FUJ00080799

Assessment Control Page

Assessment Type	Internal	**Assessment Reference**	
Area	RMGA	**Processes Assessed**	Information Security Incident Management
Contact(s)	Howard Pritchard	**Process Owner(s)**	Howard Pritchard
Planned Date	Jan 2009	**Lead Assessor**	Chris Cole
Start Date	Jan 2009	**Full Report Title**	

Assessment Summary

1. Objectives of Assessment

This Fujitsu Services Internal Assessment focused on key business functions performed in, or on behalf of, Royal Mail Group Account (RMGA), and associated Core Services delivery units, and considered, through the assessment of corporate and local processes and working practice:

- The compliance of those functions with relevant aspects of the ISO 27001:2005 standard.
- The compliance of those functions with relevant aspects of the Payment Card Industry Data Security Standard (PCI-DSS)
- Any areas suitable for promotion as good business practice across Fujitsu Services.

2. Scope of Assessment

This Fujitsu Services Internal Assessment concentrated on the Royal Mail Group Account and was conducted over 15 days. This assessment was a document review and some process implementation sampling was conducted.

Observations raised are categorised as Issues (Non-conformities) and Observations. As the contractual status of PCI-DSS compliance is uncertain all relevant finding are classified as observations only at this stage.

Corrective action plans are required for all Issues and Observations raised and should be recorded within the Assessment Database, by the Quality or Security Representative, within 10 working days of the issue of the Assessment Report.

The normal target for the implementation of corrective action plans is 60 days from the date of issue of the Assessment Report.

FUJ00080799

3. Management Summary

During this Assessment three Issues and sixteen Observations were raised against the Royal Mail Group Account.

The main ISO/IEC 27001:2005 high level findings are summarised as follows:

- Whilst the overarching RMGA Information Security Policy and supporting Information Security Incident Management documentation provide good guidance in how Information Security Incidents and Weaknesses should be reported there is a glaring document reference error that could negate the well intentioned policy statements.
- Notwithstanding this document reference error, it is evident that not all members of the RMG Account are aware of the correct process for reporting Information Security Incidents and Security Weaknesses.
- It is further observed that there are references to HORIZON specific processes within the HNG-X documentation.

The following high level observations were made that are specific to the PCI-DSS requirements

- The RMGA Customer Service PCI Incident Management Process is recognised as still being in draft format and requires updating to reflect the PCI-DSS requirements. Additional benefits will be achieved by incorporating the linkages / references to other relevant RMGA Information Security Incident Management documentation where applicable.

FUJ00080799

4. Assessment Commentary

4.1 Information Security Incident Management ISO/IEC 27001:2005

Assessment Criteria: ISO/IEC: 27001-2005 A. 13.1.1, A. 13.1.2, A.13.2.1, A.13.2.2, A.13.2.3

In general there were three issues in this area, however, there were three further observations.

- Information security events shall be reported through appropriate management channels as quickly as possible. SVM/SEC/POL/0003 V3.0- RMGA Information Security Policy states "Ensure information security events and weaknesses associated with RMGA information systems are communicated in a manner allowing timely corrective action to be taken and as referenced in CS/PRO/018 (RMGA Customer Service Incident Management Process)."

  Internal Auditor Comment:

  It is raised as an **issue** that CS/PRO/018 was made available by the Document Control Manager and it is entitled "Release 1c SYSTEM ENVIRONMENT: Processes and Procedures".

  Document Control Manager Response:

  "The correct reference for the Incident Management Process is SVM/SDM/PRO/018 - clearly there is confusion over the similar reference numbers although I don't think the documents are connected in any other way."

- It is noted that SVM/SDM/PRO/0018 V2.0 - POA Customer Service Incident Management Process, Paragraph 9.6.1.1 clearly states that, "Anyone reporting a security Incident should be encouraged to notify their Line Manager in the first instance"

  Two members of the Application Solutions Development Team, a member of the IS Design Team and a Network Engineer from IS Implementation were requested to identify who they should report security incidents to.

