



APPLICATION MANAGEMENT

STANDARD OPERATING PROCEDURE (SOP)

STANDARD OPERATING PROCEDURE			
REFERENCE	Policy/135/08		
PROTECTIVE MARKING	NOT PROTECTIVELY MARKED		
PORTFOLIO	Deputy Chief Constable		
OWNER	Chief Information Officer		
START DATE	14 October 2008		
REVIEW DATE	October 2011		
THIS POLICY REPLACES:			
VERSION	DATE	REASON FOR AMENDMENT	AMENDED BY
1.0	October 2008	N/A	N/A



CONTENTS

1	INTRODUCTION.....	3
2	KNOWLEDGE.....	3
	2.1 Terms and Definitions	3
	2.2 Responsibilities	5
3	PROCEDURES.....	6
	3.1 Risk Compliance Procedure.....	6
	3.2 Application Strategy	8
	3.3 Budgetary Control	9
	3.4 Change Control	10
	3.5 Requirements Management.....	11
	3.6 Application Security.....	13
	3.7 User Training.....	14
	3.8 Data Quality	15
	3.9 Records Management.....	16
	3.10 Disaster Recovery.....	16
	3.11 Operational Support	18
	3.12 Supplier Management	19
4	MONITORING AND COMPLIANCE.....	20
5	APPENDICES	21



APPLICATION MANAGEMENT STANDARD OPERATING PROCEDURE (SOP)

1 INTRODUCTION

- 1.1 This procedure effects and is subject to the conditions of the Application Management Policy (Ref:135/08).
- 1.2 This procedure applies to England, Wales and Scotland.
- 1.3 This procedure applies to all designated Application Managers (police officers and staff), their deputies, Senior Responsible Owners and members of the Technology department.

2 KNOWLEDGE

2.1 Terms and Definitions

Accreditation Document Set (ADS) – a document providing details on the framework of controls used to manage risk for a given software application.

Application Manager (AM) – an business portfolio employee appointed by the Senior Responsible Owner to administer a bespoke system or standard package solution provided by a third-party supplier, which may be hosted either internally or externally to the organisation.

Application Management Board (AMB) – periodical meetings chaired by the Force Applications Manager and attended by business Application Managers, during which the status of Application Management responsibilities and activities are reviewed, experiences are shared and guidance is provided.

Change Advisory Board (CAB) – an occasional meeting scheduled to discuss and ratify new business requirements, ultimately enabling a decision to be made on how to accommodate and process them.

Chief Officer Group (COG) – the 5 Chief Officers (DCC, ACC Crime, ACC Operations, Director of Finance & Corporate Services, Director of HR).

Configuration Management Data Base (CMDB) – a definitive and up-to-date cross-reference of IT components, indicating their usage and inter-dependency.



Cost Of Ownership (COO) – the total price of developing, implementing and continuing to support a system

Force Applications Manager (FAM) – the Technology incumbent with overall responsibility for the Application Management portfolio.

Information Management Board (IMB) – a bi-monthly meeting chaired by the DCC, in which COG leads, the CIO, Technology team leaders and business portfolio representatives review development progress, support activities and service status.

Information Systems Strategy For Police Services (ISS4PS) – the plan promoting a joined-up national approach to IT, optimising the sharing of information between Forces.

Information Technology Infrastructure Library (ITIL) – the accredited industry governance framework and best practice service management methodology enabling control over continuity, repeatability and auditability of processes.

Key Performance Indicator (KPI) – a statistical reporting measure used to demonstrate the degree of success in meeting an operational objective.

Operating Level Agreement (OLA) – an internal contractual document by which a supplier is bound to the provision of a service identified within a Service Level Agreement.

Red/Amber/Green (RAG) Status – the indicator employed to signify compliance (or lack thereof) with prescribed standards and pre-requisites.

Return On Investment (ROI) – the derived value of an application in terms of the tangible and intangible benefits it brings to the organisation

Senior Information Risk Owner (SIRO) – a board level executive with principal responsibility for risk management with regard to information held within the organisation. At BTP this is the Deputy Chief Constable, who is portfolio lead for Technology.

Senior Responsible Owner (SRO) – the business portfolio lead with accountability for all software applications falling under their area of authority. For the purposes of this policy and procedure a Senior Responsible Owner equates to a COG member.



