secure configuration of IT systems.
- Information deletion – compliance with external requirements, such as data protection deletion concepts needs to be implemented.
- Data masking – using techniques that mask data, such as anonymisation and pseudonymisation, to bolster your data protection.
- Data leakage prevention – taking steps to help prevent sensitive data from being leaked.
- Monitoring activities – your organisation should be monitoring network security and application behaviour to detect any network anomalies.
- Web filtering – helps prevent users from viewing specific URLs containing malicious code.
- Secure coding – using tools, commenting, tracking changes, and avoiding insecure programming methods are ways to ensure secure coding.

Annex A includes guidance for the application of attributes
Annex B: Provides cross reference between the 2013 and 2022 versions

List of Controls

5 Organisational controls

5.1 Policies for information security
5.2 Information security roles and responsibilities
5.3 Segregation of duties
5.4 Management responsibilities
5.5 Contact with authorities
5.6 Contact with special interest groups
5.7 Threat intelligence – new
5.8 Information security in project management
5.9 Inventory of information and other associated assets – change
5.10 Acceptable use of information and other associated assets – change
5.11 Return of assets
5.12 Classification of information
5.13 Labelling of information
5.14 Information transfer
5.15 Access control
5.16 Identity management
5.17 Authentication information – new 5.18
Access rights – change
5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the ICT supply chain – new
5.22 Monitoring, review and change management of supplier services – change
5.23 Information security for use of cloud services – new
5.24 Information security incident management planning and preparation – change
5.25 Assessment and decision on information security events
5.26 Response to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
5.29 Information security during disruption – change
5.30 ICT readiness for business continuity – new
5.31 Identification of legal, statutory, regulatory and contractual requirements
5.32 Intellectual property rights
5.33 Protection of records
5.34 Privacy and protection of PII
5.35 Independent review of information security
5.36 Compliance with policies and standards for information security
5.37 Documented operating procedures

6 People controls

6.1 Screening
6.2 Terms and conditions of employment
6.3 Information security awareness, education and training
6.4 Disciplinary process
6.5 Responsibilities after termination or change of employment
6.6 Confidentiality or non-disclosure agreements
6.7 Remote working – new
6.8 Information security event reporting

7 Physical controls

7.1 Physical security perimeter
7.2 Physical entry controls
7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring
7.5 Protecting against physical and environmental threats
7.6 Working in secure areas
7.7 Clear desk and clear screen
7.8 Equipment siting and protection
7.9 Security of assets off-premises
7.10 Storage media – new
7.11 Supporting utilities
7.12 Cabling security
7.13 Equipment maintenance
7.14 Secure disposal or re-use of equipment

8 Technological controls

8.1 User endpoint devices – new
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion – new
8.11 Data masking – new
8.12 Data leakage prevention – new
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities
8.17 Clock synchronization
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Network controls
8.21 Security of network services
8.22 Web filtering – new
8.23 Segregation in networks
8.24 Use of cryptography
8.25 Secure development lifecycle
8.26 Application security requirements – new
8.27 Secure system architecture and engineering principles – new
8.28 Secure coding
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit and testing – new

Definitions of findings:

Nonconformity:

Non-fulfilment of a requirement.

Major nonconformity:

Nonconformity that affects the capability of the management system to achieve the intended results. Nonconformities could be classified as major in the following circumstances:

- If there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- A number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

Minor nonconformity:

Nonconformity that does not affect the capability of the management system to achieve the intended results.

Opportunity for improvement:

It is a statement of fact made by an assessor during an assessment, and substantiated by objective evidence, referring to a weakness or potential deficiency in a management system which if not improved may lead to nonconformity in the future. We may provide generic information about industrial best practices but no specific solution shall be provided as a part of an opportunity for improvement.

How to contact BSI

Visit the BSI Connect Portal, our web-based self-service tool to access all your BSI assessment and testing data at a time that's convenient to you. View future audit schedules, submit your corrective action plans and download your reports and Mark of Trust logos to promote your achievement. Plus, you can benchmark your performance using our dashboards to help with your continual improvement journey.

Should you wish to speak with BSI in relation to your certification, please contact your local BSI office – contact details available from the BSI website:

https://www.bsigroup.com/en-GB/UK-office-locations/

Notes

This report and related documents are prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report. If you wish to distribute copies of this report external to your organization, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organization and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

This audit was conducted through document reviews, interviews and observation of activities. The audit method used was based on sampling the organization's activities and it was aimed to evaluate the fulfilment of the audited requirements of the relevant management system standard or other normative document and confirm the conformity and effectiveness of the management system and its continued relevance and applicability for the scope of certification.

As this audit was based on a sample of the organization's activities, the findings reported do not imply to include all issues within the system.

Regulatory compliance

BSI conditions of contract for this visit require that BSI be informed of all relevant regulatory non-compliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-compliance or incidents occurring after this visit will be notified to the BSI client manager as soon as practical after the event.