  One was unsure how Information Security incidents should be reported as there has not been any requirement to date. Another specified that the incident should be reported to the Account Security Team. A third offered CS-Security. The fourth offered 3 possible reporting methods including via the online reporting form and the word version of this form and via 7799.

  All of these responses are not in accordance with RMGA Information Security Policy, Paragraph 13.1.1 and POA Customer Service Incident Management Process, Paragraph 9.6.1.1

  Internal Auditor Comment:

  The major concern must lie with the not known response. All the other interviewees at least offered a viable, albeit non policy compliant, route to escalate a security incident.

  Without all staff being aware of how to report an Information Security Incident there is a risk that delays in reporting may have a detrimental effect to the overall impact levels.

  It should also be noted that other members of these and other HNG-X teams were able to correctly identify the correct initial incident reporting criteria.

- There is a requirement that all employees understand that they should not try to test a suspected weakness or prove that it is real.

  Two members of the Application Solutions Development Team were asked that if they suspected that there is a security weakness in any area of HNG-X would they attempt to prove the validity of the weakness prior to reporting.

FUJ00080799

It is raised as an **issue** that one responded that, "dependent on context and assessed immediacy and severity of risk. If risk was assessed as immediate and severe I would report without testing. If low I would seek to prove."
Another responded that, "Yes, I would confirm it with one of my technicians."

This is contrary to RMGA Information Security Policy which stipulates in Paragraph 13.1.2, "RMGA staff must be aware that they should not, in any circumstances, attempt to prove a suspected weakness themselves. If such a course of action resulted in a security Incident then it may be treated as a disciplinary issue."

Internal Auditor Comment:

It should also be noted that there is the potential for managerial pressure to render subordinate staff ie: the technician, to be in breach of policy.

- There is a requirement that Information security events shall be reported through appropriate management channels as quickly as possible. It is **observed** that SVM/SDM/PRO/0018 V2.0 - POA Customer Service Incident Management Process, Paragraph 9.1, states that, "This annex outlines the process regarding the investigation, and reporting of all security incidents concerning the HORIZON Network and all IT equipment**."**

- It is **observed** that the formal incident response and escalation procedure as captured in SVM/SEC/POL/0003 V3.0- RMGA Information Security Policy, Paragraph 13.1.2, contains an incorrect document reference to CS/PRO/018.

- It is **observed** that the formal incident response and procedures as captured in SVM/SEC/POL/0003 V3.0- RMGA Information Security Policy, Paragraph 13.2.1, contains an incorrect document reference to CS/PRO/018.

FUJ00080799

4.2 Media Management PCI-DSS

Assessment Criteria: PCI-DSS 11.1, 12.5.3, 12.9, 12.9.1, 12.9.2, 12.9.3, 12.9.4, 12.9.5, 12.9.6.

It should be noted that as the contractual status of PCI-DSS compliance is uncertain. Notwithstanding this position, all observations should be assessed to determine the priority of corrective actions dependent upon the perceived, potential non-compliance to regulatory requirements.

The following thirteen observations were made that are specific to the PCI-DSS requirements

- PCI-DSS 11.1 requires that there is a test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. It is **observed** that the documentation reviewed does not include any specific references for a response in the in the event of unauthorized wireless devices are detected.

  Internal Auditor Comment

  Furthermore wider discussion should be considered concerning the deployment of wireless IDS / IPS to identify all / any wireless devices within HNG-X. It was indicated that this may only occur within Data Centre and Corporate support facilities and the frequency of IDS / IPS deployment to monitor for wireless devices was not available but described as potentially "sporadic". No assurances of their deployment within other HNG-X areas could be given.

- PCI-DSS 12.5.3 requires the establishment, documentation, and distribution security incident response and escalation procedures to ensure timely and effective handling of all situations. It is **observed** that SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process has been produced, however it is recognised that this has not obtained senior management approval.

