Change Control Process

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security officer

Document History

Version	Author	Comments	Date
V0.1	Tony Yates	Initial Draft	13/06/2016
V0.2		Minor amendments to above	05/07/2016
V0.3	Bradley Cooper	Impact review	11/07/2016
V0.4	Andrew Clarke	Alignment with ISMS Process & Policies	06/04/2017
V0.5	Andrew Clarke	Amendments from PWG	25/05/2017
V1.0	Andrew Clarke	Revised after CISA 2.4.4 service desk notifcations and scope changes - approved	07/07/2017
V1.1	Andrew Clarke	Revised Customer Services responsibilities	27/07/2017
V1.2	Andrew Clarke	UNDONE to be replaced with ROLLBACK to match REMEDY	04/08/2017
V1.3	Andrew Clarke	Peer review required for changes that are Medium and High, including the peer reviewers name.	23/08/2017

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Process establishes the area within Brunel University London covering Change Control Management.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

This process is for IS and University IT Operational change with the CAB aligned to operational matters. For IS strategic change, changes should be submitted to CISA/PMO following the PRINCE2 Project Management IS Project methodology.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Change Manager [CAB]	Is responsible for monitoring and managing all changes. Is responsible for CAB, chairing and scheduling. Is responsible for ensuring all parties involved in changes are available
Head of Infrastructure and Operations or delegate of authority [CAB]	Is responsible for overall Change Management on all systems and infrastructure managed by IS and ensure adherence to policy.
IS Systems Manager (Operational Team Manager) or delegate of authority [CAB]	Is responsible for monitoring and managing changes on the IS operational systems. Is responsible for ensuring IS Systems Management Team Change Requests (CRs) are correctly submitted to Remedy and Change Advisory Board (CAB). Is responsible for testing relevant changes on IS systems.
Network Manager (Operational Team Manager) or delegate of authority [CAB]	Is responsible for monitoring and managing changes on the network and network appliances systems. Is responsible for ensuring IS Networks Management Team Change Requests (CRs) are correctly submitted to Remedy and Change Advisory Board (CAB). Is responsible for testing relevant changes.
Head of Development and Application Services (Operational Team Manager) or delegate of authority [CAB]	Is responsible for monitoring and managing changes on server application software. Is responsible for ensuring IS Development and Application Services Management Team Change Requests (CRs) are correctly submitted to Remedy and Change Advisory Board (CAB).

	Is responsible for testing changes on software and web applications.
Software tester	Is responsible for testing development software items updates and implementations following changes.
Software Owners	Are responsible for tracking all changes for their assets.
Cyber & Information Security Manager CAB]	Is responsible for cyber security risk assessment of changes.
Head of Customer Services [CAB] or delegate	Is responsible for ensuring that Service Desk are informed, have a presence in CAB and all relevant Service Announcements are made and status is updated.
Operational Manager / Team Leader [CAB]	Is responsible for authorisation of Low impact Changes for their respective team
CIO delegate / consultant [CAB]	Is responsible for ensuring the correct ITIL processes are adhered in full, make recommendations and approve changes on behalf of the CIO.
College IT Systems Managers stakeholders [CAB – ex-officio]	Are responsible for monitoring and managing changes on the respective College operational systems and server application software. Are responsible for testing relevant changes on College IT systems.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A12 – Operations Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.12.1.2 Change Management

1.4 Scope

The scope of this document covers all changes made to:

- All the University's information systems;
- Accessibility to and hosting of Information and data;
- Server Hardware including SAN storage devices, server chassis mounted fibre channel and Ethernet switching, on-board remote management devices and applications, HDD, CPU, Memory that requires an interruption to service delivery;
- Desktop PCs, Workstations and Laptops, (campus wide, changes to vendor/model);
- Firewalls, Encryption Devices, Routers and Secure Access Solutions;

- LAN Switching Equipment;
- Wi-Fi Equipment;
- Server Applications;
- Operating Systems;
- Printers;
- Front end interface changes (GUI);
- Backend changes, e.g. database, backup routine;
- Processes that affect the handling of Informational Assets on authoritative systems (e.g. SITS, HR, PAYROLL);

The following changes are considered routine and are therefore not subject to this Process and are out of scope:

