

**UNCLASSIFIED (RECLASSIFY after first entry)**

Blackberry Post Implementation Questionnaire V1.0



**Australian Government**  
**Department of Defence**

**Defence Signals Directorate**

**Blackberry Post Implementation  
Review**

**VERSION 1.0**

Point of Contact: Advice and Assistance Team

Phone: (02) 6265 0197

Email: [assist@dsd.gov.au](mailto:assist@dsd.gov.au)

Organisation: \_\_\_\_\_

Organisation Delegate: \_\_\_\_\_

Assessor: \_\_\_\_\_

© Commonwealth of Australia 2006

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the *Copyright Act 1968*, all other rights are reserved.

Page 1

**UNCLASSIFIED (RECLASSIFY after first entry)**

© Commonwealth of Australia 2006

**UNCLASSIFIED (RECLASSIFY after first entry)**

Blackberry Post Implementation Questionnaire V1.0

**Document Change Record**

<b>Version</b>	<b>Changed By</b>	<b>Date</b>	<b>Changes</b>
1.0	DSD Advice and Assistance Team	March 2006	Initial draft

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## Table of Contents

Document Change Record .....	2
Table of Contents .....	3
Purpose .....	4
Related Documents.....	4
Key Words.....	5
Definitions.....	5
Compliance .....	5
Checklist Guidance .....	6
Requirements.....	6
Sub-requirements .....	6
When to tick or cross .....	7
Supplying comments.....	7
Checking the implementation .....	7
Additional Requirements .....	7
Comments .....	7
Statement of Compliance.....	8
1.1 Government Policy, Approvals and Risk Assessment.....	9
1.2 Organisation Policy, Procedures, Plans, User Awareness and Training.....	10
1.3 Relevant ACSI 33 Policy .....	10
1.3.1 Protective Markings in Email .....	10
1.3.2 Portable Computers and Personal Electronic Devices.....	12
1.3.3 Password Selection Policy.....	12
1.3.4 Telephones and Pagers.....	13
1.3.5 Wireless Communications .....	13
1.4 BlackBerry Infrastructure.....	14
1.4.1 BlackBerry Enterprise Server (BES) Configuration .....	14
1.4.2 BES IT Policy Settings.....	14
1.4.3 Network Architecture.....	14
1.5 Review and Audit .....	15
2 If BlackBerry is used with ICT systems that process CABINET-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED information.....	16
2.1 Deviation from a "SHOULD NOT" .....	16
2.2 Protective Markings in Email.....	16
2.3 Waivers .....	16
2.4 Relevant Outstanding Security Issues .....	17
2.5 Implementation Review.....	17

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## Purpose

The following review is designed to assist assessors in the conduct of a Blackberry Post-Implementation Review to Defence Signals Directorate (DSD) and Australian Government Information Management Office (AGIMO) standards. This document can be used by:

- I-RAP assessors if employed by an agency for this purpose, and
- DSD.

This review **MUST** be completed within twelve months of the 'live' production implementation of BlackBerry.

Upon completion of a Post Implementation Review DSD will contact the agency to organise a post implementation interview. The DSD point of contact being the Team Leader, Advice and Assistance Team, Information Security Group.

## Related Documents

Related documentation for assessors to seek further guidance include:

- Protective Security Manual (PSM) 2005, Attorney General's Department;
- Australian Government Information & Communications Technology Security Manual (ACSI 33) March 2006, Information Security Group, Defence Signals Directorate;
- Policy and Guidance for the Use of BlackBerry by the Australian Government, Version March 2006, Information Security Group, Defence Signals Directorate;
- Australian Government Information Management Office, Implementation Guide for Email Protective Markings for Australian Government Agencies, v1 October 2005.
- Australian Government Information Management Office, Email Protective Marking Standard for the Australian Government, v1 October 2005.
- Australian Government Information Management Office, Instructions On The Allocation And Use Of BlackBerry In The Australian Government, October 2005.
- Australian Government Information Management Office, Better Practice Guidance #23 - Use of BlackBerry Devices, October 2005.
- Australian Government Information Management Office, Better Practice Guidance #24 - User Requirements for BlackBerry Devices, October 2005.

