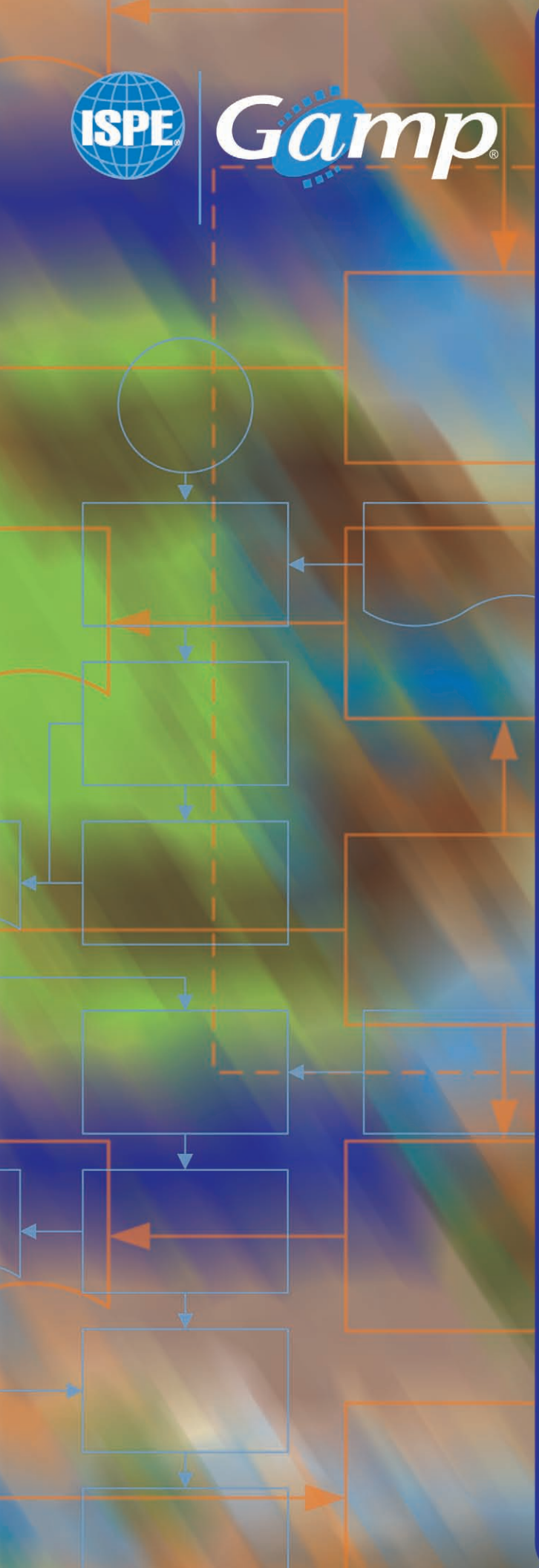


GAMP Good Practice Guide

A Risk-Based Approach to Operation of GxP Computerized Systems

A Companion Volume to GAMP® 5

GAMP Good Practice Guide

A Risk-Based Approach to Operation of GxP Computerized Systems

A Companion Volume to GAMP® 5

Disclaimer:
This Guide is meant to assist pharmaceutical organizations in determining a common understanding of the concept and principles of operation of GxP computerized systems.The International Society for Pharmaceutical Engineering (ISPE) cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

All trademarks used are acknowledged.

ISBN 1-931879-73-7

Preface

Regulated computerized systems should be maintained in a demonstrable state of control and in accordance with regulatory requirements. Maintained regulated data and records should be complete, accurate, and secure. Some regulated data and records need to be retained after system retirement.

For regulated organizations, the Return On Investment (ROI) for the significant time and resources expended in implementing new computerized systems is achieved during the Operation Phase. Recovery from a failure to maintain control of a regulated system during the Operation Phase can be both time-consuming and expensive, and increase the risk to data integrity, product quality, and patient safety.

The purpose of this ISPE GAMP® Good Practice Guide, a Risk-Based Approach to Operation of GxP Computerized Systems, is to provide detailed information to enable organizations to support their systems more effectively during the Operation Phase of the system life cycle.

It provides comprehensive guidance for maintaining control of regulated systems throughout their operational life (including acceptance and release, system handover, through to system retirement and decommissioning). When applied as intended, this Guide can provide detailed direction on the required control processes which form a substantial part of an appropriate Quality Management System (QMS).

This Guide focuses on achieving effective and efficient business processes aligned with regulatory expectations, by providing generic principles which can be applied to regulated systems using a systematic and scalable approach.

This Guide addresses the operational and support processes that need to be established to receive regulated computerized systems into the Operation Phase of their life cycle and to maintain them in a state of compliance throughout their operational life, through to system retirement.

It is applicable to systems consisting of hardware and software of all GAMP® categories.

Guidance provided is scalable and can be applied to a range of systems, including:

- laboratory systems
- process control systems
- IT applications

Whereas GAMP® 5 is primarily concerned with strategic approaches and planning of operational activities, this Guide contains more detailed information, including:

- a fuller consideration of process scope
- risk-based scalability considerations
- the appropriate assignment of roles and responsibilities
- identification of associated records
- example procedures

Process flow diagrams provided are intended to assist in making the process steps and their interrelationships clear and accessible. Wherever possible a common terminology has been adopted to describe the required management processes, to allow the guidance to be accessible to as wide a readership as possible.

Acknowledgements

This Guide was developed by a team under the **co-leadership** of **Kate Samways** and **Rob Stephenson**.

Section Writers and Reviewers

This Guide was produced by a dedicated team of subject matter experts from across the industry. The leaders of this Guide would like to recognize the following participants who took lead roles in the authoring of this document.

Karen Alexander	Pfizer Limited	United Kingdom
Winnie Cappucci	Bayer HealthCare	USA
Pam Lawrence	Perceptive Informatics	United Kingdom
Scott Lewis	Eli Lilly and Company Limited	United Kingdom
Christopher Loscombe	Eli Lilly and Company Limited	United Kingdom
Munya Mafemba	Johnson & Johnson	United Kingdom
Chris Reid	Integrity Solutions Limited	United Kingdom
Elizabeth Harrison	GSK	United Kingdom
Kate Samways	KAS Associates	United Kingdom
Genni Sanders	Systematicity Limited	United Kingdom
James Stafford	Business & Decision Limited	United Kingdom
Rob Stephenson	Pfizer Limited	United Kingdom
Simon Topham	Napp Pharmaceuticals Limited	United Kingdom
Charlie Wakeham	Pall Corporation	United Kingdom

Special thanks go to Sam Brooks (Novartis) and Chris Clark (Napp Pharmaceuticals Limited) for their editorial contributions, coaching, and tireless support of this Guide.

Many other individuals reviewed and provided comments during the preparation of this Guide; although they are too numerous to list here, their input is greatly appreciated.

ENGINEERING
PHARMACEUTICAL
INNOVATION

ISPE Headquarters
3109 W. Dr. Martin Luther King Jr. Blvd., Suite 250, Tampa, Florida 33607 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

ISPE Asia Pacific Office
73 Bukit Timah Road, #04-01 Rex House, Singapore 229832
Tel: +65-6496-5502, Fax: +65-6336-6449

ISPE China Office
Suite 2302, Wise Logic International Center
No. 66 North Shan Xi Road, Shanghai, China 200041
Tel +86-21-5116-0265, Fax +86-21-5116-0260

ISPE European Office
Avenue de Tervueren, 300, B-1150 Brussels, Belgium
Tel: +32-2-743-4422, Fax: +32-2-743-1550

www.ISPE.org

Table of Contents

1 Introduction

1.1 Overview

For regulated organizations, the Return On Investment (ROI) for the significant time and resources expended in implementing new computerized systems is achieved during the Operation Phase. The Operation Phase is usually significantly longer than the time spent in developing and delivering the system to the user community.

Regulated computerized systems should be maintained in a demonstrable state of control and in accordance with regulatory requirements. This applies to all components of the system (e.g., hardware, software, infrastructure, documentation, and personnel) throughout the system life cycle, from concept to retirement. Maintained regulated data and records should be complete, accurate, and secure. Some regulated data and records need to be retained after system retirement. Organizations should ensure that their integrity is assured for any required trending, re-evaluation, or inspection purposes within the defined retention period.

During the operational life of a GxP system, regulators usually focus on the integrity, consistency, and completeness of controls required to maintain compliance.