- Anti-virus definition and signature updates;
- Single Client / end user computing application updates;
- WSUS Windows updates – notification required, not approval;
- Backup/restore jobs;
- Development and Test environments – no live environment;
- System Admin with no risk to the Production service; providing this is documented under general housekeeping schedules;
- User Administration (creation, deletion, phone extensions, email accounts, etc.);
- Replacement of PC's/Laptops that have already been accepted into live service;
- Enlivenment of Network Ports;
- The replacement of like for like is undertaken, and that no alteration has occurred in the original design, or feature (patch update) or a work around has been put in place) - Ref Appendix C IS Incident Management;

1.5 References

Brunel University Computer Centre - Remedy Based Change Control Procedure v2.1
BUL-POL-12.6 - Patch Management
BUL-POL-12.5 - Release Management
BUL-POL-12.1.2 - Change Control Policy
UCISA – ITIL Guide to Change Management
BUL-POL-16-1 Infosec Incident Management
BUL-PROC-16-02 Infosec Incident Management Procedure

2.0 Change Process

2.1 Process Summary

This document is intended to outline the Information Services Change Control Procedure and the Remedy-based reporting and control application and ensure compliance with the ITIL UCISA Guide to Change Management.
The process is designed to inform, warn, provide an opportunity for feedback, and capture history. Part of this process is to allow a more controlled and a methodical way of making changes to the University infrastructure, to minimise outages, and to ensure that no single resource has total autonomy to request, implement and approve their own change requests.
This policy reflects operational hours Monday-Friday 08:00-18:00, outside these hours any necessary initiated changes would be viewed as a part of the BUL-PROC-16-02B IS Incident Management Procedure and would be expected that any changes made as a result of an incident would be communicated to the relevant parties prior to 08:00 for the following working day as a retrospective change submission. (Ref. Appendix C for demarcation between Incident and Change)
Operational hours do not limit planned changes that may be planned and delayed until outside these hours to lessen service impact.

2.2 Types of change

2.2.1Internally driven change

In the scope of this document are changes based on the operational or development needs of the service. These may be part of a project, a required 'standard' process or to make an improvement to the service. They will/may have an effect on the service (either short term or long term) and it is this effect that needs to be advertised to those that may need to know.

A change is typically where you are making a change to 'something' that will cause the state of the service/device/function/feature, to change, some examples below.

- Installation of patches, as they introduce new features or functionality, or provide a fix
- Installation of a new device or component which was not part of the original design
- The replacement of a part/component.
- Configuration changes
- The removal of the above

Some examples of Changes that should be reported through this procedure are listed below. These examples are not definitive and are for guidance only. If in any doubt, seek change advice for clarification from operational managers who will seek clarity if required from consultants/SME's elected by the CIO, allowing learning and feedback. The procedure ensures distribution of information and recording of history for these events:

- Operating System and application software patching;
- Network/server/application configuration changes;
- Server migrations;
- New service/application commissioning;
- Restarts of Systems/Devices.
- Network Infrastructure, both perimeter and internal;

Any changes that are within the defined scope must adhere to this process.

2.2.2 User-driven change

User-driven change is out of the scope of this document and should continue to be logged in the Remedy User Support application so progress can be tracked by the support teams involved and the person making the request.
This type of change is usually associated with single client application updates or changes of single account amendments that have no effect on University production systems.

2.3 Current Process

Currently, many processes are used to discuss and inform us of internal change, including:

Remedy/Email Change Control Process	This is the official IS Change Notification, Authorisation and Control Process.
Daily management meeting	Meeting of representatives of each team to discuss planned changes, known issues and achievements.
Email	Unstructured messages are frequently sent between teams advertising changes.
Internal meetings	Support group meetings, technical division meetings and team meetings are all regularly held to discuss and warn of changes, issues and successes.
External meetings	The department is well represented at Colleges meetings where we inform the Colleges and Institutes of changes, issues

	and successes; this includes our own Computing Contacts meeting.
Service Status and IntraBrunel (IB)	Web-based information for all users giving information of planned changes and current issues.
Calendars	Some teams use Public folders to capture change, this is used as a reference point should the change cause unforeseen issues.

2.3.1 Planning your Change

Do your planning before you submit a Change Request.

