1. **Scope**

All existing and potential new information processing systems are subject to planning to ensure adequate capacity and to clearly defined acceptance criteria.

1. **Responsibilities**

The Director (CISO) is responsible for capacity monitoring and planning, and for monitoring vulnerabilities and vendors’ releases of patches and fixes.

The Director (CISO) is responsible for authorising increases in capacity, for authorising acceptance criteria in respect of each proposed new system and for budget and cost authorisations.

The Director (CISO) is responsible for ensuring that acceptance criteria are identified, documented and included into system development and upgrade plans.

The Director (CISO) is responsible for drawing up test plans and for ensuring that new systems meet their specified acceptance criteria.

1. **Capacity Management** [ISO27002 Clause 12.1.3]
2. The initial capacity requirements of the application server for Retirement Capital are defined as:

* 10Mbps bandwidth
* 4 cores / 8 CPUs
* 16Gb RAM
* 64Gb Hard disk
* Linux Centos 7 OS

1. Retirement Capital requires available capacity sufficient to meet its peak demands plus a buffer percentage which is monitored weekly and assessed against current and future demands (as per work instruction ISMS-C-DOC 12.1.3a)
2. Capacity usage is recorded, measured and monitored and stored as ISMS-C-REC-12.1.3b and the Director (CISO) is responsible for ensuring that current requirements stay within the planned upper limits.
3. The Director (CISO) is responsible for identifying and implementing system improvements and tunings that will reduce the capacity requirements (and the change management procedure in control section 12.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx) does not apply to such changes).
4. Where there is evidence that requirements are higher than expected, the Director (CISO) investigates, identifies the cause(s) and proposes appropriate corrective action.
5. The Director (CISO) assesses, on a weekly basis (or more frequently if so required by the business), current and potential future capacity requirements in the light of planned or expected business developments and current and projected trends in Retirement Capital’s information processing capabilities and to plan appropriate capacity increases or decreases to meet those changing requirements.
6. Where an external party is involved in capacity planning issues, the owner of that external party relationship will be involved in any planning meetings.
7. Where information systems are part of the customer service or intensively used as management information systems, the Director (CISO) will ensure that business users contribute to identifying trends in usage and likely future requirements. Systems include operational systems, for example: email, Office products and operational systems, for example Orchestra.
8. **System Acceptance** [ISO27002 Clause 14.2.9 and Part 12.5.1]
9. Acceptance criteria for new information systems, upgrades to existing systems and new versions of current systems, must be identified and agreed at the initial planning stage.
10. Acceptance criteria will be specific to each system (or upgrade, etc.) and will be determined following a risk assessment. Acceptance criteria will cover business suitability, technical adequacy and security controls.
11. All new systems will be subject to testing prior to acceptance (see also control section 12.1.4 of the Manual). A test plan must be drawn up for each new system or, where appropriate, software implementation or upgrade, etc. that takes account (where relevant) of:
12. The business specification and user requirements (usability and user friendliness) for the new system.
13. The operational efficiency of the new system – i.e. does it deliver the business benefits expected of it?
14. The identified acceptance criteria.
15. Retirement Capital’s performance requirements and current capacity.
16. Methods of error recovery, system restart and contingency plans.
17. Methods of testing the systems routine operating procedures (and, where appropriate, manual procedures) to defined and agreed standards.
18. The set of required security controls (for the systems and in terms of any impact on the overall Retirement Capital) that were identified at project initiation.
19. Methods of testing for covert channels and Trojans.
20. Business continuity arrangements (in line with control section 17.1 of the Manual).
21. Interactions with other systems, to ensure that the new system will not adversely affect existing systems, including in capacity requirements.
22. Required training.
23. Ease of use.
24. When specifically requested by the customer, Retirement Capital will specify an external, formal certification and accreditation process to verify that security requirements have been addressed. The method for doing this will be determined when it is necessary to do follow this course.
25. **Technical review of applications after operating system changes** [ISO27002 Clause 14.2.3]
26. Business critical applications (identified in the Software Log [ISMS-C REC 8.1.1a](../Control%20A8%20-%20asset%20management/ISMS-C_REC_8.1.1a.docx) as high value) must pass pre-planned tests when operating systems are being changed and before implementation. These tests are subject to the change control process and all relevant information will stored under that change control.
27. The maintenance budget must be adjusted to allow for any cost changes resulting from the operational system change.
28. Business Continuity Plans must be updated.
29. **Protection of system test data** [ISO27002 Clause 14.3.1]
30. Operational databases containing personal information are not used for testing of operational software.
31. All test data for final system testing will be provided by the customer, development test data will be created in house and no person-identifiable data will be used.

***Document Owner and Approval***

The Director (CISO) is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Director (CISO) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |