

Leicestershire Police Authority

Internal Audit Report

ITIL Self Assessment Review (12.09/10)

22 December 2009

FINAL

Contents

Contents

| | Section | Page |
|---|---|------|
| 1 | Executive Summary | 1 |
| 2 | Action Plan | 5 |
| 3 | Findings and Recommendations | 7 |
| 4 | Appendix A: Detailed ITIL Compliance Findings | 10 |
| 5 | Scope and Acknowledgements | 22 |

ASSIGNMENT CONTROL:

| | | | |
|-----------------------------|-------------------------|------------------------|-----------------------------------|
| Debrief meeting: | 18 November 2009 | Auditors: | Chris Harris, Partner |
| Draft report issued: | 2 December 2009 | | Suzanne Lane, Client Manager |
| Responses received: | 21 December 2009 | | Steve Snaith, ISA Director |
| | | | Olivia Kyi Phyu, ISA Manager |
| | | | Mark Shutt, Senior ISA Consultant |
| Final report issued: | 22 December 2009 | Client sponsor: | Tim Glover, Head of IT |



This review has been performed using RSM Bentley Jennison's bespoke internal audit methodology, **i-RIS**.

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regard to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

This report is prepared solely for the use of Authority and senior management of Leicestershire Police Authority. Details may be made available to specified external agencies, including external auditors, but otherwise the report should not be quoted or referred to in whole or in part without prior consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended for any other purpose.

© 2009 Bentley Jennison Risk Management Ltd

Bentley Jennison Risk Management Ltd

Bentley Jennison Risk Management Ltd is wholly owned by RSM Bentley Jennison
Registered in England and Wales No. 3444889
Registered Office 1 Hollinswood Court Stafford Park 1 Telford TF3 3DE

1 Executive Summary

1.1 Introduction

An audit of the ITIL self assessment evidence was undertaken as part of the approved internal audit periodic plan for 2009/10.

The 'Information Systems Strategy for the Police Service' (ISS4PS) directive, which outlines a framework to improve police performance and efficiencies, has made ITIL a required practice for all forces across the country.

The Leicestershire Police Authority (the Authority) is working towards implementing selected areas of the ITIL accreditation as part of the IT Service Management Strategy, in line with the National Policing Improvement Agency (NPIA) directive. The self assessment is broken down into 11 areas. These are:

- Service Management *
- Configuration Management
- Service Desk and Incident Management *
- Change Management *
- Problem Management *
- Release Management *
- Service Level Management *
- Service Continuity Management
- Availability Management
- Capacity Management
- Financial Management

The Authority has self-assessed all areas; however, for the formal 2010 HMIC (Her Majesty's Inspectorate of Constabulary) inspection, only the 6 areas marked with an asterisk will be included in the formal assessment.

The purpose of the self assessment is to:

- Assess how well IT is performing as a service provider in meeting business requirements as defined and driven by the business;
- Identify whether a satisfactory standard of ITSM is attained;
- Provides an objective prospective of the current operational process.

In accordance with the direction from the Association of Chief Police Officers (ACPO) ICT Service Management Board, the assessment of generic processes is based on ITIL Version 2. It is recognised that the Police Service will be adopting ITIL Version 3 at a future date. ITIL Version 2 provides the foundation of ITIL Version 3.

The specific risk considered for this review was "Robust controls do not exist over service management, change management and release management processes resulting in uncontrolled changes being promoted to the production environments and disruption, unauthorised alterations and errors".

This risk relates to the following objective: "Appropriate ITIL processes are in place to increase system integrity".

1.2 Scope of the review

The objective of our audit was to determine whether sufficient evidence is in place to support the compliance with ITIL Service Management, Change Management and Release Management.

Limitations to the scope of the audit:

The following limitations to the scope of the audit were agreed when planning the audit:

- Our review focussed on reviewing the evidence that the Authority has collated and presented to us to support its self assessment scores, in preparation of the formal HMIC assessment scheduled to commence in June 2010, for Service Management, Change Management and Release Management.
- Our review was limited to a review of the file of evidence and did not assess the operation/compliance with the controls presented to us.
- We did not review evidence in detail where the maturity level has been designated as less than 3 (refer to notes below). However, to assist the Authority, we did conduct a high level review of requirements not meeting the required standard and have provided commentary regarding this in Section 4 (as classified as N/A).
- Our work does not provide any guarantee against material error, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

Notes

A satisfactory standard of IT Service Management (ITSM) is deemed to be attained with a **minimum** maturity level of 3.