Recovery from a failure to maintain control of a regulated system during the Operation Phase can be both time-consuming and expensive, and increase the risk to data integrity, product quality, and patient safety.

Operational management controls should be established prior to acceptance and release and maintained throughout the Operation Phase of the system life cycle. Incidents and changes to systems should be managed effectively and efficiently, and the required records produced and retained.

These controls are similar to those employed to comply with the Sarbanes-Oxley (SOX) Act, the Federal Information Security Management Act (FISMA), and other regulations. All share common elements with ISO 20001 (ISO 17799) (Reference 4, Appendix 4).

1.2 Purpose

The purpose of this ISPE GAMP® Good Practice Guide, a Risk-Based Approach to Operation of GxP Computerized Systems (OGCS), is to provide detailed information to enable organizations to support their systems more effectively during the Operation Phase of the system life cycle.

It provides comprehensive guidance for maintaining control of regulated systems throughout their operational life (including acceptance and release, system handover, through to system retirement and decommissioning). When applied as intended, this Guide can provide detailed direction on the required control processes which form a substantial part of an appropriate Quality Management System (QMS).

This Guide focuses on achieving effective and efficient business processes aligned with regulatory expectations, by providing generic principles which can be applied to regulated systems using a systematic and scalable approach.

Risk-based controls should be implemented at a level of formality and complexity appropriate to an organization and system.

This Guide addresses the operational and support processes that need to be established to receive regulated computerized systems into the Operation Phase of their life cycle and to maintain them in a state of compliance throughout their operational life, through to system retirement.

It is applicable to systems consisting of hardware and software of all GAMP® categories.

Guidance provided is scalable and can be applied to a range of systems, including:

- laboratory systems
- process control systems
- IT applications

Whereas GAMP® 5 (Reference 7, Appendix 4) is primarily concerned with strategic approaches and planning of operational activities, this Guide contains more detailed information, including:

- a fuller consideration of process scope
- risk-based scalability considerations
- the appropriate assignment of roles and responsibilities
- identification of associated records
- example documentation and record content

Table 2.1 links each operational process described in this Guide and the related GAMP® 5 Appendix.

The process flow diagrams provided are intended to assist in making the process steps and their interrelationships clear and accessible. Wherever possible, a common terminology has been adopted to describe the required management processes, to allow the guidance to be accessible to as wide a readership as possible.

This Guide is intended to be of interest to:

- Process Owners
- System Owners
- Subject Matter Experts (SMEs)
- Quality Unit Representatives
- End Users
- Support Organizations
- Suppliers
- Other Stakeholders

For further information, see Section 19 of this Guide (Appendix 1: RACI Roles and Processes).

This Guide is based on the output of a GAMP® Community of Practice (COP) Special Interest Group initially concerned with the topic of 'Maintaining Control during Operation' of regulated computerized systems. The material presented in this Guide has developed and evolved in parallel to guidance provided in GAMP® 5 and is intended to align with and supplement that guidance.

1.3 Benefits

This Guide aims to increase the awareness of the importance of the Operation Phase and to assist in the development, implementation, and maintenance of efficient, cost-effective, and compliant processes and procedures.

This Guide seeks to:

- provide a better understanding of both the individual operational processes and the interrelationships between them
- help organizations to assign clear roles and responsibilities to required activities throughout the Operation Phase
- embed scalable risk-based approaches into the definition and management of those internal and external operational processes

This Guide aims to help regulated organizations to achieve regulated computerized systems that are fit for intended use and compliant with applicable regulations.

1.4 Key Concepts

This Guide describes an integrated approach to the management, maintenance, and control of regulated computerized systems. GAMP® 5 (Reference 7, Appendix 4) terminology and key concepts are applied to the Operation Phase.

These GAMP® 5 key concepts are:

1. product and process understanding
2. life cycle approach within a QMS
3. scalable life cycle activities
4. science-based quality risk management
5. leveraging supplier involvement

Product and process understanding is essential to the selection of appropriate and scalable controls and procedures. This focus also gives alignment with the ISPE Product Quality Lifecycle Implementation (PQLI) Initiative.

The application of a Quality Management System based approach is aligned with ICH Q10 (Pharmaceutical Quality System) (Reference 6, Appendix 4). A quality risk management approach aligned with ICH Q9 (Quality Risk Management) (Reference 5, Appendix 4) is applied.

The opportunities for leveraging supplier resource and expertise to provide support throughout the Operation Phase are considered. The Guide also takes into account the increased use of computerized systems to support the main operational processes.

The Guide applies the widely used RACI terminology to ensure that roles and responsibilities are identified, defined, and understood (see Appendix 1 for more information).

The Guide has been aligned wherever possible and appropriate with the IT Infrastructure Library (ITIL® V3) (Reference 10, Appendix 4) and Control Objectives for Information and related Technology (COBIT®) (Reference 9, Appendix 4) approaches and terminology. (See Appendix 2 which maps the operational processes described in this Guide to ITIL® and COBIT®).

1.5 Structure of this Guide

This Guide consists of a Main Body, including introductory sections, detailed operational guidance, and sections on data migration and system retirement.

The introductory sections consist of:

- **Introduction:** Overview, Scope, Purpose, Benefits, Key Concepts, and Structure of this Guide
- **Overview of the Operation Phase**
- **What Organizations should do:** how to implement the guidance

The detailed operational guidance sections have each been structured in the same way to present the information in a consistent and accessible manner:

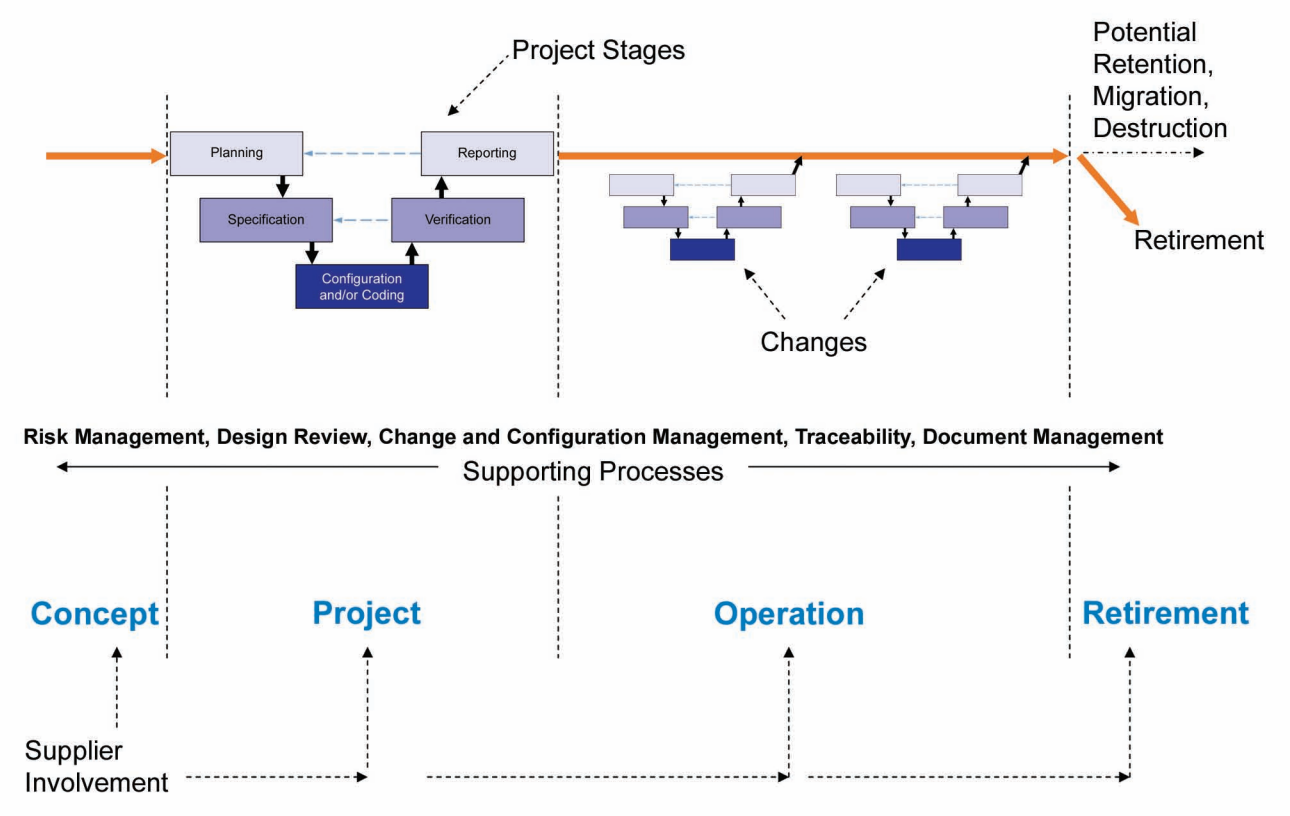
- **Introduction:** the purpose of the Operational Process being described
- **Scope:** the scope of the guideline for the Operational Process being described
- **Roles and Responsibilities:** a table in system role order summarizing the RACI assignments for the operational process and detailing main responsibilities for each role related to the operational process being described.
- **Process Flow Diagram:** representation of the Operational Process as a workflow diagram identifying critical process steps, interactions with other operational processes, decision points, and required records. Shading is used to indicate activities and records directly related to the operational processes and is reflected in the associated process narratives.
- **Process Narrative:** a tabular representation of the process flow diagram with additional guidance specific to each process step.
- **Procedural Guidelines and Considerations:** a section providing further guidance information regarding any additional considerations relating to establishing and maintaining the operational process.
- **Records and Record Content:** a list of the expected evidential records for each of the operational processes with their expected content.
- **Scalability:** a risk-based consideration of how the operational process can be appropriately scaled depending on the impact of the system on patient safety, product quality, and data integrity, and on the business impact of the system.

