Assessment Report

Reward Gateway (UK) Ltd

Assessment dates	06/06/2018 to 08/06/2018 (Please refer to Appendix for details)
Assessment Location(s)	London (000)
Report author	Simon Evans
Assessment Standard(s)	ISO/IEC 27001:2013

Table of contents

Executive summary

In line with the Information Security strategy of the organisation and the intended results of the Management System, particularly with regard to the areas assessed at this assessment, it was identified that, the management system has demonstrated that it is designed to support this strategic direction and deliver intended results.

The organization was noted to be continuing to maintain and improve the processes effectively, with particular regard to positive areas:
- Strong leadership
- Robust internal audits against standard
- Training and awareness
- New data processing agreements with existing suppliers in line with GDPR
- Log record availability within Splunk

There are however further possible opportunities to improve and reduce risks, relating to achieving the intended results regarding:
- The protection of assets in the communications room from environmental risk
- Maintenance of legal requirements
- Improvement of business continuity testing

I would like to thank all the audit participants for their assistance and co-operation which enabled the audit to run smoothly and to schedule.

Changes in the organization since last assessment

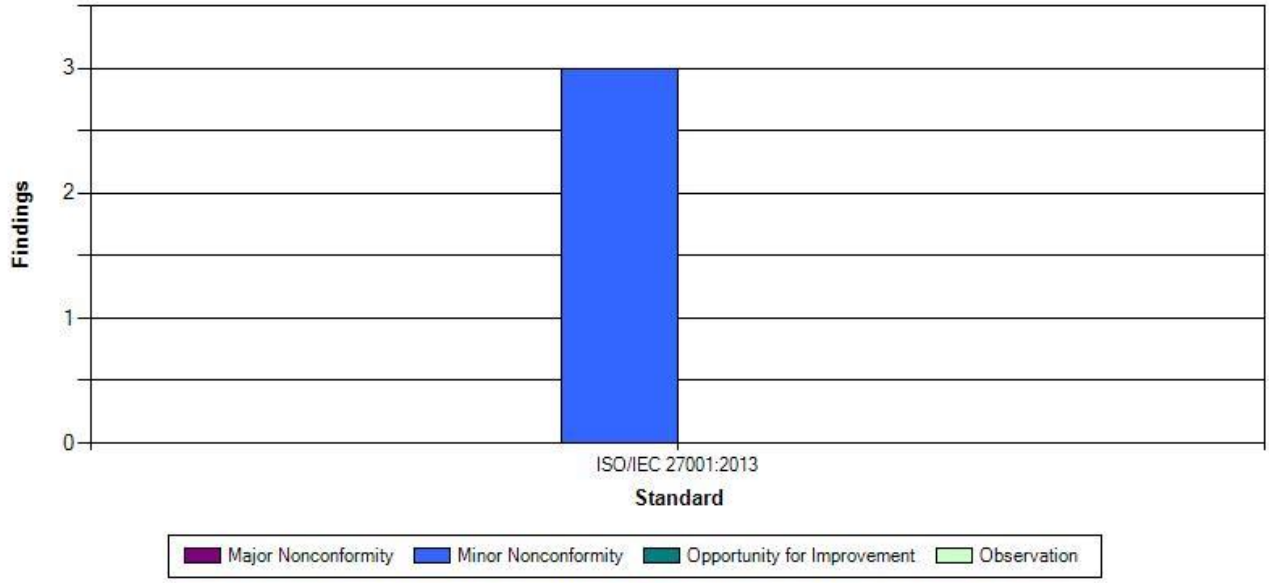
There is no significant change of the organization structure and key personnel involved in the audited management system.

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.

NCR summary graphs

Which standard(s) BSI recorded findings against



Your next steps

NCR close out process

There were no outstanding nonconformities to review from previous assessments.

3 minor nonconformities requiring attention were identified. These, along with other findings, are contained within subsequent sections of the report.

A minor nonconformity relates to a single identified lapse, which in itself would not indicate a breakdown in the management system's ability to effectively control the processes for which it was intended. It is necessary to investigate the underlying cause of any issue to determine corrective action. The proposed action will be reviewed for effective implementation at the next assessment.

Please refer to Assessment Conclusion and Recommendation section for the required submission and the defined timeline.

Assessment objective, scope and criteria

The objective of the assessment was to conduct a reassessment of the existing certification to ensure the elements of the proposed scope of registration and the requirements of the management standard are effectively addressed by the organization's management system.