Note: a working level familiarity with these documents is assumed.

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## Key Words

The table below defines the keywords used within this document to indicate the compulsory requirements for statement of compliance.

Keyword	Interpretation
<b>MUST</b>	The item is mandatory for compliance.
<b>MUST NOT</b>	Non-use is mandatory for compliance.
<b>SHOULD</b>	Valid reasons to deviate from the requirement may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by an authorised organisational security representative.  <b>Note:</b> Organisations deviating from a <b>SHOULD</b> , <b>MUST</b> document the reason(s) for doing so.
<b>SHOULD NOT</b>	Valid reasons to implement the item may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by an authorised organisational security representative.  <b>Note:</b> Organisations deviating from a <b>SHOULD NOT</b> , <b>MUST</b> document the reason(s) for doing so.
<b>RECOMMENDS</b> <b>RECOMMENDED</b>	A recommendation or suggestion.  <b>Note:</b> Organisations deviating from a <b>RECOMMENDS</b> or <b>RECOMMENDED</b> , are encouraged to document the reason(s) for doing so.

## Definitions

**Organisation**, or any of its derivations, is used to refer to any Government Agency or Government Department as well as any Service Provider seeking to provide services to Australian Government.

Please refer to the glossary in ACSI 33 for a comprehensive list of technical definitions.

## Compliance

I-RAP assessors **MUST** forward the following documents once the assessment is completed:

- completed checklist;
- additional requirements;
- comments; and
- a statement indicating the result of the assessment.

IRAP Assessors please forward completed documentation to:

The I-RAP Manager  
Information Security Group  
Defence Signals Directorate  
Locked Bag 5076  
KINGSTON ACT 2604

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## Checklist Guidance

This section provides guidance upon answering items within the checklist and provides some detail upon the obligation of the assessor.

Checklist components must not be scoped out during a review.

The titles of the documents given in this checklist are guidelines; organisations may title their policies sections/documents as appropriate.

## Requirements

Each checklist consists of requirements, designated as a bolded capital 'R' followed by an outline number. The complete requirement consists of: the requirement number, the requirement itself, and a checkbox.

For example:

**R1** Organisations **MUST** keep records. (ACSI 33 2.8.12) |

Bolded, capitalized words are key words, as described above. Key words stipulate a condition upon the requirement, and must be considered when deciding whether a requirement has or has not been met by an organisation.

Assessors should either tick or cross a requirement to indicate that an organisation has succeeded or failed in answering the requirement. The reviewer should record any comments using the comments table that is attached at the end of this checklist. Comments must be submitted with the checklist documentation.

Bracketed information towards the end of a requirement's wording implies a reference. The material that is referenced should be examined for further detail or for justification of a requirement.

DSD may prescribe requirements beyond the minimum as stated in ACSI 33 in order to achieve greater granularity for the certification context especially where requirements are drawn from the range of reference materials.

## Sub-requirements

Some requirements are broken into sub-requirements. Sub-requirements are designated with a two-level number, and a parent requirement from which all sub-requirements stem from.

For example:

**R2** Organisations **MUST**: |   
    **R2.1** Keep records; and |   
    **R2.2** Examine each record. |

The key word in the parent item '**MUST**' applies to all sub-requirements. Organisations must achieve a tick in each sub-requirement box in order to satisfy the parent requirement.

Consider another example:

**R3** Organisations **SHOULD**: |   
    **R3.1** Perform audits annually; and |   
    **R3.2** Report upon audit results. |

## UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

The key word in the parent item '**SHOULD**' applies to all sub-requirements, just like the first sub-requirement example given above this example. Organisations must achieve a tick in each sub-requirement box in order to satisfy the parent requirement. This statement should be considered in light of the guidance provided in 'When to tick or cross'.

### When to tick or cross

Ticks need only be given where the key word of the requirement is properly addressed.

For a '**MUST / MUST NOT**' you should tick when:

- The requirement is complied with explicitly.

For a '**SHOULD / SHOULD NOT**' you should tick when:

- The requirement is complied with explicitly; or
- Valid reasons exist for non-compliance and these reasons are documented.