- If preparation work is required for a Change (e.g. a request for a Change to be investigated and planned by a technical team), this should be logged as a Request in the normal way. Once that piece of work has been done and the approach and plan is accepted, the requester or implementer should formally log the Change through this Process;
- If there will be service downtime – include an appropriate statement to the service users
- Plan the appropriate resource and timeline – this may change and you may have to reschedule

2.4 The Remedy/e-mail Change Control Process – in hours

Notifications of change should be captured at the earliest possible time so that the correct CAB governance board or authorisation route can be taken as follows:

1) ECAB is an Emergency CAB facilitated preferably by email, or if email is unavailable, by verbal communications.
   Authorised by the ECAB (two CAB members, independent from the change requester & implementer and not from the requesting team) - see 2.5;
2) High– Authorised by a CAB;
3) Medium – Authorised by a CAB;
4) Low– Authorised by Operational Manager, from the respective team.
   In the event the Manager is implementing the Change, authority must be sought from the head of the tower or an alternative CAB member;

The CAB is made up of the Change Manager, IS Systems Manager, Head of Infrastructure and Operations, Network Manager, Head of Development and Application Services, Cyber & Information Security Manager, Head of Customer Services, CIO delegate / consultant and representatives from relevant stakeholder Operational Business Units and Colleges as required – ex-officio. [ref. Table 1 – responsibilities].

If an individual cannot attend, a delegate of authority must be authorised to act on their behalf.

Change Requests are created within Remedy by the implementer with input derived from technical, project, managerial and user team members as appropriate.

Each Change Request will be assigned an initial STATUS of RFC or PLANNED and then changed as it moves through the process according to the following table:

Status	Description
RFC	Request for Comments: An early stage proposal of a change that has been requested and requires CAB comments.
PLANNED	This gives formal advance warning of the change to enable feedback and management/Change Advisory Board (CAB) approval if required.
REFUSED	Used if a change is to be stopped (to be used by CAB management only).
CANCELLED	To be used if a planned change is no longer going to happen.
PRE	This is sent out just before the change is made as a reminder that the change is imminent.
DONE	This is sent immediately after the change has been made for alerting/notification whether the change was successful or not and the result. Post change monitoring for problems/side effects should be ongoing.
CLOSED	This is sent after the change, sufficient post change monitoring and approval at CAB). It confirms that the change event can be closed.
EMERGENCY	Use this only when PLANNED can't be used, because the change is being done to resolve an urgent issue/emergency.
ROLLBACK (to be changed to backed out)	This can be used in certain circumstances if a change has to be backed-out/removed.

Change Requests should incorporate as much information as necessary for the CAB to make a considered assessment of whether the Change Request should be approved or rejected.

Such information should include at least, and is located within the description field in Remedy to assist completion:

- A reason for the change containing the business justification / expected business benefits as described by the sponsor;

- A full description of the change containing High level / Management Summary of how the change will be made. This should include sequence of events and the impacted referral groups and the Services that will be impacted/affected;
- Stakeholder notification & acceptance;
- The CHANGE WINDOW for the change, date and time for the implementation (release);
- A RISK assessment based upon PROBABILITY and IMPACT; (see 2.4.1 below)
- Known Risks and Risks mitigation. Identify any actions to reduce the risks identified, or link to a separate risk plan. Also detail any stages of the implementation where a review of the go / no-go decision should be made / or any key stages involving handover to other groups;
- Who will be implementing it and the IMPLEMENTATION PLAN they will be following;
- A TEST PLAN detailing how you plan to test the changes you will be making following the implementation to assure the implementation team that the change was a success;
- EXPECTED RESULTS - List the expected results you should see from your testing;
- A ROLL-BACK PLAN explain how the changes can be rolled back from each stage of implementation if the results obtained are not as expected PEER review;
- A full commercial consideration review - Can this change be made utilising the existing resources assigned to the account, or do we need additional people – if so why;
- Detail any RISKS, ASSUMPTIONS, DEPENDENCIES that the change is based on, and also the timescales to which you can deliver;
- SECURITY REQUIREMENTS - Detail any impacts that the change may have on the current security policies that are in place. Explain how these impacts will be managed;
- PEER review required for changes that are Medium and High, including the peer reviewers name.