The scope of the assessment is the documented management system with relation to the requirements of BS EN ISO27001:27001 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment are BS EN ISO27001:27001 in relation to Reward Gateway (UK) Ltd management system documentation

Assessment participants

Name	Position	Opening meeting	Closing meeting	Interviewed (processes)
Adam Altounyan	Head of Information Security in Infrastructure	X	X	X
Asen Varsanov	Internal IS Consultant	X	X	X
Will Tracz	Chief Technical Architect	X		X
William Elliott	Office Manager			X
Robert Banks	IT Support			X
Robert Hicks	Group HR Director			X
Plamena Andreeva	HR Assistant			X
Luke Kingshott	Implementation Specialist			X
Jodie Case	Client Success Manger			X
Glenn Willshire	Client Success Manger			X
Olivia Hyde	Product Manager			X
Jamie Saunders	Head of Retail Operations			X

Assessment conclusion

BSI assessment team

Name	Position
Simon Evans	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.

RECOMMENDED - Corrective Action Plan Required ('Minor' findings only): The audited organization may be recommended for continued certification, based upon the acceptance of a satisfactory corrective action plan for all 'Minor' findings as shown in this report. Effective implementation of corrective actions will be reviewed during the next surveillance audit.

Please submit a plan to BSI detailing the nonconformity, the cause, correction and your proposed corrective action, with responsibilities and timescales allocated. The plan is to be submitted no later than 15/06/2018 by e-mail to msuk.caps@bsigroup.com, referencing the report number, or through the BSI Assurance Portal if this is enabled for your account.

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

Opening Meeting: Business Context, ISMS changes & previous findings: Clause 4:

Opening Meeting:
-The formal opening meeting included the objective of the assessment, methodology and terminology used, confidentiality, number of staff in scope, purchase order details, and the agreed assessment plan.

Context:
- There has been no significant change in the business since the last assessment. There are potential business acquisitions in the pipeline which the business is considering. This would not lead to an aggressive change in head count.
- There is no indication that the acquisitions will lead to a widening of the ISM scope
- A full list of interested parties has been produced

ISMS Change
- No significant change to the ISMS since the last assessment

Previous finding: IS 544153
- Opportunity for improvement – 'greater clarity could be given as to what constitutes a 'Standard change' which does not require CAB approval'
- Change Management Policy V1.1 date 26/06/2017 is clear on the standard change requirements and are known within the business and are accepted

Scope change:
The scope statement has been updated with a review change to read:
-The provision of integrated voluntary benefits to private, public and not-for-profit organisations. This is in accordance with the Statement of Applicability version 8 dated 12/02/2018

Leadership: top management interview: Clause 5:

Interview with Will Tracz as part of the Leadership Team
- All members of the leadership team have security backgrounds and therefore have embedded this as a business culture
- Funds are made available for staff to build security into the business framework
- Clear drive to improve security across the business; 2 minute warning implemented for raising issues to leadership
- Strong business and culture to speak up for issues
- Security objectives are regularly reviewed by top management and are aligned to strategic business direction
- Key leadership drive to bolster technical capability
- GDPR has been a key driver in discussions

Policy:
- ISMS Policy v2.4 date 01/03/2017 was viewed and was approved by senior management
- Policy includes the objectives of the ISMS
- Strategic annual objectives are set within the ISMS audit log and actions

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved. It is clear that the organization's leadership have embedded security as a culture

Planning & Operation: Clauses 6, 8:

Documents Viewed:
- ISMS Policy v2.4 date 01/03/2017
- ISMS Audit Log and Actions, v 13 dated 20/05/2018
- ISMS Manual, v8.2 dated 02/2018
- Risk Management Policy, v2.1 dated 29/05/2018
- Risk Assessment Document v16 dated 01/06/2018
- Statement of Applicability v 8 dated 12/02/2018

Evidence:

Statement of Applicability:
- Annex A controls have been implemented
- PCI:DSS controls have been considered but were covered by Annex A controls as such were discounted
- Only one control has been excluded (A14.2.7) and justification provided
- Full justification for each included control is added into the SoA

Objectives:
- Objectives are raised in the Audit Log and Actions document
- There are currently eight objectives raised for the period 2018-2021
- Objectives are aligned to business strategy and have links to identified risks

Risk Assessment:
- Risk Assessment Document outlines the risk acceptance criteria and how to perform the assessment
- Assessment document assigned criteria for the levels of treatment of identified risks
- Good evidence of threat regularity documented
- All assets have an assigned threat and consequence of loss value applied
- Currently there are 116 assets risks assessed with a potential multiplication of 90 threats per asset identified and managed
- Risks are assessed and those over a threshold are sent for treatment