For a '**RECOMMEND**' or any of its derivations you should tick when:

- The requirement is complied with explicitly.
- Valid reasons exist for non-compliance and these reasons are provided to the reviewing authority.

You should mark a requirement with a cross in all other situations.

### Supplying comments

Assessors must supply comments using the table supplied at the back of this checklist. Specific guidance on using the comments section is provided just prior to the comments table.

The comments table allows you to register comments against an individual requirement or sub-requirement.

### Checking the implementation

Assessors must verify consistency between policy, plans, and procedures. In order to verify that procedures mentioned within policy documentation are operational, assessors must have the organisations IT Security Advisor (ITSA), IT Security Manager (ITSM), or an authorised substitute demonstrate that the procedure is in use.

### Additional Requirements

Additional requirements may arise from an organisation's Risk Assessment. These requirements need to be documented and submitted to the Certifying Authority.

### Comments

Provision is made at the back of the checklist for assessors to provide their comments against individual requirements.

Assessors must comment upon individual requirements within the following checklist. Comments must provide an indication of how well an organisation complies with each requirement.

## **UNCLASSIFIED (RECLASSIFY after first entry)**

Blackberry Post Implementation Questionnaire V1.0

### **Statement of Compliance**

The formal Statement of Compliance must include signoff by the assessed organisation. The statement must stipulate that, to the best of the ITSA/ITSM's knowledge, the assessor who signed the Statement of Compliance actively participated in conducting the assessment.

Document any recommendations based on non-mandatory best practice guidelines that have not been implemented by the agency.

At minimum the Statement of Compliance, must provide the following information:

- Whether compliance was achieved;
- Comment on the requirement to inform DSD of any new or existing consideration that may render a previously compliant system non-compliant;
- Inform organisations that they should provide regular advice to DSD on significant changes to any analysed threat level; and
- Detail the conditions of maintaining compliance.

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## 1.1 Government Policy, Approvals and Risk Assessment

Requirements contained in this section are derived from the Department of Finance and Administration – Instructions on the Allocation and Use of BlackBerry in the Australian Government, AGIMO Better Practice Guidance No. 23 and No. 24. and DSD ICT Security Policy for the Use of BlackBerry by the Australian Government.

- |  |                          |
|--|--------------------------|
| <b>R1.</b> The organisation's head <b>MUST</b> approve the business requirement and use of BlackBerry.   | <input type="checkbox"/> |
| <b>R2.</b> Organisations <b>MUST NOT</b> use BlackBerry for the transmission or storage of CABINET-IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET information.     | <input type="checkbox"/> |
| <b>R3.</b> Organisations <b>MUST NOT</b> use BlackBerry with ICT systems that process CONFIDENTIAL, SECRET or TOP SECRET information.  | <input type="checkbox"/> |
| <b>R4.</b> Organisation's <b>MUST</b> conduct a Risk Assessment (RA) on the use and implementation of BlackBerry.  | <input type="checkbox"/> |
| <b>R5.</b> The RA <b>MUST</b> contain:   |                          |
| <b>R5.1</b> Documented analysis of the identified risks.   | <input type="checkbox"/> |
| <b>R5.2</b> Prioritisation of the identified risks, detailing target risk levels/predetermined standards.  | <input type="checkbox"/> |
| <b>R5.3</b> Detailed risk treatment table.   | <input type="checkbox"/> |
| <b>R6.</b> The RA <b>MUST</b> be signed by the organisation head or their delegate confirming they have read and accepted the RA, and are willing to accept the identified residual level of risk. | <input type="checkbox"/> |
| <b>R7.</b> The organisation <b>MUST</b> comply with DSD, ICT Security Policy on BlackBerry   | <input type="checkbox"/> |

## UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

### 1.2 Organisation Policy, Procedures, Plans, User Awareness and Training

Requirements contained in this section are derived from AGIMO Better Practice Guidance No. 23 and No. 24, DSD ICT Security Policy for the Use of BlackBerry by the Australian Government and ACSI 33.