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at a minimum, roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands.

  It is **observed** that within SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process, Table 1, there is a communication strategy that captures the main components of the process in defining and managing a PCI incident.

  However, whilst roles are referred to within the PCI Incident Response Plan the responsibilities are not explicitly defined although mention is made in within the document of the functions the Operations Security Manager and CISO play during the escalation and management process.

  References are made to
  - RMGA Security
  - Fujitsu Corporate Security (for minor PCI Incidents)
  - RMGA Operations Director
  - Information Security Incident Manager
  - RMGA Crisis Management Team

  However, their responsibilities are not clearly defined.

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at a minimum, roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands.

  It is **observed** that within SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process, Paragraph 2.22, the contact information for key PCI Incident Response Personnel that the RMGA CISO mobile phone number is incomplete.

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, specific incident response procedures. It is **observed** that this requirement is obfuscated by a contradiction noted in SVM/SEC/PRO/0007 – RMGA Customer

FUJ00080799

Service PCI Incident Management Process concerning which security team will investigate a PCI Minor Incident.

- Paragraph 2.12 - "Based on the evidence received the RMGA Security Operations Manager may declare an incident a PCI Minor Incident and will pass the investigation of the incident to the relevant security team within Fujitsu Corporate Security."

- Paragraph 2.14 - "(PCI) Minor Incidents will be passed to and investigated by the RMGA Security Team."

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, business recovery and continuity procedures. It is **observed** that a request for information was submitted but no response was achievable to meet the deadline requirements of this report. This does not imply non-compliance only that evidence was not made available.

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, data back-up processes. It is **observed** that the requirement for data back up processes to be captured within the Incident Response Plan was not evident within the available documentation.

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, analysis of legal requirements for reporting compromises. It is noted that SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.15.2 and Paragraph 2.16.5 captures the requirement that the investigation of a PCI Major Incident requires the formal engagement of an external Qualified Forensic Investigator (identified in the preferred supplier list) and approved by POL Head of Information Security and also by both MasterCard and VISA

  SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process also stipulates that the RMGA CISO or a nominated deputy will liaise with external organisations involved in the incident e.g. Third Parties, Forensic experts etc in preparing a Post Incident Report.

  However, it is **observed** that these are activities that occur when a major incident has been declared and that the prerequisite for the analysis of legal requirements for reporting compromises was not evident within the available documentation.

- PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, coverage and responses of all critical system components. It is **observed** that he requirement for coverage and responses of all critical system components to be captured within the Incident Response Plan were not evident within the available documentation.

- PCI-DSS 12.9.2 requires the incident response plan be tested at least annually. SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.19 correctly identifies that the PCI DSS security standard requires a documented incident process for any incident that affects or may affect the security of cardholder data. This documented process is required to be audited and tested annually and must be invoked should it be suspected that cardholder data may have been compromised.

  However, it is **observed** that a request for information was submitted but no response was achievable to meet the deadline requirements of this report. This does not imply non-compliance only that evidence was not made available.

- PCI-DSS 12.9.3 requires that there is designated, specific personnel to be available on a 24/7 basis to respond to alerts.

  It is **observed** that SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.8 states that the Initial Report or Incident Report must be passed to the first person in the list below. That person must respond with a positive written confirmation that the Report has been received and that they are dealing with it. If no such response is received within 24 hours then the Report must be passed to the next person on the list in exactly the same manner and each time allowing 24 hours for a response.

FUJ00080799

Internal Auditor Comment:

The assessment of the contents of this report will determine whether the incident is categorised as a minor or major incident. With the current cascade method there is the potential that an initial / incident report will not be assessed for up to 4 days. This has major downstream impacts for the subsequent handling of the incident.