Risk Treatment:
- All risks sent for treatment are aligned back into Annex A controls
- Six risks have been sent for risk treatment as per the process
- Four of the six risks are still actively being treated at the time of assessment

Sampled risks include:
- Asset 5 Network Infrastructure
- Asset 27 Live Member Data
- Asset 84 DNS Software
- Asset 103 Theft of data

All sampled risks have followed the methodology applied in the risk assessment document

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Support: Clause 7:

Documents Viewed:
- PCI ISA Certificate
- ISO27001:2013 Internal Auditor Certificate
- CISSP Certificate
- ISMS Manual, v8.2 dated 02/2018

Evidence:

Resources:
- Top management have encouraged the investment in bringing in competent staff to support the ISMS and infrastructure.
- The recruitment of a Head of IS in Infrastructure in 02/2018 enforces the support by top management

Competence:
- The business are fully committed to deploying competent staff into ISMS positions. This was evident in the leadership interview

Sampled Positions:
- Internal IS Consultant was viewed to have PCI ISA Certificate (Certificate 804-171 provided by PCI Standards Council) and ISO27001 Internal Auditor (Certificate 50524 by Intertek)
- Head of Information Security in Infrastructure was viewed to have CISSP (Member Number 580587: Expiry 31/07/2020)

Awareness:
- IS messages were observed on the TV screens around the office throughout the duration of the assessment
- IS messages on 'Boom' communications hub
- Sampled communications include '2 Minute Warning', GDPR, Fraud Hacking, Phishing, Password Control and Social Engineering
- Vulnerability alerts are issued via this same medium
- Annual IS training and Induction training is provided and was sampled
- Induction is from day one of employment
- 99% of staff have received training; the 1% not compliant is those currently undergoing induction as new starters

Communication:
- A communication section is covered, and was sampled, within the ISMS Manual at paragraph 1.07.4
- This determines the main channels of communication both internally and externally

Documented Information:
- All documents reviewed, as part of this assessment, had valid version control, date of version, owner, revision changes and approval notes
- Documents are located within Google Drive as a DMS
- Documents are reviewed at least once per calendar year

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Performance Management: Clauses 9, A16:

Documents Reviewed:
- ISMS 27001 Internal Audit Results January 2018
- ISMS Manual, v8.2 dated 02/2018
- Management Review Minutes March 2017

Evidence:

Internal Audits:
- Annual ISMS 27001 Internal Audit Results January 2018 was viewed
- Audits can be tracked back annually through to 2009
- Audit schedule for 2018 was viewed in the ISMS manual
- Schedule outlines 4 ISMS audits throughout 2018
- Audit for 2018 was sampled
- Eight OFIs were identified as part of the internal audit
- Internal auditor was suitable qualified to carry out the audit

Management Review:
- Management review takes place once per calendar year
- Internal ISMS performance meeting occur weekly during 1:1 meetings
- Minutes from MR in March 2017 was viewed
- All elements from the Clause 9.3 were covered within the minutes
- Minutes form the MR were reported to the Senior Leadership Team

Monitoring:
- The ISMS Manual details what will be monitored by who and at what intervals
- Monitoring results are published through to the various management and leadership teams (as per MR above)

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Improvement: Clause 10:

Documents Review:
- Incident Management Policy , v2.2 dated 01/03/2017
- Incident and IT ticketing system Jira viewed

Evidence:
- All nonconformities are tracked using an IT or Incident ticketing system as per the above policy
- Nonconformities are owned throughout the lifecycle and are tracked to completion
- Completion of the ticket includes effectiveness and analysis of the remediation

Nonconformities:
Sampled output from the internal audit
- A5.1.2 (Update of Policy) raised as ticket IN-1838 (Still in progress)
- A8.1.1 (Inventory of Assets) raised as ticket IT-6235

Sampled output from external audit
- AXP-ISO1.04 Policy review - Policy now updated
- AXP-ITO4.13 Cryptographic Standard - Updated to TLS1.2 (Change Management ticket 0015 viewed to

evidence change)

Progress against ISMS objectives
- Covered within the MR minutes from March 2017 were viewed
- Full status of the current objectives was evidenced
- Report was presented to the Organization Leadership Team
- Progress of objectives was deemed to be effective by management

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Physical & Environmental Security: Clause A11:

Documents Viewed:
- Fire risk assessment
- PAT Testing 08/2017 by CBRE
- Fire Evacuation Procedure dated 30/06/2017
- Fire Risk Assessment by CBRE dated 06/2017
- Fire evacuation report 17/05/2018
- Emergency lighting log book
- Legionnaires log book
- Legionnaire certificate of attendance 18/09/2017
- Fire extinguisher maintenance report dated 10/10/2017
- Tenant handbook