Service Level Agreement (SLA) – an underpinning counter-signed contract, defining the content and conditions under which a supplier will provide a satisfactory service to a customer.

Single Point Of Contact (SPOC) – a function holder nominated to facilitate and ensure consistency of communication between business partners or stakeholders.

User Acceptance Testing (UAT) – a process prior to the implementation of a new or changed system, whereby business users are able to determine its impact and accuracy without threatening the integrity of the live environment

2.2 Responsibilities

2.2.1 Ownership of the Application Management portfolio rests with the Force Applications Manager, reporting to the Chief Information Officer in the Technology department at BTP. Ultimate responsibility for Application Management lies with the DCC, presiding over the Information Management Board, to which the Technology department reports.

2.2.2 The Force Applications Manager is responsible for ensuring that each business application meets the necessary level of risk compliance, by monitoring, reporting on, supervising and guiding the actions undertaken by business Application Managers.

2.2.3 Senior Responsible Owners are accountable for systems which exist within their business portfolio. They will appoint appropriate members of their department as focal points for each system, to assume the role of Application Manager for the business.

2.2.4 An Application Manager may be responsible for one or more business applications, over which they will have varying degrees of control, as determined by the nature, attributes and origin of the system(s) in question.

2.2.5 In cases where BTP subscribes to an externally provided solution the influence of the Application Manager may be minimal, with Supplier Management possibly being the only area of governance falling under their remit. This would normally only prevail in extreme circumstances however, with an Accreditation Document Set existing in the majority of cases.

2.2.6 A degree of discretion will be applied by the Force Applications Manager in determining the need for certain governance components, subject to the nature of the application.



3 PROCEDURES

3.1 Risk Compliance Procedure

3.1.1 This section describes the process through which business systems will be assessed and measured for compliance with internal standards, how disparities are reported and followed up for remedial action.

3.1.2 There are no central staff resources within the Application Management portfolio of Technology, consequently business Application Managers are required to self-assess their areas of influence, whilst they are in turn indirectly monitored by the Force Applications Manager, who collates, evaluates and reports on governance.

3.1.3 Within each business portfolio the Senior Responsible Owner is ultimately answerable to local compliance, with the Senior Information Risk Manager reviewing status through the Information Management Board.

3.1.4 A collection of specific risk criteria will be employed to govern the effectiveness of Application Management by their serving Application Managers, with each allocated a RAG status. A definition of compliance classifications for all criteria may be found in the Appendix 5.1 (Application Risk Assessment Criteria).

3.1.5 These 11 criteria are listed below and the means by which these will be measured are discussed later in this document:

- Application Strategy
- Budgetary Control
- Change Control
- Requirements Management
- Application Security
- User Training
- Data Quality
- Records Management
- Disaster Recovery
- Operational Support
- Supplier Management



- 3.1.6 For each of the above risk criteria, a set of specific components must be produced and will determine the maturity of the Application Management process. Templates for mandatory documents can be obtained from the Application Management intranet site
- 3.1.6 The degree of risk to the application (and therefore compliance to BTP policy) will be subject to evidence of:
- the existence of mandatory artefacts
 - the quality of these products
- 3.1.7 RAG indicators will be used to flag alignment of each application to the risk criteria which govern it as follows:
- GREEN will confirm that all essential components are in place and are being maintained to an acceptable standard
 - AMBER will indicate that while many or all of the necessary elements are present, the quality is unsatisfactory or the degree of upkeep is insufficient
 - RED will signify that most or all of the essential items do not exist
- 3.1.8 Dip sampling of applications will enable the degree of compliance to be determined and level of risk understood, such that mitigation or management may be applied as required.
- 3.1.9 A governance health summary of BTP applications will be made publicly available via the intranet. Although the content is provided for illustrative purposes only, its format is shown in Appendix 5.2 (Application Compliance Dashboard).
- 3.1.10 A drill-down for each application, indicating performance against the 11 areas of compliance in greater detail, will be accessible from the dashboard. An example of this (again, for illustrative purposes only) may be found in Appendix 5.3 (Application Compliance Scorecard).
- 3.1.11 The Force Applications Manager will propose an action plan with each business Application Manager, to rectify areas which fall beneath the required standard of compliance, with an agreed timetable by which this must be performed.



3.2 Application Strategy

GREEN	AMBER	RED
A formalised roadmap and strategy covers the full application lifecycle; these are constantly maintained and updated.	A strategy and roadmap partially exist, or are historic and have not been maintained.	The application has no roadmap and a strategy is yet to be determined..

3.2.1 Validation of a business system's fitness for purpose ensures that economies of scale are identified, conflicting interests across the organisation are minimised and exploitation of investment is realised. This justification in turn enables an appropriate level of further funding to be identified and secured, thus enabling the application to continue to meet the needs of the area(s) it was designed to support.

3.2.2 A number of the following items is required to demonstrate compliance with this criterion, which will be determined by the nature of each application:

- an application roadmap, indicating when the system was introduced, its anticipated lifespan, showing when it is due to be replaced or retired (if known)
- a regular review programme to ensure a clear and consistent policy/procedure defines and brings control to application usage, ensuring that it conforms with any necessary legislation
- the original project documentation, illustrating the business case through which this system originated and the context in which it fulfils the needs of the business area it supports
- regular minuted Application Management progress meetings, user groups and clinics
- resource plans explaining application roles, responsibilities and team co-ordination
- a forum by which application publicity, consultation and audit is managed
- a documented succession plan, incorporating provision for continuity of skills and knowledge sharing



- an Accreditation Document Set (ADS) describing the application, its place and purpose in the organisation's business landscape and the controls which govern it

3.3 Budgetary Control

GREEN	AMBER	RED
Maintenance and development budgets are entirely held by Technology.	The annual maintenance budget is clearly held by the Technology group, but development funding is held within specific departmental budgets.	It is unclear who holds the budget for the application, or who authorises invoices related to maintenance and development.

3.3.1 A robust control over expenditure, which is both quantifiable and auditable must exist for each application, in order to direct and apportion costs effectively, minimising wastage at every opportunity.

3.3.2 The following elements are mandatory to satisfy compliance in this area:

- a budget plan detailing revenue and capital expenditure requirements over 3 years for the software application, with a regular review cycle
- an indication of anticipated and actual costs, business benefits, plus any tangible and intangible paybacks resulting from the application
- a process by which negotiation of budget with funding sources and BTP's Finance department is achieved
- identification of budget ownership and authorisation to spend against revenue or capital investment
- a documented total lifecycle cost for the system indicating purchase price and cost of ownership with regard to maintenance, upgrade and on-going support
- for new major developments, tendering processes should involve 3 alternative suppliers and provide evidence of formal quotations prior to selection and arrangement of externally resourced work
- tracking and reporting on expenditure against agreed budgets



- detailed purchase orders/procurement requests and invoices for work undertaken by suppliers
- a cost profile and budgeting plan for maintenance and development of software, in accordance with Force strategy

3.4 Change Control

GREEN	AMBER	RED
An application strategy exists that clearly sets out future upgrades and version releases.	Application version releases are known and ad hoc upgrade plans are prepared and executed, however no formal strategy exists.	No strategy exists for upgrades and version releases are not documented.

3.4.1 The stability of BTP's business systems is paramount if they are to continue to serve the organisation's needs in a prompt and efficient manner. Exposure to risk must be checked at every stage of the change cycle and suitable measures employed to reduce negative impact if it cannot be eradicated.

3.4.2 Governance of this discipline will be subject to the following criteria:

- project meetings with suppliers and implementers to define scope of change, determination of impact, a proposed schedule and a resource plan
- representation through national or local user groups to promote global understanding, negotiation and agreement upon common needs
- forward scheduling of change via requests logged with the system or service provider
- liaison with Technology through an Application Management Board
- Change Advisory Board (CAB) meetings are held on a regular basis to present new requests
- observance of the full change management lifecycle in accordance with ITIL and tracking of all activities for auditability



- the existence of system specifications, providing details of business and physical process designs for the application
- evidence of planned system testing, demonstrated via test scripts showing anticipated outcomes and actual results
- documented User Acceptance Testing (UAT), indicating functional tests and conclusions, with official sign off obtained for implementation
- a documented test procedure with defined requirements and actions is circulated and agreed
- version control is applied to upgrades via comprehensive release management of documentation and components
- release scheduling accounts for priority, risk level and impact of changes and receives a suitable degree of approval/authorisation from all affected parties
- a Single Point Of Contact (SPOC) has been established with regard to co-ordination of change
- an implementation plan is constructed, which features an agreed backout plan
- the Configuration Management Data Base (CMDB) is maintained to reflect any changes to the application or the environment in which it resides by Technology, via information received from business Application Managers

3.5 Requirements Management

GREEN	AMBER	RED
A user group directs the application owner to enhance system functionality, for which there are documented plans.	Application development is handled by one individual or a small group having no inputs from the broader based user community.	There are no further plans to develop the application.