- PCI-DSS 12.9.5 requires the inclusion of alerts from intrusion detection, intrusion-prevention, and file-integrity monitoring systems. It is recognised that the SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.16.1 captures the fact that, "The channels that might receive calls from internal parties or POL could be Business Service Centres, RMGA Corporate Security Centre, POL Security Team, and RMGA Service Desk."

  However it is **observed** that the explicit PCI requirement was not evident within the available documentation.

- PCI-DSS 12.9.6 requires the development of processes to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. Whilst a lessons learnt process is captured in referenced HNG-X Incident Management documentation is **observed** that the explicit PCI requirement was not evident within SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process

FUJ00080799

5. Observations & Non-conformities

The following Observations and Issues (Non-conformities) were raised during the course of this assessment

Issue Details

Reference / Sequence	1	**Date of Observation**	30/01/09
Category	**Issue**	**Standard / Section**	ISO 27001 13.1.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Documents Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

Information security events shall be reported through appropriate management channels as quickly as possible. SVM/SEC/POL/0003 V3.0- RMGA Information Security Policy states "Ensure information security events and weaknesses associated with RMGA information systems are communicated in a manner allowing timely corrective action to be taken and as referenced in CS/PRO/018 (RMGA Customer Service Incident Management Process)."

Internal Auditor Comment:

It is raised as an **issue** that CS/PRO/018 was made available by the Document Control Manager and it is entitled "Release 1c SYSTEM ENVIRONMENT: Processes and Procedures".

Document Control Manager Response:

"The correct reference for the Incident Management Process is SVM/SDM/PRO/018 - clearly there is confusion over the similar reference numbers although I don't think the documents are connected in any other way."

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	2	**Date of Observation**	24/01/09
Category	**Issue**	**Standard / Section**	ISO 27001 13.1.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location	Various	**Division**	RMGA
Interviewee	Various	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

It is noted that SVM/SDM/PRO/0018 V2.0 - POA Customer Service Incident Management Process, Paragraph 9.6.1.1 clearly states that, "Anyone reporting a security Incident should be encouraged to notify their Line Manager in the first instance"

Two members of the Application Solutions Development Team, a member of the IS Design Team and a Network Engineer from IS Implementation were requested to identify who they should report security incidents to.

It is raised as an **issue** that one was unsure how Information Security incidents should be reported as there has not been any requirement to date. Another specified that the incident should be reported to the Account Security Team. A third offered CS-Security. The fourth offered 3 possible reporting methods including via the online reporting form and the word version of this form and via 7799.

Notes

All of these responses are not in accordance with RMGA Information Security Policy, Paragraph 13.1.1 and POA Customer Service Incident Management Process, Paragraph 9.6.1.1

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	3	**Date of Observation**	22/01/09
Category	**Issue**	**Standard / Section**	ISO 27001 13.1.2
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location	Various	**Division**	RMGA
Interviewee	Various	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

There is a requirement that all employees understand that they should not try to test a suspected weakness or prove that it is real.

Two members of the Application Solutions Development Team were asked that if they suspected that there is a security weakness in any area of HNG-X would they attempt to prove the validity of the weakness prior to reporting.

It is raised as an **issue** that one responded that, "dependent on context and assessed immediacy and severity of risk. If risk was assessed as immediate and severe I would report without testing. If low I would seek to prove." Another responded that, "Yes, I would confirm it with one of my technicians."

This is contrary to RMGA Information Security Policy which stipulates in Paragraph 13.1.2, "RMGA staff must be aware that they should not, in any circumstances, attempt to prove a suspected weakness themselves. If such a course of action resulted in a security Incident then it may be treated as a disciplinary issue."

Notes

Internal Auditor Comment:

It should also be noted that there is the potential for managerial pressure to render subordinate staff ie: the technician, to be in breach of policy.