Evidence:
- Office is located on the 4th floor of a landlord owned building
- Ground floor reception carries out initial ID checks then allows visitors to proceed to 4th floor
- Organization occupy the whole of the 4th floor
- Access to the office, from the lift and stairwell, is via a secure door with proximity reader and bell for visitors
- Once in the office greeted by reception desk where visitors sign in using Envoy visitor recording application
- Last emergency lighting test recorded as 06/2018
- Last legionnaire test carried out 06/2018
- Fire evacuation is carried out bi-annually and evidenced
- No confidential waste bins as this is a paper free environment; however a shredder is located in the communications room
- Tenancy handbook was observed to identify the levels of maintenance carried out by the landlord and those required by the tenant

Effectiveness: The Minor Non conformity raised in this section, identified that planned objectives have not been fully realised

Supplier Relationships: Clause A15:

Documents Viewed:
- Standard T&Cs Contract
- Agreement with Strait Logics dated 15/11/2016
- Agreement with The Bunker dated 09/09/2015
- NDA with Cyber Source dated 03/2016

- NDA with Bamboo dated 08/2015

Evidence:
Suppliers include:
- Strait Logics
- The Bunker
- Cyber Source
- Bamboo

T&Cs contracts contain clauses for Data Protection, Confidentiality, IPR and data processing agreements were viewed for companies relating to Data Analytics, HR Data and Cloud Hosting

Monitoring
- Suppliers are continually monitored though annual security questionnaires
- All questionnaires follow ISO27001 format
- 2017 questionnaires for The Bunker, Strait Logics and Cyber Source were viewed
- ISO certificated for the above suppliers were evidenced
- All suppliers have been signed new data processing agreements in line with GDPR

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

IT: Clauses A8, A9, A10:

Documents Viewed:
- ISMS Manual, v8.2 dated 02/2018
- Asset Repurpose, Decommissioning and Disposal Policy, v 2 dated 05/2018
- Data Classification Policy, v 1.1 dated 30/05/2018
- Access Control Policy, v 9.5 dated 25/01/2018
- New starter Procedure, v 1.1 dated 30/03/2018
- Leaver checklist in Bamboo HR
- Encryption Policy, v 1.4 dated 01/03/2018
- Acceptable Use and IT Policy, v 2.5 dated 29/05/2018
- BYOD Policy, v2.1 dated 10/04/2107

Evidence:

Asset Management:
- All assets have an assigned impact level for CIA
- All assets are designated to a business owner
- Assets tracked in Salesforce
- A sample of assets was chosen: UK04182, UK04208, UK04176, UK04134 and UK04112.
- Assets were observed in the correct locations and asset owners correctly identified
- Assets for disposal are set aside within the restricted access communications room
- Laptops for disposal are internally wiped, with encryption keys removed to ensure no corporate data is retained, and they are then sold internally to staff or given to charity
- The AUIT Policy was observed

Data classification
- Data classification was noted to be in place in policy documentation
- Three classifications are in place; Unclassified, Commercial and Critical

- Awareness for the use of classification was noted in screens in the office

Data transfer
- No personal data is transmitted via email
- SFTP is in place (WeTransfer) for use by the business and customers
- The use of Secure File Uploader is integrated into Reward Manager and it to be used for transfer of personal data
- All laptops encrypted and have USB ports disabled to prevent data loss

Access Control
- New users are processed in Bamboo HR and an account is then created in Okta (access control system)
- Access is defined by manager and tickets raised in Jira
- Common applications are required by all staff and additional applications requested via ticket and approved by the application owner
- Okta acts as single sign on so staff leaving cannot access any platforms once the account is is disabled for the user
- Okta accounts are disabled the day of a staff member leaving following receipt of termination in Bamboo HR
- Staff do not have separate administrative accounts but will have elevated administrative access within Okta which is ticketed and activity is logged
- BYOD is in place for the use of mobiles and the use is covered in the BYOD Policy
- Phones are required to use a PIN or biometric setting, set to auto lock after one minute, enforce encryption of device backup and allows remote wipe
- Google G Suite mobile management is used to enforce the above controls
- MFA and IP protection is in place with the use of Okta

Sampled account creations:
- Lucy Thomas started 18/06/2018: ticket RG-47577
- Jenifer Frial started 04/06/2018: ticket RG-47119
- Both sampled accounts were in line with the access control policy
- It was evidence that there is a multi-step authorisation process for the levels of applications requested