This maturity level reflects the fact that the process has been recognised and is documented but there is no formal agreement, acceptance and recognition of its role within ITSM as a whole. However, the process has a process owner, formal objectives and outputs with allocated resources, and is focused on the efficiency as well as the effectiveness of the process. Reports and results are produced and available for future reference.

The difference between maturity levels 2.5 and 3 is that maturity level 3 is a repeatable process which reliably produces defined outputs.

1.3 Conclusion

We have substantiated 9 out of 12 requirements of the Authority's key designated attainment levels, from the evidence collated in the central repository for each requirement, where the Authority self assessed the related score as 'Compliant'. Our overall results are presented in the table below and detailed in Section 4.

Out of 23 total requirements, 6 were designated by the Authority as non-compliant and 5 as only partially compliant regarding the related requirements. (refer to note 1 below).

Note 1

As agreed in the limitations to the scope, we have not provided an opinion where the maturity level is less than 3 (a rating of 'not compliant' or 'partial compliance').

The above conclusion is based on our assessment to substantiate the evidence collated, and in place against each ITIL attainment level. Table 1 below summarises our findings in this area.

Table 1: Summary of ITIL Attainment Level Testing

| Requirement Number | Self Assessment Score | Evidence Supports intended score | Requirement Number | Proposed score for version 7 of Toolkit | Evidence Supports intended score |
|--------------------|-----------------------|----------------------------------|--------------------|---|----------------------------------|
| 1.1 | Partial Compliance | N/A | 4.8 | Compliant | ✓ |
| 1.2 | Compliant | ✗ | 4.9 | Compliant | ✓ |
| 1.3 | Compliant | ✓ | 6.1 | Not Compliant | N/A |
| 1.4 | Compliant | ✓ | 6.2 | Not Compliant | N/A |
| 1.5 | Partial Compliance | N/A | 6.3 | Partial Compliance | N/A |
| 4.1 | Compliant | ✓ | 6.4 | Compliant | ✗ |
| 4.2 | Compliant | ✗ | 6.5 | Not Compliant | N/A |
| 4.3 | Compliant | ✓ | 6.6 | Partial Compliance | N/A |
| 4.4 | Compliant | ✓ | 6.7 | Not Compliant | N/A |
| 4.5 | Compliant | ✓ | 6.8 | Not Compliant | N/A |
| 4.6 | Partial Compliance | N/A | 6.9 | Not Compliant | N/A |
| 4.7 | Compliant | ✓ | | | |

To support the designated ITIL attainment levels which we were unable to fully verify, the Authority needs to address the areas outlined in the supporting action plan (also refer to section 4).

1.4 Recommendations Summary

The following table highlights for each ITIL assessment component, the number of requirements that were lacking the evidence to support the score that the Authority as designated as at the time of review in November 2009.

The Action Plan in Section 2 and the supporting Action Points in Section 4 detail the specific evidence that is required to support each requirement.

Recommendations made during this audit:

| | NO OF REQUIREMENTS WHERE THE EVIDENCE REVIEWED AT THE TIME OF THE AUDIT DID NOT SUPPORT PROPOSED SCORE |
|--------------------|--|
| SERVICE MANAGEMENT | 1 |
| CHANGE MANAGEMENT | 1 |
| RELEASE MANAGEMENT | 1 |

2 Action Plan

The priority of the findings and recommendations are as follows:

Significant: An absence of an appropriate level of evidence to support the Authority's allocated attainment level. This recommendation relates the evidence that must be collated to support the Authority's related scoring.