The requester is the person asking for the Change (probably you). The implementer is the technical/SME (subject matter expert) who is going to execute the change.
See Remedy Change Request for reference (embedded)


sample RFC.docx

For changes submitted through alternative methods or retrospectively, the Change Request form in Appendix B can be submitted to ensure that the correct details are entered to Remedy at a later date. (See example below)


CR Example

Although this is quite in depth, depending on your change, there is a need to demonstrate to your peer reviewer for medium and high changes,their name should be included in the change under peer reviewed what you're undertaken, to avoid any missed commands or instructions that could cause an accidental/unforeseen outage.

Copies of all change requests are retained in Remedy to provide an audit trail;

2.4.1 Risk Assessment

Risk assessment is an important aspect of change management and control and will also be helpful in the determination of the requirement for, and appropriate seniority of, management approval to change requests.

Consider the impact and risks of the proposed change itself on the service/users and also carefully consider risk/impacts of consequential problem scenarios should the proposed change run into trouble. In addition, consider the risk/impact scenarios of not proceeding with the proposed change.

Where appropriate, unless running under an incident (BUL-PROC-16-02 Infosec Incident Management Procedure) the following Impact/Risk matrix can be used for the scenarios identified in order to facilitate consideration of the overall risk profile of the proposed change, and ***suggested*** routes for grading and ECAB has been indicated.

Service Impact

	Extreme Complete loss of service	**High** Severe loss of operating capability, where at least 50% of users would be affected	**Medium** Noticeable but limited operational impact	**Low** Minimal to service operations
Probability **Almost Certain** We are bound to expect these incidents, or they are happening right now	**ECAB**	**HIGH/ECAB**	**MEDIUM/HIGH**	LOW/MEDIUM
Probable We are likely to experience incidents of this nature soon	**HIGH/ECAB**	**HIGH**	**MEDIUM**	LOW

Possible There is some evidence to suggest we may be affected, nothing substantial	**MEDIUM/HIGH**	**MEDIUM/HIGH**	**MEDIUM**	LOW
Unlikely Incidents of this nature are uncommon but there is a chance we may experience them in the future	LOW/MEDIUM	LOW	LOW	VERY LOW

2.4.2 Change Control message structure:

Once the change has been submitted, a workflow is triggered which includes the generation of change control emails.

All Remedy generated emails about changes have a standard source address of "Change Control" and a standard Subject line format "Subject: brief description: <status>"

2.4.3 Change Control Email Circulation:

All Remedy change emails are sent to the **changegroup@brunel.ac.uk** distribution list

This is a core group of IS and other Managers comprising the CAB and a public folder address that has read access to all IS staff.

Ensure that the delegates email addresses (stakeholders) are included within the Change email field

Ensure that the recipients list is the same for all emails on the same subject.

2.4.4 Change Approval/Sign Off and Clearance to Proceed with Change

The CAB provides confirmation that the implementer/ has the approval to proceed with the change from within the process.

Release timescale: HIGH 1 day FROM CAB DATE, MEDIUM- 2 days FROM CAB APPROVAL DATE (this allows the escalation process to have sufficient time)

Therefore you need to consider your timings from submission to release.

It is an inherent requirement on all Staff and Operational Managers to consider whether escalation to a higher level is required for approval to

proceed with any change. **Note: *the requester or implementer cannot and should not authorise their own Change Request.***

The mandatory circulation of all Change Control notices to the **Information Services ChangeGroup** and relevant strakeholders on an ex-officio basis provides a broad review opportunity and the mechanism to have the foresight of the up and coming CR's, and make any representations in CAB. An issue of a REFUSED notice in cases where there would be a conflict with higher priority activity, critical University events etc., or where the CR's has not been completed to satisfy the Change Manager. The Change Manager decision is respected, however in the event, if a CAB member feels the need to escalate, this must be noted in CAB and the change will be placed on hold. A written case must be submitted within 3 hours of CAB to the CIO or if CIO is unavailable, the Head of Security or respective Delegate of Authority - who's outcome is final and will be respected.