Sampled account deletions:
- Julia Thomas departed on 31/05/2018: leavers process viewed and account no longer active
- Eleonara Manolova departed on 09/05/2018: leavers process viewed and account no longer active

Okta Admin Accounts
- Six users were observed to have administrative accounts in Okta
- Each admin was demonstrated to have varying levels of access with one super user

Cryptography
- Bycrypt is used to hash passwords in Reward Manager
- Servers and laptops encrypted to AES 128
- Laptops observed using FileVault for encryption
- Encryption recovery keys are maintained in a restricted folder in Google Drive
- The folder retaining the encryption keys was observed to only have three staff members allowed access
- Ticket IT-6374 to demonstrate the use of recovery keys was observed

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Information Security - Incident Management: Clause A16:

Documents Reviewed:
- Incident Management Policy , v2.2 dated 01/03/2017
- ISMS Manual, v8.2 dated 02/2018

Security Incidents:
- ISMS manual refers to the Incident Management Policy but provides outline controls in place
- Incident Management Policy outlines the business approach and scope of the policy
- Roles and responsibilities are clearly identified
- Collection of evidence is mandated for IT incidents
- All security incidents are recorded in Jira ticketing system

Security incidents sampled:
- IN1131 dated 21/06/2017
- IN1400 dated 17/01/2018
- IN1687 dated 03/05/2018
- IN1676 dated 01/05/2018

Incidents sampled have incident reports raised which include timelines, root cause and closure actions taken. The report includes effectiveness of the actions and captured any changes to applications or policy. All incidents were handled in line with the Incident Management Policy

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Operations Security: Clause A12:

Documents Viewed:
- Back Up Policy, v1.3 dated 28/05/2018
- Acceptable Use and IT Policy, v 2.5 dated 29/05/2018
- ISMS Manual, v8.2 dated 02/2018

Evidence:
Operational procedures and responsibilities
- Numerous documents and processes have been viewed as part of this assessment and are referred to within the appropriate sections of the report
- Change management controls were observed
- Sampled change tickets 0015, 0016, 0008 and 0018 were viewed
- The sampled tickets were all observed to have the correct levels of authorisation and requirements and, where required, links to incident tickets and IS objectives

Protection from Malware:
- Sophos Cloud SWA is utilized for Anti-virus control
- Asset BG01001 was viewed with up to date AV (version 9.7.5)
- Panorama 9 is used for patch management deployment
- Report dated 02/05/2018 was observed
- Live dashboard for Panorama 9 was observed showing only 2 devices not patched (offline)

Backup
- Cross reference Change 0008 regarding previous change control for testing backups was observed
- Backup are completed daily with incremental backup over 7 days with monthly retention
- Tests of backups are done twice annually
- Last back up test, of DB 4, was observed as being 25/05/2018
- RPO and RTO schedules are observed within the backup policy
- All backups are encrypted to AES 256 standard
- Backups are pulled to the TwinStrava OBS Gateway for retention

Logging and Monitoring
- Splunk is used as SIEM solution
- Logs are monitored daily by the DevOps team
- Logs are maintained and can be tracked for at least the past 12 months (observed)
- Logs are protected in Splunk with access strictly controlled to a small number of staff
- Clocks were viewed to synchronize from NTP at The Bunker

Control of Operational Software
- Software is only uploaded by IT staff following approval
- Sophos alerts if any unauthorised software is applied via web filtering and monitoring tools

Technical Vulnerability Management:
- Panorama 9 is deployed to identify gaps in the patch deployment program
- Any gaps are remediated once the user connects back to the network
- Urgent vulnerability releases are monitored and will go through eRFC process
- Installation of software is covered in the Acceptable Use Policy and is restricted to IT staff

Information Systems Audit Considerations:
- Internal audit controls are maintained and were viewed as part of the audit schedule
- Internal audits were sampled as part of the section above
- External audits are carried out by PwC, BSI and 2nd party Clients
- PwC are currently running a IT general controls transactional audit on behalf of the organization
- This provides assurance over the integrity of financial reports extracted from the IT systems
- All audits are conducted for legal, regulatory or contractual reasons and are approved with scope and context prior to taking place
- A pen test by MDSec, dated 04/05/2018, was sampled.
- The above report was observed to have an agreed scope and technical approach

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Communications Security: Clause A13:

Documents Viewed:
- Acceptable Use and IT Policy, v 2.5 dated 29/05/2018
- Agreement with The Bunker dated 26/06/2014 (reviewed annually)
- SLA Agreement with The Bunker dated 25/02/2016

Network Security Management
- Network management is contracted to The Bunker
- There are agreed SLA and KPIs as part of the network service

