ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

RiG CERT

Security category – 12.1. Operational procedures and responsibilities

Control – 12.1.1. Documented operating procedures
The organization should document and make available to all users operating procedures.

Documented procedures should be prepared for operational activities associated with information processing and communication activities.

The operating procedures should specify operational instructions like:
- installation and configuration of systems;
- processing and handling of information;
- backup;
- scheduling requirements - earliest job start and latest job completion times;
- instructions for handling errors and other exceptional conditions;
- support and escalation contacts in the event of unexpected difficulties;
- system restart and recovery procedures for use in the event of system failure…

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Control – 12.1.2. Change management
The organization should control changes that affect information security.

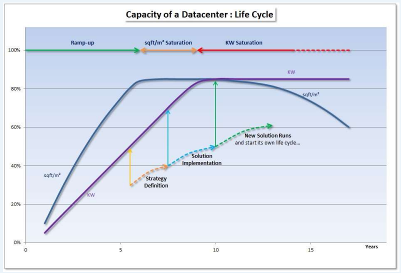
Uncontrolled changes to systems, processes or information processing facilities can cause major problems to business.

Guidelines of ISO/IEC 27002 with regards to change management:

- planning and testing of changes prior to implementation;
- assessing the potential impacts of changes, including security impacts, before implementation;
- a formal approval process for proposed changes;
- communication of change details to all relevant persons;
- how and when to abort change and actions to recover from unsuccessful changes.

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Control – 12.1.3. Capacity management
The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.



Capacity management refers to information processing facilities but also to office space and human resources.

Sufficient capacity can be achieved by increasing capacity or reducing demand for resources.

Critical systems like network gateways or main database servers should be prioritized and there should be a documented capacity plan made for those resources

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Control – 12.1.4. Separation of development, testing and operational environments
The organization should separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment.

The operational systems must be kept reliable and using the same equipment or software for both current operation and development and testing of new systems - can affect the operational environment's integrity and availability.

Its desirable that development and operational software be segregated through strong access controls.

- separate domains completely segregated from each other (if not separate log-on procedures)
- users should use different profiles for operational and testing systems;
- compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required.