Requirement: There is a need for two change managers need to be elected, one as a standby, from the CAB Matrix listing 1.2, and the change manager should be announced.

ll PLANNED Change Requests that fall in the HIGH and MEDIUM range (as indicated in AMBER and RED in the Risk Assessment matrix in section 2.4.1 above) need to be reviewed at the weekly CAB session, currently held every Wednesday as an extension to the morning management meeting. It is, therefore, important that all medium/high-risk changes are created with sufficient notice (3 working days prior to CAB) to allow for this review, and the implementer would be required to attend.

Distribution to all members of the CAB (see 2.4 for CAB members) must be provided with the CR with 3 working days' notice to ensure that sufficient investigation and risk assessment is done on the change by each member.

In addition, Service Desk must maintain full visibility of scheduled changes to ensure stakeholders have continued notification of scheduling.

All resolver team should send the appropriate member to CAB for their team's representation. However in the event, a resolver team member is not present the Change Manager reserves the right to non-attendance as their consent to the submitted CR's as no objection. In addition, a member of the service desk should attend to note any outages/impact and update the service desk team and place the appropriate service announcements.

Execute the change only after approval has been given by CAB;

Please ensure that any deviations to the Change or execution to the implementation of the change have the approval from the Change Manager, to review any potential impact.

2.4.5 Rollback (back out)

Should a change back out be required then this must be approved by the respective operational manager marking ROLLBACK in Remedy update should be processed as quickly as possible clearly indicating the reasons for reversion, contact details for assistance with ongoing service effects, identifying symptoms and any local remediation steps etc., and communication notice to be sent out.

2.4.6 Public Folder Repository

In addition to the Remedy Change database there is a public folder repository for all Change Control messages under:

Information Services, Change Control.

2.4.7 Workflow

The Remedy change management application will enforce appropriate workflow on change processes (see Remedy documentation). The majority of changes will follow:

Planned -> Pre -> Done -> Closed.

2.4.8 Non-compliance

Unauthorised changes are required to be reported to Head of Security and may be subject to formal action.

All Staff/Contractors, who believe the policy has been breached or abused must report this concern to the Head of Security and the CIO, with a reason, backed with factual evidence.

2.5 Emergency Change Process

- Emergency changes must reference a Service Desk IS Incident or Security Incident reference number;
- Remedy must still be completed before a change is carried out and passed to the Change Manager who will liaise with the two ECAB members from the responsibility matrix in 1.2 who cannot be the requester or implementer to assess risk and gain approval,

In the event no agreement can be made, the matter needs to brought to the attention of the Head of Security or the CIO for final approval.

If the emergency change is outside of normal hours, responsible endeavours must be taken to gain approval from the on call call-out list and a retrospective change processed next business day, and the implementer will be required to attend the daily operations meeting to brief the members.

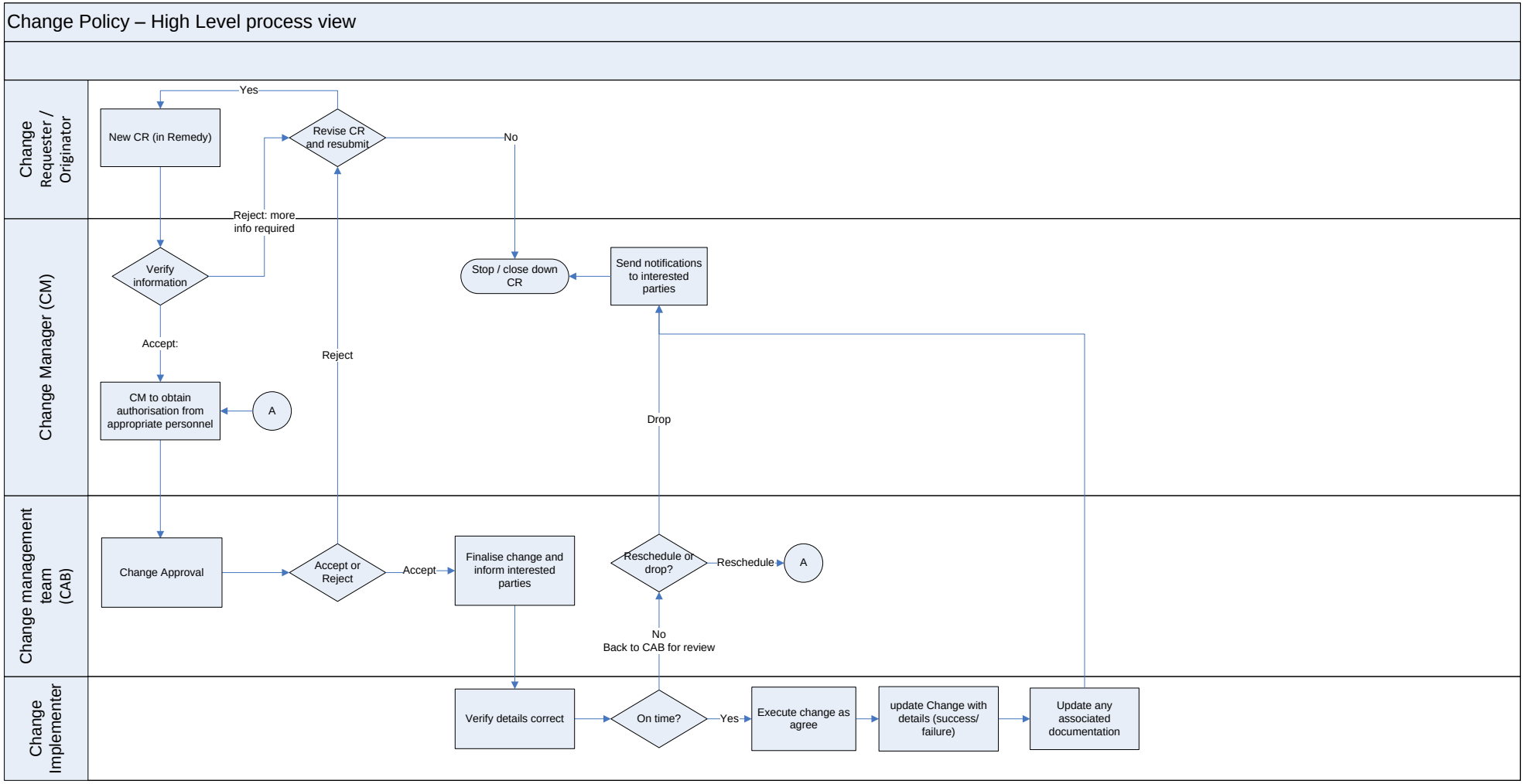
- Always give closure details (results) if it is a retrospective Change;
- An emergency change is not to be abused, and is for the most serious cases, where you can show/demonstrate to the independent members, that this is required because of an imminent service failure, *and not to be confused with "I just need to do it now",* lack of planning could be shown here;
- The risk matrix will also guide you (2.4.1);
- These changes are subject to review;

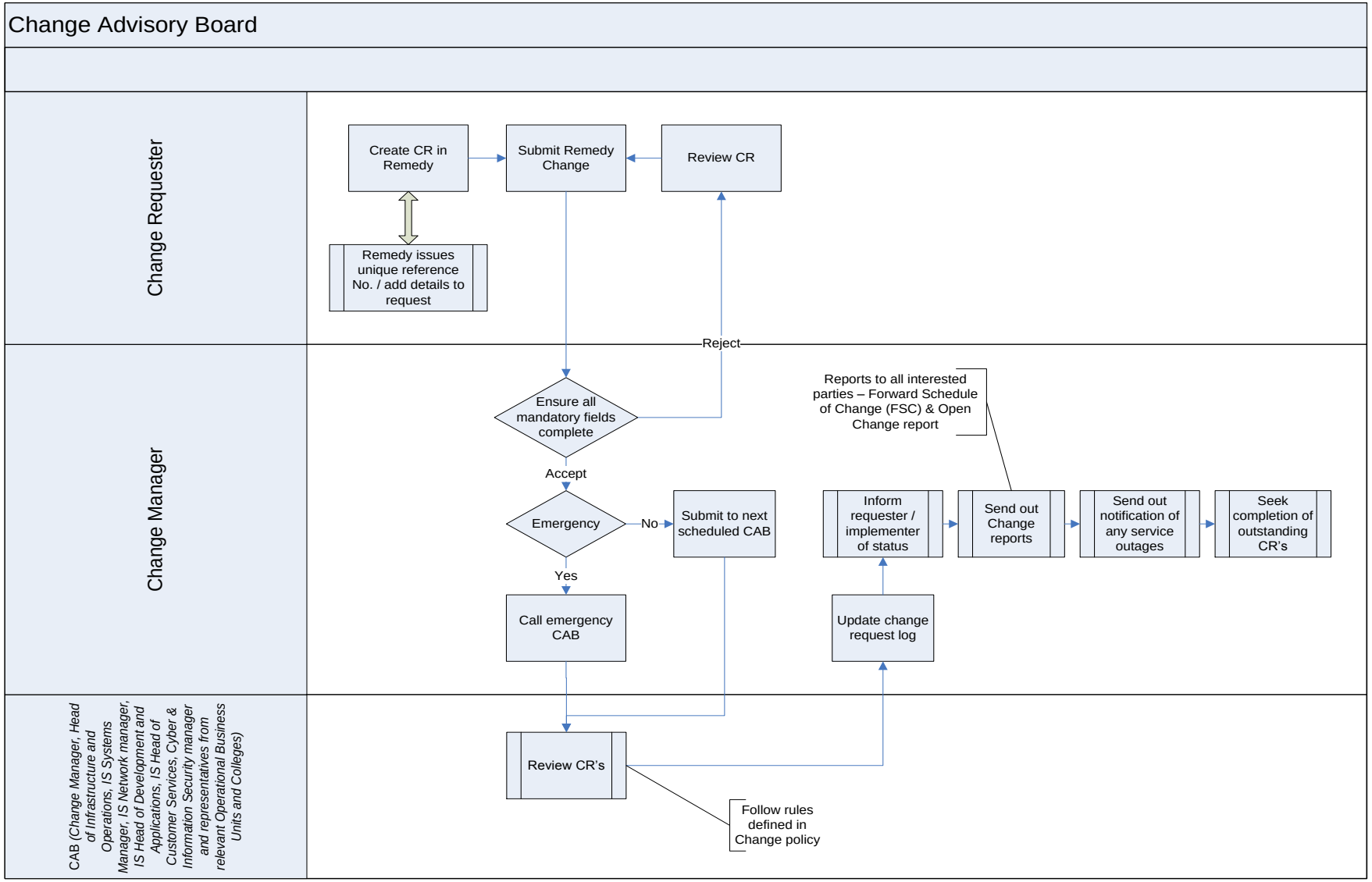
  Example of an Emergency Change:
  The University is receiving a DDOS attack, we need to patch a server or servers/devices, if we don't, we lose services and we are receiving sustained attacks now.
  The members should question, can this be undertaken as a high change rather than an emergency, as Emergency Changes will most likely cause an unforeseen outage owing to the unplanned nature of an emergency change but if the change is required immediately, it is essential that if approved, Stakeholders who will be affected and Service Desk are informed.

- Example of a non-Emergency Change:
  I need to restart my server or device, as my service monitoring tools have been lost.

  Knowing this will cause an outage to customers, it is frustrating that the monitoring has been lost, but no customer service has been impacted, This can be a planned change under High or medium but stakeholder/customer and service desk need to be informed.

APPENDIX A: Change Management Process flows




Change Advisory Board
Change Requester
Change Manager
CAB (Change Manager, Head of Infrastructure and Operations, IS Systems Manager, IS Network manager, IS Head of Development and Applications, IS Head of Customer Services, Cyber & Information Security manager and representatives from relevant Operational Business Units and Colleges)
Create CR in Remedy
Submit Remedy Change
Review CR
Remedy issues unique reference No. / add details to request
Reject
Ensure all mandatory fields complete
Accept
Emergency
No
Submit to next scheduled CAB
Yes
Call emergency CAB
Review CR's
Follow rules defined in Change policy
Update change request log
Inform requester / implementer of status
Reports to all interested parties – Forward Schedule of Change (FSC) & Open Change report
Send out Change reports
Send out notification of any service outages
Seek completion of outstanding CR's

APPENDIX B: CR (Change Request)