- All applications are segregated and access is strictly controlled to only those with a defined business need

Information Transfer
- Information transfer was observed in the Acceptable Use document
- The use of Secure File Uploader is integrated into Reward Manager and it to be used for transfer of personal data
- This is used by customers and company employees using HTTPS (TLS1.2)
- A test using Qualys (SSL Labs) was observed to demonstrate the protocols as being TLS1.2
- The use and transfer of files using Secure File Uploader was observed by creating a test file
- The test transfer was correctly observed in the Uploader log
- Staff are directed not to transfer personal data via email

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Business Continuity Management: Clause A17:

Documents Viewed:
- Business Continuity Policy, v1.5 dated 06/2018
- Business Impact Analysis for Business Operations
- Business Impact Analysis for Client Support Team
- ISMS Audit Log and Actions, v 13 dated 20/05/2018
- Network capacity reports from New Relic

Evidence:

Information Security Continuity:
- Business Continuity Policy identifies 12 areas of threat which may lead to the activation of the BCP
- There are 4 BCPs in place which will correlate to the 12 areas above
- Business Impact analysis surveys were observed for individual departments
- The BIAs were observed with considered IS risks and SLAs included
- The use of SaaS solutions has minimised the requirement for staff to work from office locations
- In time of emergency staff can work from home as all offices are paperless
- All extant policies remain valid if staff are working from an office location or from home

Testing:
- The organization have an objective set to increase their approach to Business Continuity by simulating possible incidents
- Test for the restore of DB4 was viewed in the audit log and correlating event log from 25/05/2018
- Failover tests was observed from 11/08/2017
- Internet connection failover test was observed from 16/10/2017
- There is good evidence of testing of backups and failovers but the rest of the business continuity plan and impact analysis documents have not yet been considered for testing (See NCR to this section)

Redundancies:
- Capacity is monitored using New Relic for the Development, Staging and Production environments
- Capacity is monitored daily DevOps team
- Capacity limits are set at production requests per second for staging and reports were viewed showing highest use at 1,500 requests per second
- Reports for staging and development were also viewed to reveal less than half capacity being used

Effectiveness: With the Minor Non conformity raised in this section it is identified that planned objectives have not been fully realised

HR Security: Cause A7:

Documents Viewed:
- Disciplinary Policy, v1.1 dated 03/2018
- New Starter Procedure, v1.1 dated 04/04/2018
- Leavers Process, v1
- Leavers Checklist in Bamboo HR
- Employee Handbook, v2.0 dated 03/2018

Evidence:
New Starters
- All jobs are identified and then entered into the Greenhouse candidate management system
- All unsuccessful candidate's CVs are kept in the system for 6 months under GDPR
- Last cleanse was carried out prior to GDPR and was following an internal Privacy Impact Assessment
- HR Director is single point of authorisation for new recruitment process to begin
- All contracts contain clauses for confidentiality, IPR protection and Data Protection
- Disclosure checks are not require for all staff

A sample of new starter records were reviewed for the following:
- Harjinder Shemar and Douglas Kisuule (DBS Observed)

The following records were observed kept:
- Starter Checklist used to ensure that the process has been followed
- Signed Contractual Documents: 05/2018 and 06/12/2018 respectively
- Signed confidentiality, IPR and DPA requirements in contract
- Passport and references viewed
- Access Created: Ticket IT6674 (RG47243) and IT5535 (RG44068)
- Induction Training

Movers/Transfers
- Alisa Pencheva and Anton Kostadinov
- Transfer Checklist used to ensure that the process has been followed.

Records were observed showing
- Access amended via tickets RG46422 and IT5792
- Movers checklist on Bamboo HR profile

Leavers
A sample of records for leavers was observed for the following:
- Chris Justice and Ivana Apostolova

The following was observed respectively
- Leaver Checklist was observed to be used in Bamboo HR
- Checklist demonstrated process had been followed
- Resignation acceptance letter with reminder of confidentiality and IPR
- Asset return - monitored through checklists viewed in Bamboo HR
- Access removed via ticket IT6768

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Legal & Regulatory Compliance: Clauses 4.2, A18:

Document Viewed:
- Register of Legal and Other Aspects, v3.0 dated 03/03/2017

Evidence:
The register contains a full list of regulatory and contractual legislation applicable to the business. This includes (not exhaustive):
- Environmental Protection
- Control of Waste
- Electronic Communications
- Data Protection 1998
- Human Rights
- Computer Misuse
- PCI:DSS

The register contains an explanation of applicability to the organization and how it is monitored and included in policy.