- R8.** The organisation **MUST** have policies and associated procedures for the use of the BlackBerry service.
- R9.** There **MUST** be a clear correlation between the Risk Assessment (RA) and the organisation's BlackBerry policies.
- R10.** BlackBerry policy and procedures **SHOULD** contain instructions on:
- R10.1** Activation of the "Lock Handheld" and "Kill Handheld" signals.
  - R10.2** Sharing of BlackBerry devices between users.
  - R10.3** The action users must follow in the event of loss or damage to the device.
- R11.** Organisations **MUST** ensure that staff acknowledgement of the policies and associated procedures are recorded before they are allowed to use the service.
- R12.** Prior to staff being issued with BlackBerry devices for use, they **SHOULD** be trained in the use of the system, including security requirements and the application of e-mail protective markings.
- R13.** Organisations **MUST** ensure user passwords for unlocking the BlackBerry device meet the password selection policy of ACSI 33.
- R14.** Organisations **MUST** ensure that BlackBerry handheld devices running version 3.6 of the handheld software are stored and handled in accordance with the security classification of the information on them.
- R15.** BlackBerry devices **MUST** be supplied, supported, managed and used in accordance with an organisations ICT policy.

### 1.3 Relevant ACSI 33 Policy

These requirements contained in the following sections have been derived from ACSI 33 Part 3 Chapters 4, 5, 6, 8, and 10.

#### 1.3.1 Protective Markings in Email

These requirements are derived from the Department of Finance and Administration – Instructions on the Allocation and Use of BlackBerry in the Australian Government, Email Protective Marking Standard for the Australian Government, Implementation Guide for Email Protective Markings for Australian Government Agencies and ACSI 33.

- R16.** Organisations **MUST** implement the relevant requirements for email protective markings as per the most current release of ACSI 33.

## UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

- R16.1** Agencies **MUST** have policy governing the use of email.
- R16.2** Agencies **MUST** ensure that the standards for blocking unmarked and outbound emails are applied to automatically forwarded emails.
- R16.3** Agencies **SHOULD** warn staff that the automatic forwarding of email to other staff members may result in the new recipient seeing material that:  
a) They do not have a need to know, or  
b) The intended recipient and/or sender considered private.
- R16.4** Agencies **MUST** ensure that all agency-originated emails that contain security classified information are marked with a protective marking that identifies the maximum classification and set of caveats for the information in the body of the email and any attachments.
- R16.5** Users **MUST** select or insert protective markings on all user generated emails.
- R16.6** Organisations **SHOULD** prevent staff from sending unmarked emails by blocking the email at:  
a) The user's computer, and/or  
b) The email server.
- R16.7** Organisations **MUST** configure systems to block any outbound emails with a valid protective marking indicating that the content of the email exceeds the classification of the:  
a) Receiving system, and/or  
b) The path over which the email would be transferred.
- R16.8** Organisations **SHOULD** log the fact that emails were blocked.
- R17.** The organisation **MUST** implement protective markings in accordance with the AGIMO Implementation Guide and Standards for email protective markings.
- R17.1** The implemented protective markings are in accordance with the format and location as specified in the Standard.
- R17.2** Protective markings are included in the emails Subject field and/or the X-headers such that they are clearly visible to the recipient in another agency.
- R18.** Organisations **MUST** security classify and protectively mark all email including to/from BlackBerry.
- R19.** Controls **MUST** also be implemented at the email server(s) and gateway(s) to restrict the delivery of inappropriate security classified information into and out of an agency, including to BlackBerry.
- R20.** Organisations **MUST** ensure that email that does not have a protective marking is not transmitted to BlackBerry.

## UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

### 1.3.2 Portable Computers and Personal Electronic Devices

- R21. If intending to use portable computers or PEDs to process classified information, organisations **SHOULD** ensure that all data collection and communications functions of the device not identified as business requirements, are removed or disabled as effectively as possible within the limitations of the particular device.  
(e.g. Bluetooth, infrared)
- R22. Organisations **SHOULD** put a protective marking on all portable computers and PEDs.
- R23. Organisations **SHOULD** put a label warning against unauthorised use on all portable computers and PEDs.
- R24. An additional label **SHOULD** be affixed requesting that a lost portable computer or PED be handed into any Australian Police Station or, if overseas, an Australian Embassy, Consulate or High Commission.
- R25. Organisations **SHOULD** develop an emergency destruction plan for any portable or PED used in high risk environments.
- R26. Organisations **MUST NOT** permit privately owned or managed BlackBerry handhelds to connect to classified agency systems.
- R27. Organisations **MUST** reconfigure the BlackBerry default IT policy settings to reflect agency IT policies prior to providing handhelds to users for activation.