Three Appendices discuss RACI Roles, processes and their relationship to ITIL® (Reference 10, Appendix 4) and COBIT® (Reference 9, Appendix 4), and provide a list of control records.

2 Overview of the Operation Phase

Figure 2.1 (from GAMP® 5) shows the Operation Phase in the context of the complete system life cycle.

Figure 2.1: Life Cycle Phases Highlighting the Operation Phase



Organizations should ensure that appropriate operational processes, procedures, and plans have been implemented and are supported by appropriate training, in preparation for acceptance and release, and system handover. Suppliers may be involved in support and maintenance activities.

Compliance and fitness for intended use should be maintained throughout the Operation Phase. This may be achieved by the use of documented procedures and training that cover use, maintenance, and management.

The Operation Phase of a system may last many years, and may include changes to:

- software
- hardware
- system configuration
- business process regulatory requirements

The integrity of the system and its data should be maintained and verified as part of periodic review. Data life cycle considerations are inherent in the operational, support, and management processes described.

Opportunities for process and system improvements should be based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Information from Incident Management and Corrective and Preventive Action (CAPA) processes can provide significant input to the evaluation.

Change management should provide a reliable mechanism for rapid implementation of technically sound improvements following the approach to specification, design, and verification described in GAMP® 5 (Reference 7, Appendix 4). The rigor of the approach, including the extent of documentation and verification, should be based on the risk and complexity of the change and the risk to patient safety, product quality, and data integrity.

Maintaining system compliance during operation requires the performance of interrelated activities and the approach taken should be scaled according to the nature, risk, and complexity of the system. Figure 2.2 gives an overview of the major relationships between related groups of these activities.

Groups may contain several individual related processes, procedures, and plans (see Table 2.1).

Figure 2.2: Major Information Flows between Operational Activities

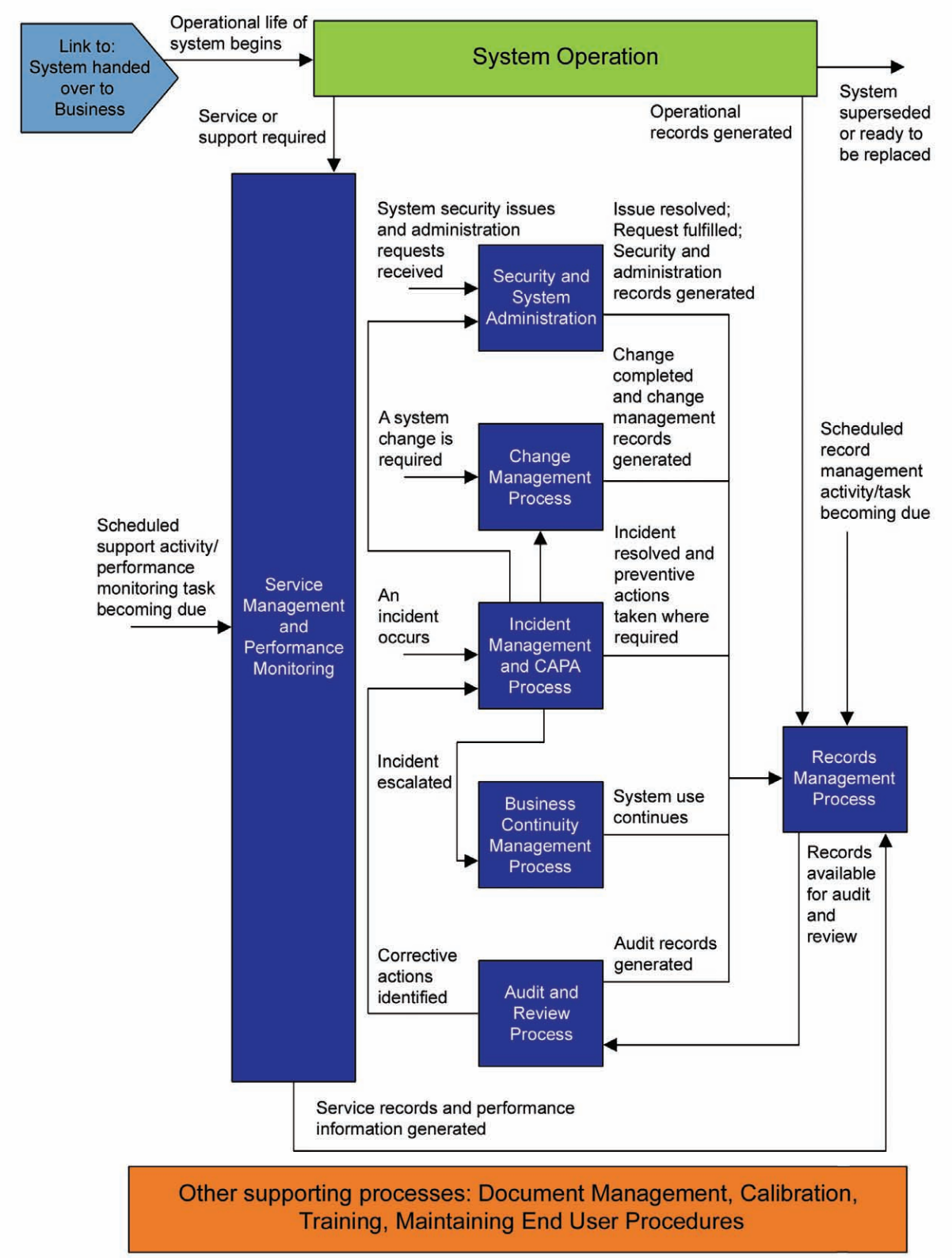


Table 2.1: Grouping of Operation Phase Processes

Group of Processes	Process	This Guide Section	GAMP® 5 Appendix
Handover	• Handover Process	5	O1
Service Management and Performance Monitoring	• Establishing and Managing Support Services • Performance Monitoring	6 7	O2, S5 O3
Incident Management and CAPA	• Incident Management • CAPA	8 9	O4 O5
Change Management	• Operational Change and Configuration Management • Repair Activity	10 11	O6 O7
Audits and Reviews	• Periodic Review • Internal Quality Audits	12	O8 -
Business Continuity Management	• Back Up and Restore • Business Continuity Planning (includes Disaster Recovery Planning)	13 14	O9 O10
Security and System Administration	• Security Management • Systems Administration	15 16	O11 O12
Records Management	• Archiving and Retrieval[1]	-	O13
Plus the following processes included in the scope of this Guide:			
Data Migration	• Data Migration	17	D7
System Retirement	• System Retirement, Decommissioning, and Disposal	18	M10

These operational processes are supported by QMS activities, such as document management training management, calibration management, and the maintenance of end user procedures. For further information, see GAMP® 5 and ISPE GAMP® Good Practice Guide: Calibration Management (Reference 8, Appendix 4).

For further information on the individual support and maintenance processes required to maintain the compliance of regulated computerized systems during operation, see the sections of this Guide listed in Table 2.1.

[1] For a more detailed discussion of archiving and retrieval, see ISPE GAMP® Good Practice Guide: Electronic Data Archiving (Reference 8, Appendix 4).