3.5.1 For a business solution to deliver true benefit to its users, rigid control must be applied during the definition of needs stage. All appropriate parties must



be identified and included in this process to prevent key design considerations from being overlooked or disregarded.

3.5.2 The following attributes will regulate this criterion for all new requirements, to avoid request creep and under-delivery of system functionality:

- a formalised consultation procedure exists with a Single Point Of Contact
- a standard process for planning development is followed
- scheduled meetings between business users take place with minuted actions to determine and define needs
- documentation of functional needs is produced, which is subject to stringent version control
- a documented Business Case is produced which defines the requirement, anticipated Return On Investment and Cost Of Ownership
- a feasibility study is undertaken to explore the Business Case and determine the viability of the requirement, with regard to logistics, organisation and expenditure
- functional analysis is performed to break down and define the process flows which represent the existing and potential business system
- a physical design document determines and recommends an appropriate solution for the business requirement
- an impact assessment evaluates the nature of the proposed deliverables and their effect upon the organisation (in terms of processes, personnel once implemented)
- performance issues are recorded in order that they might be addressed via future enhancement



3.6 Application Security

GREEN	AMBER	RED
An up-to-date Accreditation Document Set exists for the application.	The application was known to comply with the corporate security policy from a previous assessment, however this is now out of date.	No security documentation exists, therefore it is unknown whether the application complies with corporate security policy requirements.

3.6.1 Rigorous control over access and authority to BTP business systems prevents misuse of the information upon which the organisation depends, in order to fulfil its purpose.

3.6.2 This will be governance checked by the existence and quality of the following:

- documentation in the form of a security operating procedure within the Accreditation Document Set (ADS)
- periodic security inspections to determine exposure and relevance of authority and access rights
- an authorisation process to provide, revoke or restore access to an application and associated documentation
- evidence of official signoff for control of access rights by Application Manager
- an authority register containing a matrix of users and their granted levels of authority
- full auditability and a documented means of demonstrating control over authority
- a scheduled backup strategy with ad hoc restore capability
- evidence of penetration testing to ensure that the application is secure from unauthorised admission
- a vetting and authorisation procedure to grant appropriate clearance for third party access



3.7 User Training

GREEN	AMBER	RED
A current training plan and course materials are both available; courses are either scheduled or arranged according to need.	Courses have been held, however no plan exists to assess changing needs and no current course materials exist.	There are no training plans for this application and no structured in house training available.

3.7.1 To take full advantage of the potential benefits offered by software applications, a high degree of knowledge must be developed and maintained within the user area of focus. Content, presentation and transfer of learning material should be sensitive to the needs of the target audience and differentiate their required level of experience, whether expert or novice.

3.7.2 Evidence of these factors will influence application compliance:

- demonstrated functional and technical knowledge of the system in the form of business process maps, where people, actions and technology are defined
- an understanding of the demands and responsibilities placed on Application Managers at BTP, which includes an appreciation of ITIL concepts
- a maintained gazetteer of trained users, with succession planning accounted for via the inclusion of deputies
- a training course catalogue describing educational support available for the application
- quality assured training courses and materials, adjusted to reflect change and therefore fit for purpose
- a formally maintained training plan and schedule for staff to ensure system features are understood and exploited
- the availability of refresher courses to cater for occasional or lapsed users



3.8 Data Quality

GREEN	AMBER	RED
Data quality is governed by a procedure, with guidance provided via a good practice guide; training in data quality is audited and extended to all staff.	Monitoring is ad hoc, there are no standards or evidence of an audited improvement plan having taken place.	No mechanism or process exists to identify minimum data standards or to assess actual data quality.

