

## vIssue, Problem and Change Management Approach

### 1. Purpose

This document outlines our approach to Issue, Problem and Change Management. It is intended to be a *client facing summary* document that has been compiled from information held within Computeam's internal QA systems, which forms part of our ISO9001 accreditation.

### 2. Scope

This covers requests for Business as Usual (BAU) service requests, emergency system issues/failures, through to transitional changes to existing systems, infrastructure or platforms that would normally be planned and managed as part of project delivery.

### 3. Comparison of Issue Management, Problem Management, and Change Management

#### Issue Management

Focuses on the immediate resolution of incidents or service interruptions. The goal is to restore normal service operation as quickly as possible. It is reactive and short-term in nature and, whilst care should always be exercised in the execution, it therefore rarely requires any formal change approval.

#### Problem Management

Aims to identify and eliminate the root cause of recurring issues. It is both proactive and reactive, with a medium to long-term focus. The goal is to prevent incidents from happening again but implementing solutions to root causes, whilst more often than not, retaining the existing systems or infrastructure.

#### Change Management

Manages changes to systems or services in a controlled manner and is usually performed on system changes or upgrades that are otherwise functioning as expected (eg: a Cloud migration from an on-premise solution). The goal is to minimise the risk and disruption from changes, but also to capture any potential end user considerations as part of the change.

	<b>Issue Management</b>	<b>Problem Management</b>	<b>Change Management</b>
<b>Purpose</b>	Resolve issues quickly	RCA and suggested fixes	Planned changes, normally when replacing or upgrading existing systems.
<b>Approach</b>	Reactive, rarely needs any formal change approval	Proactive & reactive	Planned
<b>Outcome</b>	Service restored	Re-occurrence of issues prevented	System improvements delivered in a controlled and risk managed way.
<b>Tools</b>	Ticketing System	Knowledge base, previous tickets	Scope of Work documents ' / Project & Service Tickets

#### 4. Change Categories

Changes should be categorised under one of the three ITIL change categorisations:

- **Standard Change:** Low risk, pre-authorised, changes that are well-understood and fully documented and can be implemented without any need for authorisation.
  - Firewall changes
  - Routine patching / upgrading of non-critical systems
- **Emergency Change:** Changes that must be implemented immediately to resolve a major incident or prevent one. Examples include, but are not limited to:
  - Critical “zero day” security patches
  - Replacing failed hardware in a production environment
  - Rollback of a deployment that has caused a service outage
  - Blocking of a malicious IP during a cyber attack

Standard and Emergency changes are likely those that are predominantly used by the Service Delivery team.

- **Normal Change:** Changes that need to be scheduled, assessed and authorised following a pre-determined process.
  - Upgrading of critical business hardware software resulting in downtime (eg; AP or firewall firmware upgrades)
  - Migration of business-critical services between platforms (eg, transition between two online backup solution)

A Normal change would generally be one managed by the Project Management Office (PMO) as part of project delivery, or by the Service Delivery team as part of Problem Management.

## 5. Summary

- All changes must be captured in the Change Management System (ConnectWise PSA).
- All works undertaken, whether undertaken as BAU work (Incident Management), implementing fixes to resolve RCA issues (Problem Management) or changes because of a system transition (Change Management) must be fully documented and recorded within the service/project relevant ticket.
- Risk / impact assessments must be considered for all changes, recognising that for normal BAU works, this may not be appropriate and/or necessary.
- All Normal changes must be reviewed and approved by a senior Computeam consultant. For service transitions, this would be covered as part of the Scope of Work creation - for issues identified after RCA, this should be recorded within the relevant service ticket. This ensures that any required roll back process can be quickly identified and implemented.
- Where appropriate, client approval should be sought when the end user experience would differ as a result of a change.
- Where possible, changes must be tested in a non-production environment before deployment, but we recognise that within the education sector, this is unlikely to be possible. Where appropriate and possible, testing should be undertaken on a sub-set of resources that may be affected.

## 6. Change Freeze Policy

In certain circumstances, Computeam reserves the right to implement a “change freeze” for a period of up to 30 days. This measure may be necessary due to specific factors such as the imminent end of support for systems & services, the scheduling of significant planned works, or other exceptional operational requirements where change management could impact or conflict. The purpose of a change freeze is to safeguard the stability and integrity of business-critical services and infrastructure during periods of heightened risk or major transition.

During a change freeze, no non-essential changes will be permitted, except where required to address critical incidents or major security vulnerabilities. The duration and scope of the freeze will be clearly communicated to all stakeholders at the point of a submitted change request, and any exceptions will require approval from the Change Management Team. This approach ensures that all parties are aware of the restrictions in place and that service continuity is prioritised.

Version	Date	Initials	Changes
1.0	July 2025	CR/PR	First publication
1.1	December 2025	PR	Added Change Freeze Policy