3 What Organizations Should Do

3.1 Introduction

To ensure compliance with regulatory expectations organizations should be able to demonstrate that the maintenance and support needs for each system have been reviewed. Appropriate procedures, processes, and records should be established. This evaluation should be performed during the Project Phase; specific elements may be addressed in the Operation Phase.

Operational processes may be generic in nature, system specific, or generic with system specific schedules attached.

Table 4.1 shows how operational processes are related and how they may trigger other operational processes or support processes.

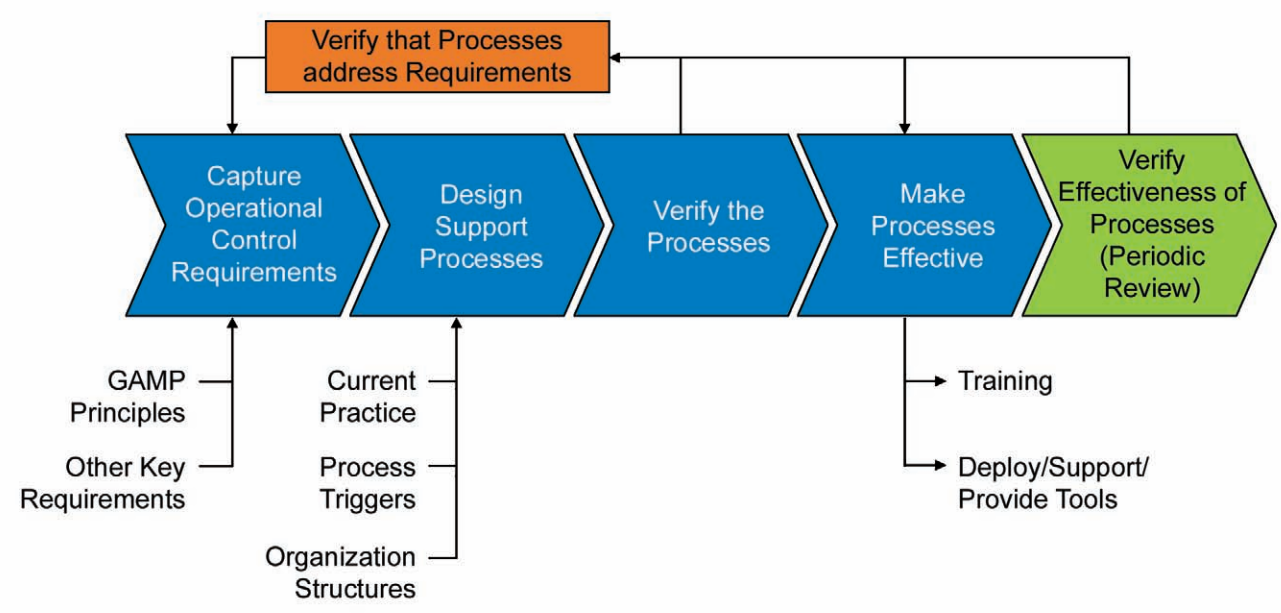
A possible approach to establishing operational control is discussed.

The key steps of this approach include:

- capture operational control requirements (ideally, during the Project Phase)
- design operational processes (ideally, during the Project Phase)
- verify the processes (ideally, during the Project Phase)
- deploy processes
- verify effectiveness of processes

The relationship between these steps is shown in Figure 3.1 and described in this section. These relationships can be subject to ongoing change. It is particularly important to ensure that the processes continue to address requirements and that any updates are managed under change control.

Figure 3.1: Establishing Operational Control



3.2 Capture of Operational Control Requirements

Organizations should be able to demonstrate that processes to achieve operational control requirements are established and that records are maintained for the required retention period, to demonstrate that controls are effective.

The interrelationships between these processes should be considered, to ensure that operational incidents and changes to systems during their operational life cycle are effectively managed, and that the security and integrity of critical records and processes are maintained.

A consistent approach to addressing should be established. Business and regulatory requirements should be considered, e.g.:

- Environmental, Health and Safety regulations
- Sarbanes-Oxley (SOX) controls
- Privacy and Data Protection regulations (such as Health Insurance Portability and Accountability Act (HIPAA)
- Industry specific regulations, such as Payment Card Industry Data Security Standards (PCI DSS)
- local regulations

3.3 Design of Operational Processes

Current practices for the operational management of existing systems within the organization need to be understood before developing a detailed plan for the implementation of operational controls. There may be a significant number of support and review processes established, which already may have been subject to audit and review.

Where there are existing processes a gap analysis can be developed against the operational control requirements statements in order to identify improvement activities.

Controlling procedures which describe the processes should be practical. A definition of the current processes should be produced by consulting those involved. It is generally better to improve and simplify existing processes rather than to create new procedures.

Where a gap is identified and there is no current process supporting a set of key requirements, a new process will need to be designed and implemented. The need to understand how the various processes interrelate is critical to maintain operational control; process design should consider how other processes may be triggered and responsibilities for each process step should be clearly assigned.

A critical consideration in the design of processes and the creation of procedures is the organizational structure of the enterprise; this will determine who has overall responsibility for each process and who is responsible for task steps within the process. For small organizations some of these controls may be achieved through the consistent application of written procedures. For larger organizations, electronic systems may be used to assign roles and permissions, keep track of critical records, and ensure that activities are notified to the correct individuals or teams and escalated appropriately, e.g., in the case of service or control failures. Paper-based systems may be adequate.

3.4 Verification of Processes

Once the processes have been established, procedures documented, and personnel trained, they should be verified to ensure that the required level of control is in place. Subsequent amendments to the processes should be managed under change control.

3.5 Deployment of Processes

Once processes have been verified, they should be deployed consistently throughout an organization. This may be achieved by a deployment plan which should include a communication plan, the roll-out of training, where appropriate, and provision of the necessary resources, e.g., record forms and log books, personnel.

3.6 Verification of the Effectiveness of Processes

For regulated systems, the Quality Unit should be involved in the review and approval of operational processes. The scope and depth of involvement of the Quality Unit depends on the impact of a system on patient safety, product quality, and data integrity, and should be documented. Opportunities to combine with other compliance testing of internal controls may be considered, e.g., SOX audits.

The Quality Unit should verify effectiveness of operational processes by audit and review using internal assessment tools and Periodic Review.

Appropriate metrics can help to ensure key performance indicators are being met and to support investigation or improvement initiatives.

4 Process Relationships

Table 4.1 shows the interrelationships and dependencies between operational processes and other related processes.

Table 4.1 is intended to help organizations implement a comprehensive set of operational processes and records in a structured way by:

- ensuring completeness: showing which processes should be supported by controlling procedures
- providing an aid to navigation: supporting users when undertaking an impact analysis to establish which other processes may be triggered

Table 4.1: 'Triggers and Checks'

For each process in the top row, the vertical column indicates those processes that potentially trigger another process (t) or are part of a checking process (c). E.g., **O7 Repair Activity** may trigger **O6 Operational Change and Configuration Management**; **O1 Handover** may check that an **O7 Repair Activity** process is in place.	O1 Handover	O2 Establishing and Managing Support Services	O3 Performance Monitoring	O4 Incident Management	O5 Corrective and Preventive Action	O6 Operational Change and Configuration Management	O7 Repair Activity	O8 Periodic Review	O9 Backup and Restore	O10 Business Continuity Management	O11 Security Management	O12 System Administration	D7 Data Migration	M10 System Retirement, Decommissioning, and Disposal
O1 Handover														
O2 Establishing and Managing Support Services	c		t		t			c						
O3 Performance Monitoring	c	t		t	t			t/c		t				
O4 Incident Management	c		t/c					c			t			
O5 Corrective and Preventive Action	c		t	t				t/c						
O6 Operational Change and Configuration Management	c		t	t	t		t	c		t				
O7 Repair Activity	c	t	t/c	t	t			c		t				
O8 Periodic Review			t	t	t									
O9 Backup and Restore	c	t	t			t		c		t			t	t
O10 Business Continuity Management	c			t	t			c						
O11 Security Management	c			t	t			t/c						
O12 System Administration	c	t		t	t			c						
D7 Data Migration						t		c						t
M10 System Retirement, Decommissioning, and Disposal		t	t	t				t						
• Training	c	t	t	t	t	t		c		t				
• Calibration	c		t		t		t	c						
M9 Document Management	c				t	t		t/c						t
• Application Specific Operational Use SOPs	c				t	t		c						
• SDLC Processes and Procedures	c				t	t		c						
• Validation Processes	c				t	t		c					t	t

Note: Archiving and Retrieval (O13) is not included in this table as a more detailed discussion of this topic is included in the ISPE GAMP® Good Practice Guide: Electronic Data Archiving (Reference 8, Appendix 4).