| Para | Recommendation | Categorisation | Accepted Y/N | Management comment | Implementation date | Manager responsible |
|-------|---|------------------|--------------|--|-----------------------------|---------------------|
| 3.1.1 | Management should ensure that adequate, detailed documentary evidence is in the central repository to support the attainment ratings assigned for each of the ITIL self assessment maturity questions. | Significant | Y | This will be achieved in time for the HMIC | 31 st March 2010 | Deviya Mistry |
| 3.1.2 | The authority should implement the 'Action Points' in Appendix A, in order to maintain the current ITIL attainment levels. | Significant | Y | The Action Points will be incorporated into the IT Business Plan which will be used as the Service Improvement Plan. | 31 st March 2010 | Tim Glover |
| 4.1.2 | To achieve the current level of the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> ▪ A Service Improvement / Management Plan which details the short term activities (e.g. 6 months), and high level medium term activities (12- 24 months). | Merits Attention | Y | The Business Plan will incorporate the Service Improvement Plan | 31 st March 2010 | Tim Glover |
| 4.2.2 | To achieve the current level of the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> ▪ Uniquely identifiable Request for Changes (RFC), and the request forms updated to allow a unique reference number; and ▪ The RFC register should be implemented and embedded within the change management process. | Merits Attention | Y | The change management process will be updated to include a unique identifier for each change. | 31 st March 2010 | Deviya Mistry |

2 Action Plan

The priority of the findings and recommendations are as follows:

Significant: An absence of an appropriate level of evidence to support the Authority's allocated attainment level. This recommendation relates the evidence that must be collated to support the Authority's related scoring.

| Para | Recommendation | Categorisation | Accepted Y/N | Management comment | Implementation date | Manager responsible |
|-------|---|------------------|-----------------|---|----------------------------|---------------------|
| 4.3.4 | <p>To achieve the current level of the self assessment score, the Authority needs to provide the following evidence:</p> <ul style="list-style-type: none"> ▪ The detail of the testing strategies should be documented and auditable with each release / RFC. This should detail the test performed, the results of the test and formal acceptance from the "system owner". | Merits Attention | Y | A risk based approach is taken. Testing is often the responsibility of our suppliers. The extent of testing will be negotiated with system owners and will be based on the operational urgency of the change/release, the scope and complexity of the change, the confidence in the suppliers testing strategy and the viability of a regression strategy. The test strategy will be documented in detail within the support documentation for the system and in outline on the change request. | 30 th June 2010 | Change Requestors |

3 Findings and Recommendations - Controls Arrangements

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all audit testing undertaken.

| | CONTROLS (ACTUAL AND/OR MISSING) | ADEQUATE DESIGN (YES/NO) | TEST RESULT / IMPLICATIONS | RECOMMENDATION | CATEGORISATION |
|-------|--|--|--|--|----------------|
| | RISK DESCRIPTION: | ROBUST CONTROLS DO NOT EXIT OVER SERVICE MANAGEMENT, CHANGE MANAGEMENT AND RELEASE MANAGEMENT PROCESSES RESULTING IN UNCONTROLLED CHANGES BEING PROMOTED TO THE PRODUCTION ENVIRONMENT AND DISRUPTION, UNAUTHORIZED ALTERATIONS AND ERRORS. | | | |
| 3.1.1 | Evidence to support the ITIL self assessment attainment ratings are available, and stored in a central repository. | No | Evidence to support the attainment level awarded to a number of ITIL requirements have not been made available, and stored in a central file. As a result there is a risk that the Authority may not be able to demonstrate the compliance to the documented attainment levels in the HMIC assessment in June 2010. | Management should ensure that adequate, detailed documentary evidence is in the central repository to support the attainment ratings assigned for each of the ITIL self assessment maturity questions. | Significant |
| 3.1.2 | The Authority has submitted its ITIL self assessment, and stated where it is in compliance to the individual requirements. Where the Authority has indicated that policies, procedures and measures are in place to meet those initiatives, supporting evidence is compiled. | No | The areas with insufficient supporting evidence are detailed at Appendix A. | Management should ensure that the 'Action Points' in Appendix A, are implemented in order to maintain the current ITIL attainment levels. | Significant |

4 Appendix A: Detailed ITIL Compliance Findings

- N/A - Conclusion not provided for self assessment scores that are not fully compliant.
- ✘ - Evidence available does not support the self assessment score.
- ✓ - Evidence available supports the self assessment score.