3.8.1 Accuracy, validity and timeliness of information is critical to the decision-making processes which operate within the Force, therefore scrupulous control over update methods and activities is essential.

3.8.2 The following components will determine compliance:

- a best practice guide for data management
- a standards template illustrating tolerances and margins of data accuracy
- integrity of data content, tested periodically by sampling methods
- a process to implement an auditable improvement plan for resolving data quality issues and trends
- on-going accuracy monitoring to assure data quality maintained
- defined accountability and ownership of data
- alignment with Force Information Management strategy
- existence of an audit trail facility to satisfy inspection demands
- a provision by which a data cleansing exercise may be requested and scheduled



3.9 Records Management

GREEN	AMBER	RED
An audited review/retention/disposal schedule exists and is applied.	Review/retention/disposal schedules exist but compliance is either unaudited or incomplete.	There are no records management standards or documented review/retention/disposal processes for the application.

3.9.1 Safekeeping, archiving and purging of protectively marked information must be performed in a regulated, predictable manner, to ensure that the organisation adheres to legal obligations, yet enables retrieval of data for which there is a foreseeable need.

3.9.2 Management and storage of information will be measured by compliance with the following:

- the existence of a published strategy and standards providing guidance on data storage and usage
- a schedule for review/retention/disposal of information exists and is maintained
- where possible data retention periods are considered and built into applications by design
- the access to, processing of and distribution of personal information conforms with Data Protection Act legislation
- protective marking of information and data is applied in accordance with Force policy

3.10 Disaster Recovery

GREEN	AMBER	RED
A full Disaster Recovery Plan exists for this application.	Disaster Recovery details exist but not in an approved or easily accessible format.	No Disaster Recovery Plan or documentation exists.



3.10.1 The ability of the organisation to withstand major unforeseen problems and continue to function is a fundamental requirement. Whilst there is an inherent dependency on the underlying architecture, business applications must be recoverable to a known point, enabling the service to be resumed as seamlessly as possible.

3.10.2 Resilience of an application and its recoverability following an unplanned event will be determined in accordance with the following criteria:

- a provision exists under the main support contract, with regard to providing technical assistance for business critical systems out of the Birmingham disaster recovery site
- risk detection processes and alerting mechanisms are in place to provide notification of critical issues to support staff
- appointed technical support staff and key users are nominated and in a position to respond as/when required
- full system backup and restoration facilities are in place and a catalogues is maintained to identify storage volumes
- storage media is secured in a separate but accessible location from the system hardware, to enable rapid recovery
- a BTP business continuity plan exists to enable departments to operate from designated venues in the event of a major incident - this will be subject to system criticality to the Force
- a full disaster recovery plan is in place to enable applications to be made are available in descending sequence of business criticality
- the presence of appointed gold, silver, and bronze controls and an escalation procedure exists to support this structure
- a documented testing process and schedule is in place for each application and is periodically invoked to ensure that it satisfies the needs of the organisation
- a knowledge base is maintained to log vital information and experience for future reference



3.11 Operational Support

GREEN	AMBER	RED
Both systems and applications are actively managed and monitored on a regular basis by multiple staff.	Users and Service Desk have a contact who normally fixes incidents when they occur, but there is no on-going system or application management.	Either no regular system or application management takes place, or only one person is capable of performing each activity.

3.11.1 Software applications are dependent on a host of underpinning facilities, which must be continuously monitored and maintained in order to provide a reliable and resilient service to the users.

3.11.2 The nature of the system and where it is hosted, will dictate the level of service required, which will be delivered in accordance with active formalised agreements, featuring some or all of the following components:

- a counter-signed Service Level Agreement is in place for each supplier of application software and services to formalise their obligations to BTP
- Operating Level Agreements are present to consolidate internal cross-team management of support responsibilities and these are regularly reviewed
- a formal contract exists with Technology to provide Service Desk support, enabling application incidents to be managed in response to user calls in accordance with pre-determined priorities
- an escalation process exists, which is observed by the Service Desk and suppliers and respects the severity of each call and the responsiveness required to resolve it
- capacity planning of the underlying hardware infrastructure is scheduled periodically to ensure it is robust, resilient and responsive enough to support the applications which are dependent on it
- a schedule for regular data and underlying software backups exists and is supported by a logging process
- a service catalogue entry exists for each application, detailing the key attributes of the system, its purpose, contacts, restrictions and dependencies