Notes:

The O, D, and M numbers in Table 4.1 and throughout this Guide refer to specific appendices in GAMP® 5. For example, O1 refers to Appendix O1 *Handover* in GAMP® 5 (Reference 7, Appendix 4).

Topics in the Table 4.1 with no number, e.g., Training and Calibration, do not have a dedicated Appendix in GAMP® 5, but are covered in appropriate sections of GAMP® 5.

Table 4.1 provides an indication of where 'triggers' and 'checks' may be appropriate. As organizations may arrange or scope their business processes differently or use different terminology, Table 4.1 is subject to interpretation.

- A 'trigger' is intended to represent the concept that one process may initiate the use of another process.
- A 'check' is intended to represent the concept that one process may seek to assure that another process has been defined, approved, and is in place.

5 Handover

5.1 Introduction

The Handover process defines the controls required for the transition of a computerized system from a project into the Operation Phase. The process ensures that the environment into which the system is to be received is prepared, to ensure that the system can be used and supported in a controlled manner. The Handover process should ensure that:

- Project (including license and warranty agreements) and project validation activities are complete.
- Configuration items (software, hardware, documentation) are transferred to user and support organization.
- Document management and archiving controls are established and required documentation is archived.
- Operational and support organizations are established and roles defined.
- System management, use, administration, and operational processes are established.
- Support services are defined.
- System users, administrators, and support organizations are trained.
- Data setup is complete (including cutover activities).
- Security setup is complete.
- Residual risks and issues are transferred to user and support organizations.

Note: other processes may be responsible for delivery of the listed activities and creation of the listed documentation, e.g., several of these activities may be included in the verification tasks within the scope of the Validation Plan. The handover process should ensure that the listed activities have been completed and appropriately documented.

This section is related to Appendix O1 of GAMP® 5 (Reference 7, Appendix 4).

5.2 Scope

This process applies to the transition of systems from the Project Phase to the Operation Phase. The principles of this process apply to computerized systems; it can be scaled according the complexity of the system and organization. This process also can be applied when upgrading systems or when changing support organizations.

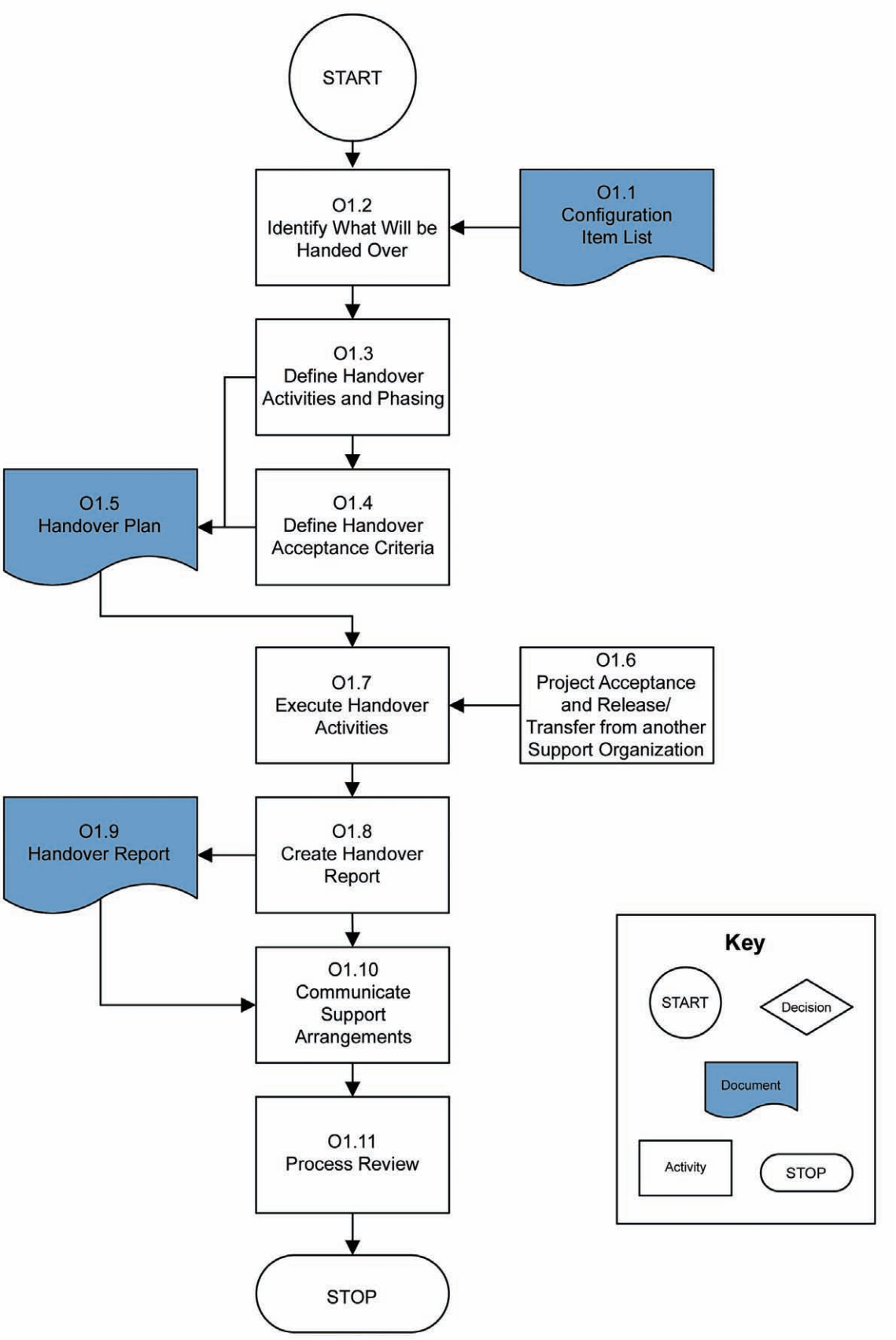
5.3 Roles and Responsibilities

Table 5.1 provides an indicative example. Organizations should allocate roles and responsibilities based on organizational structure and the specific system.

Table 5.1: Roles and Responsibilities for Handover

Role	RACI Role	Responsibilities
Process Owner	R	• takes responsibility for accepting the system into operation • takes responsibility for resolution of residual system issues and risks following acceptance and release
System Owner	R	• takes responsibility for the availability and support and maintenance of a system and for the security of data residing on that system • ensures that system documentation, Standard Operating Procedures (SOPs), system manuals, support agreements, and training are delivered prior to completion of Handover • shares responsibility for resolution of residual system issues and risks following acceptance and release
Project Manager	A	• ensures that Handover activities are incorporated into project plans • ensures that residual issues and risks are communicated and accepted by the Process Owner and System Owner • ensures that acceptance and release decision mandates that Handover activities and documentation are delivered
End User	I	• provides input into development of SOPs and training • attends system and SOP training • works to established operational procedures
Quality Unit	C	• reviews validation report and compliance with quality standards/procedures to ensure control and any residual risks are acceptable for acceptance and release
Platform Support (SME)	R	• takes responsibility for technical platform documentation • establishes Service Level Agreements (SLAs) where required • provides input into development of SOPs and training • attends or delivers training, provides system support, and technical requirements • supplies ‘as built’ system documentation
Application Support (SME)	R	• takes responsibility for technical application documentation • establishes SLAs where required • provides input into development of SOPs and training • attends or delivers training, provides system support, and technical requirements • supplies ‘as built’ system documentation
System Administrator	R	• responsible for technical/data setup and administrative procedures (e.g., security administration, maintenance, backup, and restore)
Supplier	C	• provides input to a client SLA or provides a standard supplier SLA • attends SOP/support training if involved in support • delivers training, system support, and technical requirements • supplies or makes available ‘as built’ system documentation and software
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