4.1 Service Management

| | Se q. No. | Assessment against Service Management requirement | Self Assessme nt Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|---|------------------------------|--|------------|---|
| 4.1.2 | 1.2 | Is there a Plan for taking Service Management forward? [Mandatory]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> The ITIL Business Case outlines the high-level aims and benefits of running with the project. <p><u>Note</u></p> <p>The Head of IT has acknowledged that the plan for taking Service Management forward involves reviewing the outcomes from the current self assessment audit, and the Ryton User Group's findings in preparation for the HMIC inspection in June 2010.</p> | ✘ | To achieve the current level of the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> A Service Improvement / Management Plan which details the short term activities (e.g. 6 months), and high level medium term activities (12- 24 months). |
| 4.1.3 | 1.3 | Is there evidence of Senior Management showing leadership on service management capability? [Mandatory]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> IT Intranet site contains information regarding ITIL strategy, and service level agreements, which have been agreed with business leads. Note: This information was only obtained verbally, and not available on the file. Head of IT has over 20 year's experience | ✓ | Evidence available supports the self assessment score. However, management should provide the following evidence in the central repository: <ul style="list-style-type: none"> The service level agreements, which have been agreed with the business leads. |

| | Seq. No. | Assessment against Service Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|----------|---|-----------------------|--|------------|---|
| | | | | <p>of service development, implementation, support and maintenance. Note: This information was only obtained verbally, and not available on the file.</p> <ul style="list-style-type: none"> A catalogue of services is documented which defines each service and its allocated Business system owner and Account Manager / Technical lead. Note: This information was only obtained verbally, and not available on the file. | | <ul style="list-style-type: none"> Qualifications and experience of IT Director / Senior Management relating to Service Management. The Service catalogue which lists the services provided by the IT Department and the service owners which have been allocated from the business. |
| 4.1.4 | 1.4 | <p>Are staff service management skills reviewed (current and required) and ITIL training needs identified to enable staff to perform their role effectively? [Mandatory].</p> | Compliant | <p>The following was identified to substantiate the Authority's allocated score:</p> <ul style="list-style-type: none"> The email communication is evidenced, which supports that all staff in the Department undertake a minimum overview training, and an ITIL simulation training event is being arranged for Dec 2009. All Service Desk staff undergo ITIL foundation level qualification Note: This information was only obtained verbally, and not available on the file. The email communication is documented that states the Senior Management Team proposal for key members of IT staff to adopt areas of responsibility in relation to their job role. | ✓ | <p>Evidence available supports the self assessment score. However, management should provide the following evidence in the central repository:</p> <ul style="list-style-type: none"> Training records / training certificates or completed attendance lists to substantiate that the training was undertaken. |

4.2 Change Management

| | Se q. No. | Assessment against Change Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|--|-----------------------------|---|------------|---|
| 4.2.1 | 4.1 | Have roles and responsibilities for all Change Management activities (as identified ITIL Governance V1.1 Section 4.3) been defined and agreed? [Mandatory]. | Compliant | <p>The following was identified to substantiate the Authority's allocated score:</p> <ul style="list-style-type: none"> The Change Management Process document specifies the requirement of all changes to be approved by the Change Advisory Board (CAB). <p><u>Note</u> The Account Managers are responsible for coordinating and managing the change management activities.</p> | ✓ | <p>Evidence available supports the self assessment score.</p> <p>However, management should provide the following evidence in the central repository:</p> <ul style="list-style-type: none"> The Change Advisory Board meeting schedule, group terms of reference and sample meeting minutes; Change Management activities are defined within the roles and responsibilities of an IT staff member's Job Description; |
| 4.2.2 | 4.2 | <p>Are there Change Management procedures either documented or supported by software which:</p> <ul style="list-style-type: none"> Ensure all Requests for Change are recorded and uniquely identified; Identify whether an Impact Assessment is required in accordance with a risk assessment Conduct Impact Analyses against the Request for Change (as appropriate) Ensure Requests for Change are reviewed (if appropriate) by | Compliant | <p>The following was identified to substantiate the Authority's allocated score:</p> <ul style="list-style-type: none"> Example template of a blank request for change form and an example completed form is provided. <p><u>Note</u> The request for change forms considers the impact of the change and the impact analyses. Changes are recorded on the Request For Change (RFC) forms and are currently identified by the name of the change; however a unique identifier is not assigned. We acknowledge that a revised change request form has been drafted, which should address this requirement once it is implemented.</p> | ✗ | <p>To achieve the current level of the self assessment score, the Authority needs to provide the following evidence:</p> <ul style="list-style-type: none"> Uniquely identifiable RFC, and the request forms updated to allow a unique reference number. The RFC register should be implemented and embedded within the change management process. <p>Additionally, management should provide the following evidence in the central repository:</p> |