Strong evidence has been produced throughout the assessment surrounding the protection of documents within the SaaS solution

Effectiveness: With the Minor Non conformity raised in this section it is identified that planned objectives have not been fully realised

System Development and Acquisition: Clause A14:

Documents Viewed:
- ISMS Internal Audit results
- Secure Development Policy, v 1.2 dated 01/03/2018

Evidence:
- The organization have adopted the Microsoft Secure Development Lifecycle for Agile process
- Process outlines training, requirements, design, implementation, verification, release and response
- The use of OWASP Top 10 vulnerabilities is in use
- The Jira ticketing system is set up to match the development lifecycle

Projects were noted in the 90 day vision board providing outline of current in-flight projects
- Employee Communications project sampled
- Project was required following client feedback requiring feedback (emoji buttons) buttons to an existing application
- Sampled project was observed to follow the Agile process
- Tickets RGD47458, RGD28967 and RGD32374 were observed in the project
- The tickets in Jira are set out so the progression can be tracked in the gateways through to release

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Awareness: Clause A7.2.2:

A sample of six employees from the following departments were interviewed:
- IT
- Implementation
- Support x 2
- Product
- Retail

The interviews highlighted a strong awareness the following:
- Signposting of IS policies, procedures and controls
- Password complexity and control
- Up to date AV
- Incident reporting and ticket raising
- IS training and awareness packages (Exam histories viewed)
- Email security (Phishing and Social Engineering)
- Physical security measures
- Network security controls and restrictions
- Secure file transmission using the uploader

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Minor (3) nonconformities arising from this assessment.

Finding Reference	1637527-201806-N1	**Certificate Reference**	IS 544153
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A11.2.1
Category	Minor		
Area/process:	Physical & Environmental Security: Clause A11		
Statement of non-conformance:	Equipment within the communication room is not adequately protected from hazards and other risks in line with the standard		
Clause requirements	Equipment siting and protection Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		
Objective evidence	The communication room was observed to contain a number of cardboard boxes in close proximity to, and preventing immediate access to, the communications cabinet. This was agreed with the client.		
Cause			
Correction / containment			
Corrective action			

Finding Reference	1637527-201806-N2	**Certificate Reference**	IS 544153
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A17.1.3
Category	Minor		
Area/process:	Business Continuity Management: Clause A17		
Statement of non-conformance:	There is no validation of the business continuity plan to ensure the whole plan is valid and effective as required by the standard		
Clause requirements	Verify, review and evaluate information security continuity The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.		
Objective evidence	The organization conducted a full restore from backup of a database in 05/2018 but there are no other entries within the audit schedule to conduct additional BCP validation tests which would validate the rest of the BCP. This is contrary to the standard, and the internal objectives which outline the requirement to conduct at least two business continuity tests each year.		

Cause	
Correction / containment	
Corrective action	

Finding Reference	1637527-201806-N3	**Certificate Reference**	IS 544153
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A18.1.1
Category	Minor		
Area/process:	Legal & Regulatory Compliance: Clauses 4.2, A18		
Statement of non-conformance:	The Register of Legal and Other Aspects register was not fully up to date with current legislative acts applicable to the organization as required by the standard		
Clause requirements	Identification of applicable legislation and contractual requirements All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.		
Objective evidence	The Register of Legal and Other Aspects has not been reviewed since 03/2017 and has not taken into account the introduction of the DPA 2018 and GDPR even though changes have been made to the organization's policies and processes		
Cause			
Correction / containment			
Corrective action			

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 BS EN ISO27001:27001 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment are BS EN ISO27001:27001 in relation to Reward Gateway (UK) Ltd 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	Clause
28/11/2018		0900	Opening Meeting	
		0930	Business Context/ISMS changes & previous findings: 4	
		1000	Leadership: top management interview: 5	
		1030	Planning & Operation: 6, 8 - risk assessment - risk treatment	
		1100	Support: 7 Resources, Competence, Awareness, Documented information	
		1130	Performance Evaluation: 9 - internal audits - Management Review - Monitoring and measurement	
		1200	Improvement: 10 - Nonconformity - Improvement	
		1230	Information Security - Incident Management A16	
		1300	Lunch	
		1330	Information security in business continuityA17	
		1400	Legal & regulatory compliance: 4.2, A18	
		1430	HR security: A7	
		1500	Sales Department: A7.2.2	
			Employee Savings Department: A7.2.2	
		1530	Report Preparation	
		1600	Closing Meeting	

Appendix: Your certification structure & on-going assessment programme

Scope of certification

IS 544153 (ISO/IEC 27001:2013)

The provision of integrated voluntary benefits to private, public and not-for-profit organisations. This is in accordance with the Statement of Applicability version 8 dated 12/02/2018

Assessed location(s)

The audit has been performed at Central Office.