5.4 Handover Process Flow Diagram



5.5 Process Narrative

Process Step/Decision/Record	Description
O1 Handover	**A risk-based process by which a Project Team (or other support organization) transfers a system into the Operation Phase.**
O1.1 Configuration Item List	This list should be generated in the Project Phase under the **Configuration Management** process and should include system components and documentation.
O1.2 Identify What Will be Handed Over	The Handover process should transition system components, accountabilities, knowledge, documentation, procedural controls, and support agreements to relevant organizations. Such organizations include Process Owners, System Owners, SMEs (Platform Support, Application Support, etc.), End Users, Supplier Organizations, Document Management, and Quality Units. Process and System ownership, roles and responsibilities, and documentation ownership should be explicit.
O1.3 Define Handover Activities and Phasing	Handover is a series of activities required to transfer a system into Operation. These activities should be defined and agreed by the transferring and receiving parties. **Note:** specific Handover activities may not be completed before system acceptance and release. There should be an explicit action plan for undelivered Handover items before acceptance and release within the context of a risk and impact analysis.
O1.4 Define Handover Acceptance Criteria	Acceptance criteria may be used to define the basis by which Handover activities are deemed complete, e.g., approved training records are in established; SLAs have been created, reviewed, and approved.
O1.5 Handover Plan	The Handover Plan should document the tasks, responsibilities, timing, and acceptance criteria to establish when Handover is complete. The Handover Plan should be approved by the transferring and receiving parties. The Handover Plan may be a separate document or may be incorporated within relevant project documentation.
O1.6 Project Acceptance and Release/Transfer from another Support Organization	The deliverable/technical aspect of the Handover process, can start only: • when a project team completes the Project Phase and hands over the system for operational use • when the support of a system already in operation is handed over from one support provider to another Planning for Handover should be initiated at an earlier stage to ensure that the Handover is managed effectively.
O1.7 Execute Handover Activities	The Handover Plan should be executed. Meetings between transferring and receiving groups should be scheduled, as appropriate, to ensure that progress is made to complete agreed activities.
O1.8 Create Handover Report	The Handover Report should summarize Handover activities against the Handover Plan. Deviations should be assessed for impact and appropriate action should be taken.

5.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O1.9 Handover Report	The Handover Report should document completion of all agreed activities and acceptance of any items that are not complete (may be covered by Validation or Project Report). Approval by Project Manager and System Owner signifies acceptance of the system into the Operation Phase. The Handover Report may be an input to O1.10 Communicate Support Arrangements.
O1.10 Communicate Support Arrangements	Support organizations, processes, and agreements are communicated to system users. This may be undertaken by the System Owner with support from the Project Team.
O1.11 Process Review	Following Handover a review should be conducted to identify any lessons learned and any opportunities for improvement in the Handover process. This may be undertaken by the System Owner with support from the Project Team. The process review also may be scheduled to coincide with the review of SOPs. (This is independent of a review of the project.)

5.6 Procedural Guidelines and Considerations

5.6.1 Project Acceptance and Release or Transfer from another Support Organization

Handover planning should be considered when transferring a new system into the Operation Phase, when implementing significant system modifications or upgrades, or when changing support organizations or end user groups.

The Handover process should ensure that the system is fit for Handover and that the operation and support organizations are ready to take ownership of system use and management (roles defined, operational processes and procedures in place, residual risks accepted and support organizations in place to maintain compliance). Accountability and responsibility for the system (hardware, software, documentation, and data) is transferred from the project organization to the Process Owner and System Owner, respectively.

External support organizations may be used, e.g., where expertise or resources are not available within the user organization. Where support services are provided for systems which may have a high impact on processes or where the scope of external support services provided is high, a supplier assessment should be considered in consultation with the Quality Unit.

5.6.2 Define Handover Plan

Handover activities can be broken down into several areas and should ensure that:

- Project (including license and warranty agreements) and Validation Activities are complete.
- Configuration Items (software, hardware, documentation) are accessible to user and support organizations.
- Document Management and Archiving controls are in place and required documentation is archived.
- Operational and Support Organizations are in place and roles defined.
- System Management, Use, Administration, Operational and Support Processes and SOPs are in place.
- Operational and Support Services are defined and organizations in place.

- Skills and knowledge are transferred, including training of System Users, Administrators and Support organizations.
- Data Setup is complete.
- Security Setup is complete.
- Residual Risks and Issues are handed over to user and support organizations.

Section 5.7.1 provides an example structure and content of the Handover Plan.

Documentation should be in an "as built" state. Handed over documentation should be under document management control and stored in secure electronic or physical document repositories. Documents which require ongoing maintenance (e.g., design documents) should be accessible by support organizations to allow maintenance under configuration management. Documents which do not require ongoing maintenance (e.g., executed test documentation) should be accessible for information purposes and archived for historical access.

Handover may be phased and activities may be scaled according to the complexity of a system, in regard to:

- geographic distribution of the system
- number of sites
- consistency in intended use
- use of third party support organizations

Other considerations for a phased Handover include whether the system is to be implemented vertically (e.g., system supports complete business process in one area, site, or division) or horizontally (e.g., functionality is provided to support an aspect of a business process across several areas, sites, or divisions).

Handover Plans should be agreed by Project Managers, Support Organizations, and User Organizations, including Quality Units.

For complex projects, a Handover manager may be beneficial in coordinating between the project team and the operating organization.

5.6.3 Define Acceptance Criteria

Acceptance criteria should be established to ensure that the providing and receiving organizations are able to determine clearly that a Handover activity is complete. Criteria may include:

- 'as built' documentation available and approved
- validation summary report approved (confirming satisfactory specification, design, and testing of the system)
- training records updated for all planned training
- user and support organization roles defined
- review and monitoring processes are in place
- instrumentation added to calibration schedules

- availability of maintenance schedules with defined responsibilities
- SLAs approved and issued
- number of critical errors encountered in the first defined period of use

5.6.4 Completion of Handover Activities

Handover is considered complete when all activities in the Handover Plan are complete and all defined acceptance criteria have been met.

Project managers (or Handover managers) should monitor a Handover Plan regularly.

5.6.5 Communication

A Handover Report should be created to define the outcome of Handover activities. For less complex systems and projects, this may be summarized in a Validation Summary Report.

During Handover, Project Managers should communicate progress and discuss issues with Process Owners, System Owners, and Support Organization leaders.

5.7 Records and Record Content

5.7.1 Handover Plan

The Handover Plan (which may be incorporated into another document, e.g., the Validation Plan) should include:

- Purpose and Scope
- Operational Organization:
  - define roles and responsibilities of receiving organizations:
    - > process and system owner
    - > internal support organizations (application and platform)
    - > external support organizations
    - > quality unit
    - > documentation control and archiving organizations
- Configuration Items (refer to configuration item list)
  - system software components including version and build number (and licensing)
  - system hardware components
  - technical documentation (specifications, certificates, and manuals)
  - user documentation (user requirements, test documentation, plans, reports)

- system, design and configuration documentation, including security matrix

• Activities

- confirmation of project and validation activities
  - > validation summary report approved
  - > performance qualification completed and post implementation monitoring planned or performance qualification incorporated into post implementation monitoring
- handover of configuration items
  - > system hardware and software installation
  - > system software and configuration archiving
- document management and archiving
  - > update documentation to “as built” state
  - > system use documentation handover activities
  - > support documentation handover activities
  - > document archive activities
  - > document storage and access requirements
- operational and support organizations
  - > Process Owner
  - > System Owner
  - > applications support organization
  - > platform support organization
  - > external support organization(s)
- process and procedures
  - > performance monitoring
  - > incident management
  - > CAPA
  - > change management (including configuration management)
  - > repair
  - > periodic review

  - > business continuity management and disaster recovery
  - > backup and restoration
  - > security management
  - > archive, refresh, and retrieval
  - > retirement and decommissioning
  - > document management
  - > training
  - > calibration
  - > system use
- support services
  - > SLAs
  - > support service governance structure
  - > updates to system Inventory
  - > calibration schedules and relevant certificates
  - > maintenance schedules
  - > provision of spare parts
- training
  - > users
  - > administrators
  - > support organizations
  - > management
  - > ongoing training (ownership, responsibilities, procedures)
- data setup
  - > data migration (for further information see Chapter 17 of this Guide)
  - > data setup
  - > isolation of test data from runtime environment
- security setup

> manage users, e.g., add new users, change user profiles, disable users

- risk and issues handover

> residual risks handed over from project risk management process

> pending changes

> known issues (including minor deviations)

> active work-arounds

- Schedule of Handover Tasks, Sequence, and Responsibilities to incorporate any phased Handover associated with the complexities of the system implementation (see Section 5.6.2 of this Guide)
- Acceptance Criteria
  - Criteria defined for each handover activity. Used to determine when activity is complete.