Request ID:	**Title:**	
STATUS		
System:		
Impact:	**Probability:**	**Priority:** *Urgency x Impact*
Wider Programme:		
Change Sponsor <Peer Review>:		
Raised By: <<Change owner>> **Ext:**		**Date Raised:**
Implementation Date:		**Implementation Time:**
Who is affected:	<<Customer user groups>>	
Team / Person Responsible:	<<Name of person who is responsible for change>>	
Stakeholder(s):	<<Names, Colleges and departments affected by change>>	
Impact Assessment:	<<Name of person(s) completing this CR>>	

Management Summary
Reasons for Change: <<This section contains the business justification / expected business benefits as described by the sponsor – it will be completed by Sponsor and Change Management>>
Description of Changes: <<High level / Management Summary of how the change will be made. This should include sequence of events and the impacted referral groups>>

Impact Analysis / Investigation
Implementation Plan
<<Detailed description of how your referral group will make the change and what change should be made>>

Commercial Considerations
<<Can this change be made utilising the existing resources assigned to the account, or do we need additional people – if so why?>> <<Please provide effort estimate (days) in all cases, if this change requests additional change>>
Assumptions / Dependencies / Timescales
<<Please detail any risks, assumptions, dependencies that the change is based on, and also the timescales to which you can deliver>>

Implementation Costs

	Effort Estimate	**Valid Until:**
	Cost Estimate:	
Approved / Rejected (Delete as appropriate)	**Signature:**	**Date:**

Risk Management / Test Plan	
Test Plan:	<<Detail how you plan to test the changes you will be making>>
Expected Results:	<<List the expected results you should see from your testing>>
Known Risks:	<<List the identified and known risks with the change, or link to a separate risk plan>>
Risk Mitigation:	<<Identify any actions to reduce the risks identified, or link to a separate risk plan>>
Checkpoints:	<<Detail any stages of the implementation where a review of the go / no-go decision should be made / or any key stages involving handover to other groups>>
Rollback Arrangements:	<<Explain how the changes can be rolled back from each stage of implementation if the results obtained are not as expected>>
Security Requirements	

Security Impact:	<<Detail any impacts that the change may have on the current security policies that are in place >>
Security Plan:	<<Explain how these impacts will be managed>>

Implementation			
Implementation Notes:		Actual Implementation Date / Time:	
Planned Implementation Date / Time:	<<Which Servers>>	To be completed Out of Working Hours	<<Yes / No>>
Server Outage(s) Required	**Signature:**	**Date:**	
Approved / Rejected (Delete as appropriate)			

Documentation	
Technical documentation:	
User documentation:	
Final Acceptance	
Acceptance Notes	
Signature:	**Date:**

APPENDIX C: Incident / Change demarcation

It is established that a change is where you knowingly affect the end user service and this requires the Change process to be completed.

However certain events will fall under incident management, BUL-PROC-16-02B IS Incident Management Procedure, in this case where a system/device fails and effects the end user or not, an incident ticket should be raised.
Depending on the risk of the remediation of the incident (see risk matrix), if the service has failed for the end user, there is little point in seeking a change, as the system/device has failed.

This would be handled under the incident.
Example:

- Storage that has multiple hard disks, a disk failure has occurred- it has been established this is hot swappable, therefore local operations management approval would be sufficient an incident ticket would be raised and work on the remediation, once complete set the incident to resolved.
  As you have not changed anything feature wise of the original setup to the design of the device, this would not constitute a change, unless you knowing are going to use a not like for like replacement, then change management would apply.

- If we take the same example again, but now add the fact that the system is completely down, an incident ticket should be raised, and the remediation should start, however if the resolution is to use another part that Is not of the original setup, apply a patch, or re work the design to remediate the incident, this would constitute a change, as you have made a change to the original setup.
  This would require a change, however the restoration of service has precedence, and once service is restored, a *retrospective change should be submitted,* using the status and setting to *retrospective in remedy,* and clearly indicating this was from an incident, with supporting details, including incident number and the CMDB is updated accordingly.

Other User experienced incidents examples:

Application

- Service not available (this could be due to either the network or the application, but at first the user will not be able to determine which);
- Error message when trying to access the application;
- Application bug or query preventing the user from working;
- Disk space full;
- Technical incident;

Hardware

- System down;
- Printer not printing;
- New hardware, such as scanner, printer or digital camera, not working;
- Technical incident