### 1.3.3 Password Selection Policy

- R28. Organisations **MUST** ensure that users implement a password to control access to the BlackBerry handheld that either:  
a) Is a minimum of 12 characters with no complexity testing, or  
b) Meet the password selection policy in ACSI 33.
- R29. Organisations **SHOULD**:  
a) Require passwords to be changed at least every 90 days,  
b) Prevent users from changing their passwords more than once a day,  
c) Check passwords for poor choices'  
d) Force the user to change an expired password on initial logon or if reset, and  
e) **NOT** allow passwords to be reused within 8 password changes
- R30. Organisations **SHOULD**:  
a) Configure BlackBerry devices with a screen and/or session lock'  
b) Configure the lock to activate after no more than 15 minutes of user inactivity,  
c) Configure the lock to completely conceal all information on the screen,  
d) NOT permit the screen to appear to be turned off while the session is still active,  
e) Require the user to reauthenticate before the system is unlocked, and  
f) NOT permit users to disable the locking mechanism.

## UNCLASSIFIED (RECLASSIFY after first entry)

### Blackberry Post Implementation Questionnaire V1.0

- R31.** Organisations **SHOULD**:
- a) Lock user accounts after a specified number (a minimum of 3 up to a maximum of 5) of failed logon attempts,
  - b) Remove or suspend user accounts as soon as possible after the user no longer requires access due to changing roles or leaving the agency, and
  - c) Suspend inactive accounts after a specified number of days.
- 

#### 1.3.4 Telephones and Pagers

- R32.** Organisations **SHOULD** ensure that staff are aware of the audio risk posed by using (BlackBerry) mobile phones in areas where classified conversations may occur.
- R33.** Organisations **SHOULD NOT** use (BlackBerry) mobile phones for the transmission of IN-CONFIDENCE information unless:
- a) The security they use has been approved by DSD, or
  - b) They can ensure that:
    - 1) The (BlackBerry) mobile phone user is located within Australia, and
    - 2) Only voice traffic is passed.
- 
- R34.** Organisations **MUST NOT** use (BlackBerry) mobile telephones for the transmission of RESTRICTED or PROTECTED information unless the security they use has been approved by DSD.
- R35.** Organisations **MUST NOT** use paging services (e.g. SMS, MMS) to transmit classified information.

#### 1.3.5 Wireless Communications

- R36.** Organisations **SHOULD NOT** use wireless communications (e.g. Bluetooth) for the transmission of classified information.
- R37.** Organisations **MUST NOT** enable Bluetooth serial port connection on any BlackBerry handheld.
- R38.** Organisations **MUST** disable the wireless functionality of BlackBerry handhelds when in areas processing CONFIDENTIAL or SECRET information, by:
- Turning off the RF Wireless function,
  - Turning off the BlackBerry handset, or
  - Removing the battery.
- 
- R39.** Organisations **MUST** comply with ACSI 33 policy regarding the use of PEDs in classified environments.

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## 1.4 BlackBerry Infrastructure

These requirements are derived from the ICT Security Policy for the Use of BlackBerry by the Australian Government.