5.7.2 Handover Report

The Handover Report should provide a summary of completion of Handover Activities and acceptance criteria. The report should demonstrate that acceptance criteria have been met. Handover Reports may include:

- Handover Activity
- Planned Completion
- Actual Completion
- Acceptance Criteria
- Reference to evidence of Acceptance Criteria
- List or Reference to List, of Handover Documents
- Outstanding items (e.g., bugs, functionality gaps, deviations) and how they will be tracked to completion (e.g., via a CAPA unique ID)

5.8 Scalability

A separate System Handover Plan may be required, depending on the competence of suppliers (determined by an appropriate risk-based approach, e.g., use of the appropriate level of supplier assessment), the size and complexity of the system, and the size and complexity of the receiving operation and support organizations.

For less complex systems, a Handover Plan may be integrated into Project Plans or the Validation Plan. A checklist pro-forma also may be used. Handover Reports may be incorporated into Validation Summary Reports.

A Handover Manager may be appointed for large and complex systems, particularly for multi-site or global roll-outs.

The criticality of systems has only limited impact on the scalability of Handover Plans; large, complex systems with low to medium impact may benefit from Handover planning.

6 Establishing and Managing Support Services

6.1 Introduction

This guidance aims to define the process by which internal and external support services are defined, agreed, and managed to ensure that:

- Services are defined clearly.
- Roles and responsibilities, and interfaces between or within organizations, are defined clearly.
- Service delivery controls are established.
- Appropriate skills are established.
- Document and record ownership are defined clearly.
- Escalation procedures are established.
- Service performance can be monitored.
- Quality requirements are defined.

This section is related to Appendix O2 of GAMP® 5 (Reference 7, Appendix 4).

For further information on outsourced IS/IT environments, see GAMP® 5, Appendix S5 Managing Quality within an Outsourced IS/IT Environment.

6.2 Scope

This process applies when establishing internal and external support services. This guidance covers the identification of support services, creation of SLAs, delivery of support services, and the monitoring of performance against agreed service levels.

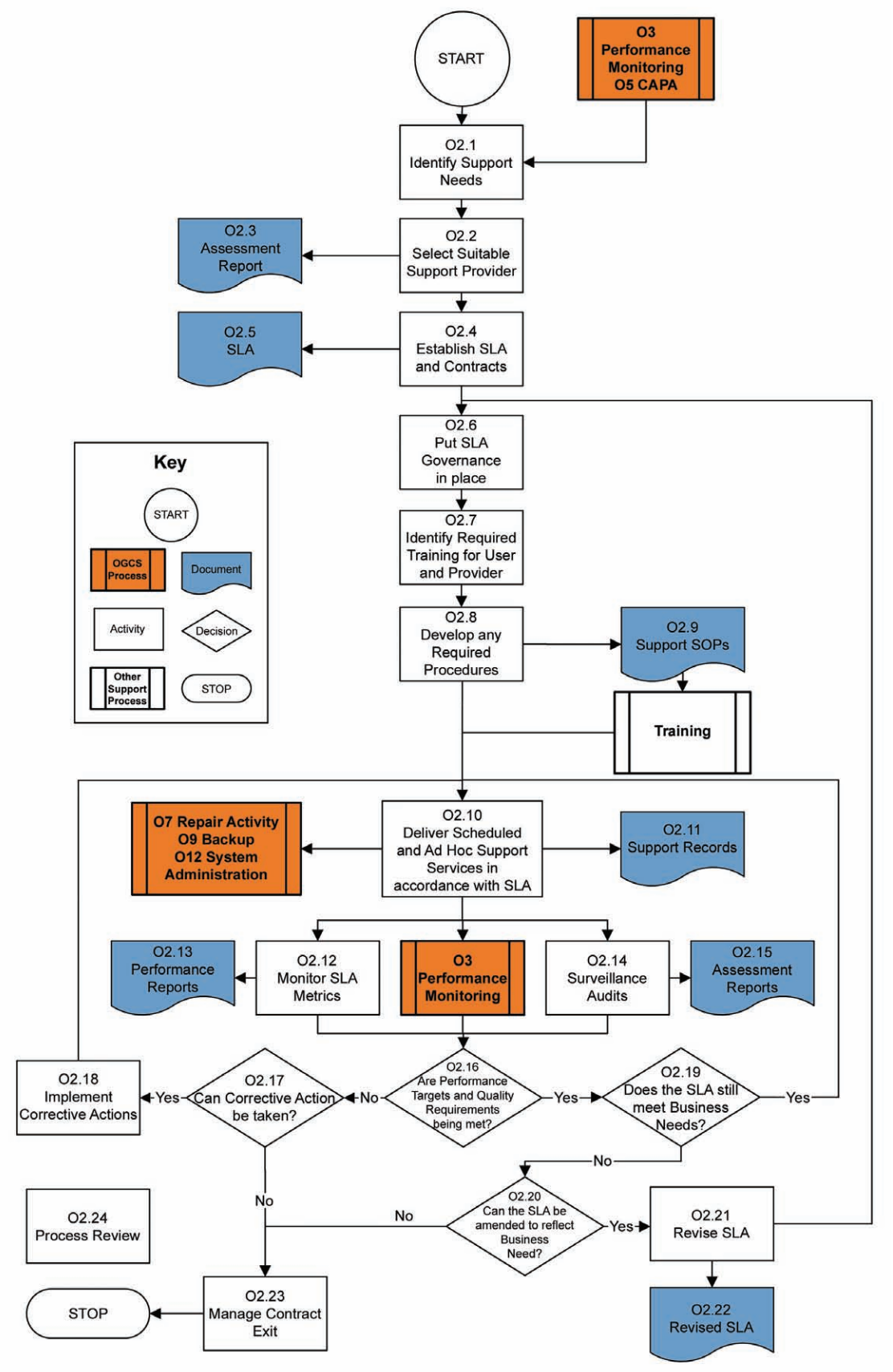
6.3 Roles and Responsibilities

Table 6.1 provides an indicative example. Organizations should allocate roles and responsibilities based on organizational structure and the specific system.

Table 6.1: Roles and Responsibilities for Establishing and Managing Support Services

Role	RACI Role	Responsibilities
Process Owner	C	• supports the determination of system impact and criticality of support service requirements • supports the determination of whether internal or external support organizations should be used
System Owner	A	• ensures that appropriate service providers are identified and evaluated • ensures that SLAs are in place • monitors the performance of services provided against agreed metrics • manages the service contract • defines the interfaces between user and support organizations • ensures that training in technical requirements and user procedures is provided to the support organization (where required) • ensures that the handover process has provided required procedures, documentation, skills, roles, etc., to enable effective support to be delivered • owns the support records
Project Manager	R	• ensures that SLAs are established prior to Handover (where required)
End User	I	• is made aware of support services and means of accessing support services • follows defined procedures and SLAs when accessing support services
Quality Unit	C	• evaluates external and internal support organizations • ensures that regulatory and quality requirements, e.g., audit, documentation standards, procedural controls, record keeping, and training are defined within support contracts and SLAs • reviews effect of deviations from agreed service definition and levels
Platform Support (SME)	R	• provides support (or manages external support) in accordance with agreed SLAs
Application Support (SME)	R	• provides support (or manages external support) in accordance with agreed SLAs
System Administrator (SME)	R	• provides support (or manages external support) in accordance with agreed SLAs
Supplier	C	• provides support in accordance with agreed SLAs
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

6.4 Establishing and Managing Support Services Process Flow Diagram



6.5 Process Narrative

Process Step/Decision/Record	Description
O2 Establishing and Managing Support Services	**An operational process for ensuring that maintenance and support contracts are appropriately specified and managed.**
O2.1 Identify Support Needs	Process Owner and System Owner identify support required for a system from both internal and external support organizations. A review of support requirements may be triggered by the operational processes **O3 Performance Monitoring** and **O5 Corrective and Preventive Action**.
O2.2 Select Suitable Support Provider	Appropriate support organization is identified. If provider is an external supplier and services are high impact an audit or other means of supplier assessment should be considered. Internal reviews may be less formal, but necessary checks should be performed.
O2.3 Assessment Report	Prior to agreement, Assessment Report is created and observations addressed (where possible). The Assessment Report should include an evaluation of any risk factors identified.
O2.4 Establish SLA and Contracts	SLA is established, reviewed, and approved by both parties. Where there is a contractual element this should be included in Contract documentation.
O2.5 SLA	SLA defines support services required, governance requirements, tools and procedural controls, resources, training requirements, escalation procedures, metrics, etc. (For further information on proposed SLA content, see Section 6.7.1 of this Guide).
O2.6 Put SLA Governance in Place	Governance organization is established. Roles and communications processes are defined in the SLA.
O2.7 Identify Required Training for User and Provider	Training needs are identified. Support and maintenance services providers should be competent to perform their required tasks. This includes GxP training where necessary (e.g., external providers).
O2.8 Develop any Required Procedures	SOPs required to control the support service are established by required parties. SOPs controlling interfaces between receiving and supplying organizations should be defined.
O2.9 Support SOPs	Required support SOPs are established, reviewed, and approved by relevant parties. Once in place these trigger training activities.
Training	Training in user organization or provider organization procedures or systems may be required. Training will be delivered by relevant party. Training records are established to document training.
O2.10 Deliver Scheduled and Ad Hoc Support Services in accordance with SLA	Scheduled and ad hoc support requests are processed and delivered in accordance with agreed procedures. These procedures are reflected in other operational processes, other support processes, and in related processes, such as validation.
O2.11 Support Records	Records documenting delivered support should be established. Records are determined by the type of support provided.