London / IS 544153 (ISO/IEC 27001:2013)

Location reference	0047299068-000
Address	Reward Gateway (UK) Ltd 265 Tottenham Court Road London W1T 7RQ United Kingdom
Visit type	Re-certification Audit (RA Opt 2)
Assessment reference	8702533
Assessment dates	06/06/2018
Deviation from audit plan	No
Total number of Employees	84
Effective number of Employees	84
Scope of activities at the site	Main certificate scope applies.
Assessment duration	3 day(s)

Certification assessment programme

Certificate number - IS 544153
Location reference - 0047299068-000

		Audit 1	Audit 2	Audit 3	Audit 4	Audit 5	Audit 6	Audit 7	Audit 8	Audit 9
Business area/location	**Date (mm/yy):**	11/18	06/19	06/19	11/19	06/20	06/20	11/20	04/21	04/21
	Duration (days):	1	0.5	1	1	0.5	1	1	0.5	5
Business Context/ISMS changes & previous findings: 4		X		X	X		X	X		X
Leadership: top management interview: 5, A5, A6		X		X	X		X	X		X
Planning & Operation: 6, 8 - risk assessment - risk treatment		X		X	X		X	X		X
Support: 7 Resources, Competence, Awareness, Documented information		X		X	X		X	X		X
Performance Evaluation: 9 - internal audits - Management Review - Monitoring and measurement		X		X	X		X	X		X
Improvement: 10 - Nonconformity - Improvement		X		X	X		X	X		X
Information Security - Incident Management A16		X		X	X		X	X		X
Information security in business continuity: A17		X		X			X			X
Legal & regulatory compliance: 4.2, A18		X			X			X		X
HR security: A7		X			X			X		X
IT operational security: A12				X			X			X
System Development and Acquisition: Clause A14		X			X			X		X
IT communications security: A13							X			X
Sales Department: A7.2.2		X						X		X
Client Services Department:				X						X

A7.2.2									
Development Department: A7.2.2				X					X
Finance Department: A7.2.2						X			X
Employee Savings Department: A7.2.2	X						X		X
Physical & environmental security: A11			X						X
Supplier relationships: A15						X			X
Triennial Reassessment & Strategic Review									X
Programme Management time		X			X			X	

Mandatory requirements – recertification

Review of assessment finding regarding conformity, effectiveness and relevance of the management system:

The organization was noted to be continuing to maintain and improve the processes effectively, with particular regard to positive areas:
- Strong leadership
- Robust internal audits against standard
- Training and awareness
- New data processing agreements with existing suppliers in line with GDPR
- Log record availability within Splunk

There are however further possible opportunities to improve and reduce risks, relating to achieving the intended results regarding:
- The protection of assets in the communications room from environmental risk
- Maintenance of legal requirements
- Improvement of business continuity testing

Management system strategy and objectives:

It is anticipated that the management system will continue to mature and will remain effective over the next cycle

Review of progress in relation to the organization's objectives:

Interview with Will Tracz as part of the Leadership Team
- All members of the leadership team have security backgrounds and therefore have embedded this as a business culture
- Funds are made available for staff to build security into the business framework
- Clear drive to improve security across the business; 2 minute warning implemented for raising issues to leadership
- Strong business and culture to speak up for issues

- Security objectives are regularly reviewed by top management and are aligned to strategic business direction
- Key leadership drive to bolster technical capability
- GDPR has been a key driver in discussions

Review of assessment progress and the recertification plan:

All areas will be assessed and have been included in the assessment plan for the next cycle in line with the current number of staff against the duration calculator

BSI client management impartiality and surveillance strategy:

Current impartiality has been maintained and the current assigned T and P codes are sufficient. This is a single site audit and consideration is provided in the assessment plan

Continue with the current total assessment days/cycle.

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

'Just for Customers' is the website that we are pleased to offer our clients following successful registration, designed to support you in maximising the benefits of your BSI registration - please go to www.bsigroup.com/j4c to register. When registering for the first time you will need your client reference number and your certificate number (47299069/IS 544153).

Should you wish to speak with BSI in relation to your registration, please contact our Customer Engagement and Planning team:

Customer Services
BSI
Kitemark Court,
Davy Avenue, Knowlhill
Milton Keynes
MK5 8PP

Tel: +44 (0)345 080 9000

Email: MK.Customerservices@bsigroup.com

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 on-site 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.