### 1.4.1 BlackBerry Enterprise Server (BES) Configuration

- R40. Organisations using BlackBerry **MUST** use the “Enterprise” (BES) service.
- R41. Organisations may use versions 3.6 to 4.x for the transmission and storage of UNCLASSIFIED, X-IN-CONFIDENCE and RESTRICTED information.
- R42. Organisations **MUST NOT** use peer-to-peer (“PIN to PIN”) communications to transmit classified information.
- R43. Organisations **MUST NOT** use the “BlackBerry Desktop Redirector”.
- R44. It is **RECOMMENDED** that the “Mobile Data Service” (MDS) be configured to use the organisation’s proxy server.
- R45. Where RIM have provided the functionality to do so, organisations **SHOULD** separate BES services by installing them on different servers.
- R46. Organisations **SHOULD** manage the BES via a physical console.
- R47. Organisations **SHOULD** disable the use of the Wireless Transport Layer Security (WTLS) mode.
- R48. Organisations **SHOULD** apply the relevant patches as specified in ICT Security Policy for the Use of BlackBerry by the Australian Government.
- R49. It is **RECOMMENDED** that organisations install a host-based firewall on the BES and that it is configured to limit traffic to the minimum necessary to allow the BES to perform its authorised tasks.

### 1.4.2 BES IT Policy Settings

- R50. Organisations **MUST** configure all IT policies within the BES to at least meet those specified in the DSD *ICT Security Policy for the Use of BlackBerry by the Australian Government*. This document is available from the Quick Links section of the DSD website, [www.dsd.gov.au](http://www.dsd.gov.au)

### 1.4.3 Network Architecture

- R51. Organisations **SHOULD** install the BlackBerry router in a neutral subnetwork between the trusted corporate LAN and the Internet.
- R52. It is **RECOMMENDED** that organisations install an internal firewall between the BES and their internal mail servers.
- R53. Organisations **MUST** ensure that information is transferred between BlackBerry handhelds and the agency’s systems in accordance with ACSI 33.

# UNCLASSIFIED (RECLASSIFY after first entry)

Blackberry Post Implementation Questionnaire V1.0

## 1.5 Review and Audit

These requirements are derived from the AGIMO Better Practice Guidance #23.

- R54. Organisations **SHOULD** undertake internal – and from time-to-time external – checks of compliance with policies governing the use of BlackBerry devices.
- R55. Organisations **SHOULD** undertake regular reviews of agency policies, to test their currency and adequacy.
- R56. Organisations **SHOULD** perform a technical review designed to reveal any previously undetected compromises or other failures of security at least annually.

## 2 If BlackBerry is used with ICT systems that process CABINET-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED information

These requirements contained in this section are derived from the:

- Australian Government Information and Communications Technology Security Manual (ACSI 33) Part 1, Part 2 Chapter 7
- Department of Finance and Administration – Instructions on the Allocation and Use of BlackBerry in the Australian Government
- AGIMO Better Practice Guidance No. 23 and No. 24
- DSD ICT Security Policy for the Use of BlackBerry by the Australian Government

### 2.1 Deviation from a “SHOULD NOT”

R57. The organisation **MUST** document the reasons for deviating from a “**SHOULD NOT**”.

R58. The documentation **MUST** include:

R58.1 The reasons for the deviation

R58.2 An assessment of the residual risk resulting from the deviation

R58.3 The date by which the decision to deviate from a “**SHOULD NOT**” will be reviewed

R58.4 The ITSA’s involvement in the decision

R58.5 CEO approval

### 2.2 Protective Markings in Email

R59. Controls **MUST** also be implemented at the email server(s) and gateway(s) to restrict the delivery of inappropriate security classified information into and out of an agency, including to BlackBerry.

R60. Organisations **MUST** ensure that email that does not have a protective marking is not transmitted to BlackBerry.

### 2.3 Waivers

R61. The organisation **MUST NOT** have waivers in place relevant to the implementation of BlackBerry.

## 2.4 Relevant Outstanding Security Issues

**R62.** The organisation **MUST NOT** have any relevant outstanding issues arising from:

**R62.1** Internal or external system security reviews

**R62.2** Internal or external audits

## 2.5 Implementation Review

**R63.** When did organisation first implement BlackBerry?

Pilot: \_\_\_\_\_

Full  
Implementation: \_\_\_\_\_

## **Comments**

The following table will assist you to record responses to Post-Implementation Review.

You should enter a response for each check-marked requirement in the checklists, even where you do not wish to record any issues. This will assist in preparing your statement of compliance report, and will assist in maintaining appropriate historical records. It will also keep numbering consistent.

---

<b>Requirement</b>	<b>Comment</b>
<b>R1</b>	
<b>R2</b>	