| | Se q. No. | Assessment against Change Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-----------|-----------------|---|-----------------------------|---|------------|---|
| | | a Change Advisory Board <ul style="list-style-type: none"> Ensure Requests for Change are authorised at the appropriate management level [Mandatory]. | | A RFC register has recently been devised and at the time of the review this did not contain sufficient records to confirm that the register is fully embedded. | | <ul style="list-style-type: none"> Change Advisory Board meeting schedule, group terms of reference and sample meeting minutes. |
| 4.2. 3 | 4.3 | Are all changes assessed appropriately for their impact and prioritised accordingly? (standard changes are not required to be assessed and prioritised) [Mandatory]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> The RFC forms contain a section for the requestor to consider the impact of the change (section 2.6). Example RFC demonstrating that all changes are assessed appropriately. Senior Management Team Meeting minutes demonstrating and example of the changes discussed and prioritised. | ✓ | Evidence available supports the self assessment score. |
| 4.2. 4 | 4.4 | Is a back out (remediation) plan prepared and agreed prior to implementation of major RFCs? [Desirable]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> The RFC form examples show regression strategies (section 3.5 on request forms). <p><u>Note</u></p> <p>Changes will only be considered if an adequate back out mechanism has been defined, which the requester is confident in. If this is not possible, it must be explained and the risks mitigated with adequate control measures - for approval by the Change Advisory Board.</p> | ✓ | Evidence available supports the self assessment score. However, management should provide the following evidence in the central repository: <ul style="list-style-type: none"> The Back out plan for a sample of RFCs. These should identify the activities to be carried out in the event that implementation of the RFC was unsuccessful. |
| 4.2. 5 | 4.5 | Are regular Change Advisory Boards held to review Requests for | Compliant | The following was identified to substantiate the | ✓ | Evidence available supports the self |

| | Se q. No. | Assessment against Change Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------------|-----------------|--|-----------------------------|---|------------|--|
| | | Change and are the decisions and actions recorded? [Mandatory]. | | Authority's allocated score: <ul style="list-style-type: none"> A sample of meeting minutes demonstrating the frequency of the meetings and that the decisions and actions of the CAB are recorded and documented. | | assessment score. |
| 4.2. | 4.7 | Are different procedures followed to expedite the assessment and approval of urgent / emergency changes as opposed to normal changes? [Desirable]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> The procedures for the Emergency Change Management Process are documented as a process flowchart within the Change Management Process document. | ✓ | Evidence available supports the self assessment score. However, management should provide the following evidence in the central repository: <ul style="list-style-type: none"> A sample of Emergency RFCs to substantiate against the emergency change procedure. |
| 4.2. | 4.8 | Is a schedule of forthcoming changes produced which is clear and easily available to staff? [Desirable]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> Screenshots are provided of the IT change calendar (available to all requestors) on Microsoft Outlook, which is linked to the staff leave calendar to ensure sufficient resources are in place. | ✓ | Evidence available supports the self assessment score. |
| 4.2. | 4.9 | After implementation, are major and unsuccessful changes subject to a Post Implementation Review? (For the purpose of the assessment, a change is successful if it is implemented successfully within the required timescale). [Desirable]. | Compliant | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none"> The change reviews post implementations are held as a standing item in the Change Advisory Board. Note: This information was only obtained verbally, and not available on the file. | ✓ | Evidence available supports the self assessment score. However, management should provide the following evidence in the central repository: <ul style="list-style-type: none"> A sample of the CAB meeting minutes and agenda's, highlighted to demonstrate where the post |

| Se q. No. | Assessment against Change Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-----------|--|-----------------------|------------------------------------|------------|---------------------------------|
| | | | | | change reviews are undertaken. |