- each system in use at BTP has an appointed and acknowledged Application Manager, who performs this role as the focal point for the organisation - conversely a clear definition of Technology roles exists to determine the appropriate point of contact in the event of a requirement from the business
- an official out of hours support rota exists for business critical systems, to ensure that stability and availability of the application is provided in accordance with the needs of the organisation
- corrective and preventive maintenance activities are scheduled and users are notified to minimise impact and periods of unavailability
- support and user documentation is comprehensive and accurate and is maintained in line with changes to the system
- incident trends are monitored and thematic or repeated issues are resolved through problem management
- a Key Performance Indicator (KPI) dashboard is in place for all applications to indicate performance of the system across critical measurement factors

3.12 Supplier Management

GREEN	AMBER	RED
Regular supplier meetings are held.	Supplier meetings have been held, but are not regularly scheduled.	There is no regular management or co-ordination of suppliers.

3.12.1 As a minimum level of governance, Application Management must cater for co-ordination and regular communication with suppliers.

3.12.2 To accommodate this the following criteria must be observed:

- a contract file is maintained for each supplier, containing representative and escalation details, action plans and documents



- all costs related to provision of application support and development services are visible and auditable
- an engagement plan exists whereby a defined agenda for regular supplier meetings is scheduled with minutes/actions taken
- an agreed preventive maintenance schedule exists to alleviate unwarranted system downtime
- supplier delivery schedules are monitored and managed to ensure that commitments to BTP are undertaken as agreed
- contractual Service Level Agreements are maintained and regularly reviewed to reflect on-going customer needs
- Key Performance Indicators for applications are regularly reported and accurately reflect the supplier's ability to respond to the needs of the organisation

4 MONITORING AND COMPLIANCE

- 4.1 The Force Applications Manager will oversee compliance of systems in use at BTP and determine mandatory governance components, however it is the responsibility of the business Application Managers, their line managers and Senior Responsible Owners to ensure that compliance processes are adhered to.
- 4.2 The procedure described under Section 3 will be used to establish the degree of exposure to risk for each business application. This will be determined by the Force Applications Manager in conjunction with each appointed business Application Manager.
- 4.3 A RAG (Red/Amber/Green) status will be allocated to all risk criteria pertinent to each application, in accordance with their accepted level of compliance. Please refer to Appendix 5.1 (Application Risk Assessment Criteria).
- 4.4 Where the required grade is not evident, an action plan will be devised and an agreed target date assigned, by which compliance must be achieved by the business Application Manager.
- 4.5 Once a sufficient level of compliance has been attained the Force Applications Manager will undertake random dip sampling to monitor and



assess adherence to the procedure in accordance with the stipulated risk management criteria.

- 4.6 Lack of compliance with policy will be communicated via the Information Management Board to ensure that any necessary corrective actions are reviewed and prioritised.
- 4.7 A regular Application Management Board will be held periodically with a sub-set of Application Managers, as a forum to ensure that issues are discussed and addressed, improvements and strategic changes are communicated.
- 4.8 An “Application Management” section will be accessible from the “Applications” tab on the BTP Intranet, wherein the governance process and inherent responsibilities are documented.
- 4.9 A risk “dashboard” providing a snapshot of all BTP systems and their overall compliance status will be accessible from this page and will be maintained by the Force Applications Manager, who will refresh it regularly to reflect the latest status. Please refer to Appendix 5.2 (Application Compliance Dashboard) for an illustration of this.
- 4.10 A “scorecard” will exist for each application, which may be accessed by following the appropriate link from the “dashboard”. This will indicate the RAG status and an explanation for each of the Application Management criteria allocated. An illustration of this may be found in Appendix 5.3 (Application Compliance Scorecard).
- 4.11 Governance documentation received from Application Managers will be centrally maintained by the Force Applications Manager and linked to the “scorecard” for visibility as appropriate.
- 4.12 The over-arching Application Management Policy and SOP will be reviewed and (where necessary) revised and communicated periodically, to ensure that it continues to meet requirements.

5 APPENDICES

5.1 [Application Risk Assessment Criteria](#)

5.2 [Application Compliance Dashboard](#)

5.3 [Application Compliance Scorecard](#)