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	4	**Date of Observation**	30/01/09
Category	**Observation**	**Standard / Section**	ISO 27001 13.1.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

There is a requirement that Information security events shall be reported through appropriate management channels as quickly as possible. It is **observed** that SVM/SDM/PRO/0018 V2.0 - POA Customer Service Incident Management Process, Paragraph 9.1, states that, "This annex outlines the process regarding the investigation, and reporting of all security incidents concerning the HORIZON Network and all IT equipment."

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	5	**Date of Observation**	30/01/09
Category	**Observation**	**Standard / Section**	ISO 27001 13.1.2
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

It is **observed** that the formal incident response and escalation procedure as captured in SVM/SEC/POL/0003 V3.0- RMGA Information Security Policy, Paragraph 13.1.2, contains an incorrect document reference to CS/PRO/018.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	6	**Date of Observation**	30/01/09
Category	**Observation**	**Standard / Section**	ISO 27001 13.2.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

It is **observed** that the formal incident response and procedures as captured in SVM/SEC/POL/0003 V3.0-RMGA Information Security Policy, Paragraph 13.2.1, contains an incorrect document reference to CS/PRO/018.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	7	**Date of Observation**	23/01/09
Category	**Observation**	**Standard / Section**	PCI-DSS 11.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Bill Membery	**Interviewee's Role**	TSS
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

PCI-DSS 11.1 requires that there is a test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. It is **observed** that the documentation reviewed does not include any specific references for a response in the in the event of unauthorized wireless devices are detected.

Notes

Furthermore wider discussion should be considered concerning the deployment of wireless IDS / IPS to identify all / any wireless devices within HNG-X. It was indicated that this may only occur within Data Centre and Corporate support facilities and the frequency of IDS / IPS deployment to monitor for wireless devices was not available but described as potentially “sporadic”. No assurances of their deployment within other HNG-X areas could be given.

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	8	**Date of Observation**	30/01/09
Category	**Observation**	**Standard / Section**	PCI DSS 12.5.3
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location	IRE11	**Division**	RMGA
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

PCI-DSS 12.5.3 requires the establishment, documentation, and distribution security incident response and escalation procedures to ensure timely and effective handling of all situations. It is **observed** that SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process has been produced, however it is recognised that this has not obtained senior management approval.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	9	**Date of Observation**	24/11/08
Category	**Observation**	**Standard / Section**	PCI-DSS 12.9.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at a minimum, roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands.

It is **observed** that within SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process, Table 1, there is a communication strategy that captures the main components of the process in defining and managing a PCI incident.

However, whilst roles are referred to within the PCI Incident Response Plan the responsibilities are not explicitly defined although mention is made in within the document of the functions the Operations Security Manager and CISO play during the escalation and management process.

References are made to

- RMGA Security
- Fujitsu Corporate Security (for minor PCI Incidents)
- RMGA Operations Director
- Information Security Incident Manager
- RMGA Crisis Management Team

However, their responsibilities are not clearly defined.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	10	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.1
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at a minimum, roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands.

It is **observed** that within SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process, Paragraph 2.22, the contact information for key PCI Incident Response Personnel that the RMGA CISO mobile phone number is incomplete.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	11	**Date of Observation**	30/01/09
Category	**Observation**	**Standard / Section**	PCI-DSS 12.9.1
Corporate Process		**Local Process**	ISMS
Unit	RMGA	**Country**	UK
Location		**Division**	RMGA
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, specific incident response procedures. It is **observed** that this requirement is obfuscated by a contradiction noted in SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process concerning which security team will investigate a PCI Minor Incident.

- Paragraph 2.12 - "Based on the evidence received the RMGA Security Operations Manager may declare an incident a PCI Minor Incident and will pass the investigation of the incident to the relevant security team within Fujitsu Corporate Security."
- Paragraph 2.14 - "(PCI) Minor Incidents will be passed to and investigated by the RMGA Security Team."