4.3 Release Management

| Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-----------|---|-----------------------|---|------------|---|
| 4.3.4 | 6.4 Is testing of releases performed with appropriate input? [Mandatory]. | Compliant | <p>The following was identified to substantiate the Authority's allocated score:</p> <ul style="list-style-type: none"> A brief summary of the test strategy is documented on the RFC form. Testing varies from being conducted in the Authority to being conducted by the supplier using sanitised data. <p><u>Note</u> Testing does not take place for all releases due to nature of system/service however, this must be made clear and approval sought through the change/release processes.</p> | X | <p>Evidence available supports the partial compliance self assessment score.</p> <p>To achieve the current level of the self assessment score, the Authority needs to provide the following evidence:</p> <ul style="list-style-type: none"> The detail of the testing strategies should be documented and auditable with each release / RFC. This should detail the test performed, the results of the test and formal acceptance from the "system owner". <p>Additionally, management should provide the following evidence in the central repository:</p> <ul style="list-style-type: none"> A sample of the RFC forms with additional testing documentation and formal user acceptance. |
| 4.1.1 | 1.1 Is there an overarching Service Management Policy which | Partial Compliance | No evidence was available in the central repository to substantiate the Authority's | N/A | To achieve level 3, the minimum level of compliance for the self |

| | Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-----------|-----------------|---|-----------------------------|--|------------|--|
| | | includes the strategy and framework for implementing all ITIL disciplines? [Mandatory]. | | allocated score. <u>Note</u> A process document is currently being drafted which aims to outline the Authority's approach to Service Management. | | assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none">▪ A vision for Service Management and a Service Improvement Plan. |
| 4.1. 5 | 1.5 | Do management manage risks to the service management organisation and services? [Desirable]. | Partial Compliance | The following was identified to substantiate the Authority's allocated score: <ul style="list-style-type: none">• A risk management system, Orchid, lists significant risks to the organisation/services provided by IT. Risks are also addressed in IT Business plan. <u>Note</u> Our review of the Orchid risk management system has confirmed that no risks to service management had currently been identified. Further discussions with the Head of IT have identified supplementary information that was not evidenced on the self assessment return or the central store of supporting evidence: low risks to operations are discussed weekly at the weekly technical senior management team meetings; risks to service continuation and mitigation / remediation strategies are considered as part of the business continuity planning process; and the Service Catalogue defines the criticality of each of the services provided by the IT Department and the assessment of the capability of recovering these services. | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none">▪ Risks are discussed within the weekly technical senior management team meetings: a sample of meeting minutes and the group's terms of reference which outlines this responsibility.▪ Risks to the continuation of services are adequately managed through the Business Continuity planning process;▪ The Service Catalogue which includes the assessment of the criticality of the services provided to the organisation and the assessment of the Authority's capability of recovering those services. |

| | Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|--|-----------------------------|--|------------|--|
| 4.2.6 | 4.6 | <p>Is the following information recorded in a Request For Change:</p> <ul style="list-style-type: none"> a. RFC number (plus cross reference to Problem report number, where necessary) b. Description and identity of item(s) to be changed (including CI identification(s) if Configuration management system is in use) c. Reason for Change / Business Case d. Name of person proposing the Change e. Date that the Change was proposed f. Change priority g. Timescale h. Impact and resource assessment (which may be on separate forms where convenient). Note an Impact Assessment may not be completed if the associated Risk Assessment is low i. CAB recommendations where appropriate (which may be held separately, with impact and resource assessments, where convenient) j. Authorisation signature (could be electronic) k. Authorisation date and time l. Scheduled implementation | Partial Compliance | <p>The following was identified to substantiate the Authority's allocated score:</p> <ul style="list-style-type: none"> • A draft revised RFC form includes all of the items identified in "assessment against change management requirement". The current RFC form lacks a unique reference number, details of the configuration items to be changed as a result of the change and the change priority. <p><u>Note</u> The Authority is due to go live with the revised RFC form in November subject to change approval.</p> | N/A | <p>To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence:</p> <ul style="list-style-type: none"> ▪ Working examples of the revised RFC form including the requirements, with the appropriate sections highlighted to demonstrate compliance. |

| | Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|---|-----------------------------|---|------------|---|
| | | (Release identification and/or date and time) m. Status of RFC – e.g. 'logged', 'assessed', 'rejected', 'accepted', 'sleeping'. [Mandatory]. | | | | |
| 4.3.1 | 6.1 | Have roles and responsibilities for all Release Management activities (as identified ITIL Governance V1.1 Section 4.5) been defined and agreed? [Mandatory]. | Not compliant | No evidence was available in the central repository to substantiate the Authority's allocated score. <u>Note</u> We acknowledge that the Authority is drafting the Release Management procedures which outline the roles and responsibilities of members within the release management process. | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> The Release Management procedures should be completed and communicated to all relevant staff; Release Management activities are defined within the roles and responsibilities of an IT staff member's Job Description; |
| 4.3.2 | 6.2 | Is there a documented Release Management Policy which includes Release numbering, frequency and the level in the IT infrastructure that will be controlled by definable Releases? [Mandatory]. | Not compliant | No evidence was available in the central repository to substantiate the Authority's allocated score. <u>Note</u> We acknowledge that the Authority is drafting the Release Management procedures and related guidance. | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> As above, the Release Management procedures should be completed and communicated to all relevant staff in a timely manner. |
| 4.3.3 | 6.3 | Are Release Management procedures either documented or | Partial | The following was identified to substantiate the | N/A | To achieve level 3, the minimum level of compliance for the self |

| | Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|---|-----------------------------|---|------------|--|
| | | <p>supported by software. Documentation for Major Releases / RFCs should: <i>(The Authority must determine the threshold for what will constitute a major release/change)</i></p> <ul style="list-style-type: none"> • Define an exact, detailed timetable of events, as well as who will do what (i.e. a resource plan) • Lists the CIs to install and decommission; • Identify test plans and acceptance criteria • Document an implementation and rollout plans; • Includes production of Release notes and communications to end users and the service desk. <p>[Mandatory].</p> | Compliance | <p>Authority's allocated score:</p> <ul style="list-style-type: none"> ▪ The RFC form provides a documented and auditable trail of changes and releases and the requirements are met within the RFC forms. ▪ The timetable of releases is scheduled on the Change calendar. This information was only obtained verbally, and not available on the file. <p><u>Note</u> The current helpdesk software does not support the release management procedures.</p> | | <p>assessment score, the Authority needs to provide the following evidence:</p> <ul style="list-style-type: none"> ▪ Screenshots should be provided of the IT change calendar to demonstrate the timetable of releases and the consideration of staff resources. |
| 4.3.5 | 6.5 | <p>Are releases accompanied by the documentation and/or release notes which contain sufficient information to describe the content and impact (e.g. business, functional, technical, human, etc) of the release? [Mandatory].</p> | Not compliant | <p>No evidence was available in the central repository to substantiate the Authority's allocated score.</p> <p><u>Note</u> The release notes are captured with the RFC. The RFC considers the impact by asking the requestor to detail whether the change / release has any impact on planned events, resources of the service desk, downtime and other technical considerations such as security implications, changes to Active Directory, amendments to connectivity and capacity within the</p> | N/A | <p>To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence:</p> <ul style="list-style-type: none"> ▪ Release notes (/ RFC forms) should be provided as evidence with the relevant sections highlighted which describe the content and impact of the release. |

| | Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|--|-----------------------------|---|------------|--|
| | | | | infrastructure. | | |
| 4.3.6 | 6.6 | Are back out (remediation) plans produced and tested for a release? This must include the processes for restoring the system to live running in the event of an operational emergency and for rolling back the system should the upgrade not be successful. [Desirable]. | Partial Compliance | No evidence was available on file to substantiate the Authority's allocated score. <u>Note</u> Brief remediation plans are captured within the RFC form. Recovery plans are documented for all services provided by the IT Department. Note: This information was only obtained verbally, and not available on the file. | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> The Back out plan for a sample of releases as documented on the RFC forms. This must identify the activities to be carried out in the event that implementation of the RFC was unsuccessful; The formal corporate data recovery plan should be provided for a number of services. |
| 4.3.7 | 6.7 | Is the Configuration Management Database updated to include: a. Definitions of planned Releases, including the constituent hardware and software CIs b. Records of the CIs impacted by planned and past | Not compliant | No evidence was available in the central repository to substantiate the Authority's allocated score. <u>Note</u> A draft revised RFC form includes a section within the Change Management Summary which | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> Working examples of the revised RFC form including |

| | Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-------|-----------------|--|-----------------------------|---|------------|--|
| | | Releases, covering both hardware and software c. Information about the target destination for the Released components (e.g. the physical location for hardware and the servers that will receive the software changes). [Desirable]. | | requires the requestor to list the configuration items to be changed as part of the change / release. | | the change to configuration items, with the appropriate section highlighted to demonstrate compliance. |
| 4.3.8 | 6.8 | Are emergency releases managed according to a defined process which interfaces with the emergency change procedures? [Desirable]. | Not compliant | No evidence was available in the central repository to substantiate the Authority's allocated score. <u>Note</u> The Emergency Release procedures are being drafted as part of the Release Management Procedures and Guidance and it is understood that the process that is to be followed is similar to the emergency change management process. | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> ▪ The Release Management procedures that contain the Emergency Release procedures should be completed and communicated to all relevant staff; ▪ The review / update of Emergency changes should be added as a standing item at the Change Advisory Board. |
| 4.3.9 | 6.9 | After implementation, are releases subject to a Post Implementation Review that considers: a. Whether the Release is built and implemented on schedule, and within budgeted resources (excluding any problems that are outside the | Not compliant | No evidence was available in the central repository to substantiate the Authority's allocated score. <u>Note</u> The post implementation review of releases is discussed as a standing agenda item at the Change Advisory Board. | N/A | To achieve level 3, the minimum level of compliance for the self assessment score, the Authority needs to provide the following evidence: <ul style="list-style-type: none"> ▪ A sample of post implementation reviews and a corresponding sample of |

| Se q. No. | Assessment against Release Management requirement | Self Assessment Score | Evidence in the central repository | Conclusion | Recommended supporting evidence |
|-----------------|---|-----------------------------|------------------------------------|------------|--|
| | <p>control or responsibility of Release Management);</p> <p>b. Whether the planned composition of a Release matches the actual composition ;</p> <p>c. Incidence of build failures;</p> <p>d. Secure and accurate management of the DSL;</p> <p>e. Results of acceptance testing (including piloting if applicable);</p> <p>f. Use of the back out plan due to unacceptable errors;</p> <p>g. Accurate and timely distribution and implementation of a release to all remote sites;</p> <p>h. Evidence of unauthorised reversion to previous versions at any site;</p> <p>i. Evidence of use of unauthorised software at any site;</p> <p>j. Feedback from users;</p> <p>k. Necessary corrective or follow-up action taken, together with any process improvements.</p> <p>[Desirable].</p> | | | | <p>Change Advisory Board minutes where the release is appraised post implementation.</p> |

5 Background

5.1 Objectives and Risks

The audit considered the organisation's objectives for the area under review and the risks to the achievement of those objectives.

| | |
|--|---|
| Objective of the area under review: | To provide assurance that appropriate ITIL processes are in place to increase system integrity. |
| Risk description: | Robust controls do not exist over service management, change management and release management processes resulting in uncontrolled changes being promoted to the production environments and disruption, unauthorised alterations and errors. |
| Controls/risk mitigation strategies within the scope of this audit: | The primary focus of IT Service Management (ITSM) is the application of the ITIL best practices framework to enable IT to be a more effective service provider across the enterprise. ITIL self-assessment will be performed in Autumn 2009. |

5.2 Determination of Audit Approach

In determining the audit approach, we took into account:

| | |
|---|---|
| Factors relevant to the selection of the audit approach: | Review of evidence to support scored attainment levels. |
| Audit tool selected: | Key Controls Testing. |
| Audit approach used: | Audit testing clearly focussed on a small number of material or key controls. |

The conduct of this audit complied with the standards set in the National Police Improvement Agency ITIL Self Assessment.

5.3 Acknowledgements

The following staff gave their time and co-operation during the review and we would like to record our thanks:

| Name | Position |
|----------------|------------------------------------|
| Deviya Mystery | IT User Support Manager |
| Tim Glover | Head of IT |
| Jaswant Minhas | Senior Information Systems Analyst |