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

Issue Details

FUJ00080799

Reference / Sequence	12	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.1
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee		**Interviewee's Role**		
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, business recovery and continuity procedures. It is **observed** that a request for information was submitted but no response was achievable to meet the deadline requirements of this report.

Notes

This does not imply non-compliance only that evidence was not made available.

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	13	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.1
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, data back-up processes. It is **observed** that the requirement for data back up processes to be captured within the Incident Response Plan was not evident within the available documentation.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	14	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.1
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, analysis of legal requirements for reporting compromises. It is noted that SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.15.2 and Paragraph 2.16.5 captures the requirement that the investigation of a PCI Major Incident requires the formal engagement of an external Qualified Forensic Investigator (identified in the preferred supplier list) and approved by POL Head of Information Security and also by both MasterCard and VISA

SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process also stipulates that the RMGA CISO or a nominated deputy will liaise with external organisations involved in the incident e.g. Third Parties, Forensic experts etc in preparing a Post Incident Report.

However, it is **observed** that these are activities that occur when a major incident has been declared and that the prerequisite for the analysis of legal requirements for reporting compromises was not evident within the available documentation.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	15	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.1
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.1 requires the creation and implementation of an incident response plan in the event of system breach that addresses, at minimum, coverage and responses of all critical system components. It is **observed** that he requirement for coverage and responses of all critical system components to be captured within the Incident Response Plan were not evident within the available documentation.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	16	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.2
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.2 requires the incident response plan be tested at least annually. SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.19 correctly identifies that the PCI DSS security standard requires a documented incident process for any incident that affects or may affect the security of cardholder data. This documented process is required to be audited and tested annually and must be invoked should it be suspected that cardholder data may have been compromised.

However, it is **observed** that a request for information was submitted but no response was achievable to meet the deadline requirements of this report.

Notes

This does not imply non-compliance only that evidence was not made available.

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	17	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.3
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Document Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.3 requires that there is designated, specific personnel to be available on a 24/7 basis to respond to alerts.

It is **observed** that SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.8 states that the Initial Report or Incident Report must be passed to the first person in the list below. That person must respond with a positive written confirmation that the Report has been received and that they are dealing with it. If no such response is received within 24 hours then the Report must be passed to the next person on the list in exactly the same manner and each time allowing 24 hours for a response.

Internal Auditor Comment:

The assessment of the contents of this report will determine whether the incident is categorised as a minor or major incident. With the current cascade method there is the potential that an initial / incident report will not be assessed for up to 4 days. This has major downstream impacts for the subsequent handling of the incident.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	18	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.5
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Documents Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.5 requires the inclusion of alerts from intrusion detection, intrusion-prevention, and file-integrity monitoring systems. It is recognised that the SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process Paragraph 2.16.1 captures the fact that, "The channels that might receive calls from internal parties or POL could be Business Service Centres, RMGA Corporate Security Centre, POL Security Team, and RMGA Service Desk."

However it is **observed** that the explicit PCI requirement was not evident within the available documentation.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	

FUJ00080799

Issue Details

Reference / Sequence	19	**Date of Observation**	30/01/09	
Category	**Observation**	**Standard / Section**	PCI-DSS	12.9.6
Corporate Process		**Local Process**	ISMS	
Unit	RMGA	**Country**	UK	
Location		**Division**	RMGA	
Interviewee	Documents Review	**Interviewee's Role**	Internal Auditor	
Area Contact	Howard Pritchard	**Assessor's Name**	Chris Cole	

Issue

PCI-DSS 12.9.6 requires the development of processes to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. Whilst a lessons learnt process is captured in referenced HNG-X Incident Management documentation is **observed** that the explicit PCI requirement was not evident within SVM/SEC/PRO/0007 – RMGA Customer Service PCI Incident Management Process.

Notes

Corrective Action Details

Corrective Action To Be Taken

Actionee		**Reviewing Manager**	
Forecast Completion Date		**Actual Completion Date**	
Verified By		**Date Verified**	