6.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O7 Repair Activity **O9 Backup** **O12 System Administration**	Other operational processes, relating to the specific service provided are invoked to control the service.
O2.12 Monitor SLA Metrics	User and Supplier organization report and review performance of user and supplier organization against agreed support metrics. Deviations are reviewed and risks mitigated in accordance with their priority.
O2.13 Performance Reports	Performance reports document actual performance against SLA metrics.
O3 Performance Monitoring	The operational process **O3 Performance Monitoring** is triggered once support services are delivered.
O2.14 Surveillance Audits	Audits are conducted periodically to ensure that agreed quality systems are being adhered to.
O2.15 Assessment Reports	Assessment Report is created and observations addressed, including those where no action is required.
O2.16 Are Performance Targets and Quality Requirements being met?	Where there is a deviation from performance targets or surveillance audits, deviations from stated standards are identified; action needs to be taken to address the problem. The Root Cause of the problem should be evaluated and relevant preventive and corrective actions taken to address the deviations, where possible.
O2.17 Can Corrective Action be taken?	Root Cause assessment will determine what actions can be taken to address deviations from agreed service levels or quality requirements. It may not be possible to address a problem or problems may be recurring. In such cases, it may be necessary to change the scope of the services provided or seek an alternative service provider (internal or external).
O2.18 Implement Corrective Actions	Corrective action is taken to address deviations from stated service levels and quality requirements. This may include changing service levels, implementing new processes and procedures, additional training, or changes in resources, etc.
O2.19 Does the SLA still meet Business Needs?	The defined support service may be meeting SLA performance requirement and quality requirements; however, business needs may have changed resulting in a change to the SLA or exit from the contract.
O2.20 Can the SLA be amended to reflect Business Need?	SLA is modified to reflect new business requirements. This may lead to changes in governance structure, service levels, SOPs, and training.
O2.21 Revise SLA	SLA is modified, reviewed, and approved to reflect revised services and service levels.
O2.22 Revised SLA	SLA is revised to reflect new business requirements.
O2.23 Manage Contract Exit	An alternative support provider may be required (internal or external) or a system may have been retired. Contract exit should be considered when establishing an SLA to ensure that full control can be regained of the support service. Documentation and record ownership should have been identified at the outset of the contract.

6.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O2.24 Process Review	From time to time, a review should be conducted to identify any lessons learned and any opportunities for improvement to the process for Establishing and Managing Support Services. This may be undertaken by the System Owner. This type of process review may be scheduled to fall in line with the review of SOPs for currency.

6.6 Procedural Guidelines and Considerations

6.6.1 Identify Support Needs

Process Owners and System Owners, with in-house support (SMEs), should determine the scope of required support services and identify potential suppliers.

6.6.2 Select Suitable Support Supplier

Process Owners and System Owners should consult with the Quality Unit to determine the need for Supplier Assessment. The need for assessment will be determined by a number of criteria, including:

- scope of services to be provided
- criticality of services to be provided (business and regulatory impact)
- previous history of the supplier
- use of own or supplier quality processes

If required, supplier evaluation should be conducted and documented in accordance with GAMP® 5 Appendix M2: Supplier Assessment (Reference 7, Appendix 4) or other in-house supplier assessment processes and procedures.

The output of the evaluation determines whether the supplier can be used, the adequacy of existing service management and delivery controls, and any additional controls that may be required.

For internal organizations, an assessment should be conducted to ensure that appropriate service management and delivery controls are established.

Where shortfalls are identified, these should be reported and a remediation plan established.

6.6.3 Establish Service Level Agreement and Support Contracts

SLAs should be established to define the scope of services to be provided, controls to be used, training needs, service performance metrics, and roles and responsibilities. For further information see Section 6.7.1 of this Guide. There may be a hierarchy in the provision of support, e.g., first level support is provided by local IT, second level support is provided by a global organization collecting solutions and managing supplier relations.

A Quality Unit should ensure that quality controls, such as training, GxP record keeping, documentation standards, and ongoing audit program are defined.

SLAs will be needed for each support organization.

Procurement and legal departments should be consulted when drawing up external SLAs and contracts.

For each support organization, service performance metrics and escalation procedures should be defined.

Interfaces between client and supplier organizations should be defined clearly, including:

- how services are accessed
- whether or how remote access is permitted
- how upgrades should be managed
- how file transfers are achieved

The definition of interfaces should include access to quality documentation and records, including SOPs, contact numbers, use of call logging systems, roles and responsibilities, etc.

A governance structure should be established for managing the provision of services. Governance considerations include:

Business Management

- ensuring Intellectual Property and critical data are identified and protected
- ensuring Non-Disclosure Agreements are in place, where necessary
- defining relevant laws, regulations, licensing agreements, and directives
- identifying policies and standards impacting support services

Contract Management

- establishing and monitoring conformance to contract and SLAs
- managing deviations
- scope change management

Quality Management

- surveillance audits for the quality of the service provision, monitoring quality controls
  (This is distinct from Performance Monitoring. See Chapter 7 of this Guide, which focuses on how the system itself is performing.)

Customer/Supplier Relationship Management

- effectiveness of client/supplier interfaces and governance structures
- adherence to commitments

6.6.4 Training

User organization and supplier organization personnel may need to be trained prior to commencing services. Training should consider:

- GxP requirements (GLP, GCP, GMP, GDP) as appropriate

- user and supplier procedures, (including system administration, handling back-end access, data ownership, and management)
- requirements of SLAs
- system and technical documentation
- security requirements (where necessary)
- any other relevant regulations, (e.g., data associated with personally identifiable information)

6.6.5 Standard Operating Procedures

SOPs may need to be developed to control the services being provided. Where there is an interface between user organization and supplier organization procedures, this should be addressed.

Procedures should be part of a user's and a supplier's quality management system. It should be clear which procedures are to be used.

6.6.6 Routine and Ad Hoc Support

Routine and ad hoc support should be provided in accordance with the agreed SLA and support procedures. All support activities (including any validation activities) should be documented using service reports, change control records, maintenance records, or other relevant records as defined by governing support service SOPs and SLA.

6.6.7 Service Performance Monitoring and Periodic Audits

Service performance should be monitored against agreed SLAs. Deviations from agreed SLAs should be evaluated and appropriate corrective actions taken. Where there is a quality impact from a deviation, relevant Incident and CAPA processes should be employed.

Periodic quality audits should be conducted (if deemed necessary by the scope and criticality of the services provided). Observations should be reviewed with the service provider and appropriate action taken to address an observation.

The root cause of any deviations from an SLA should be determined. Decisions regarding changes to service management and delivery controls, additional training, changes to metrics or in certain cases change of service provider may result.

6.7 Records and Record Content

6.7.1 Service Level Agreement Content Considerations

Content to be considered when developing SLAs includes:

- Scope:
  - system scope (what system is to be covered by the service)
  - service scope:
    - > system upgrades

> backup and restoration

> archiving and retrieval

> data maintenance

> disaster recovery

> fault feedback, fault diagnosis, and rectification (fault reporting, workarounds, patches, and service releases, etc.)

> documentation maintenance

> product updates

> maintenance spares and consumables

> routine testing and calibration

> system management and housekeeping

> handling of technical queries

> information security management

> security administration

> change management

> access for diagnostic purposes (e.g., remote login)

> ownership of off-line test facilities/tools/temporary licenses

> hardware repairs

> calibration

> software escrow

> database performance monitoring, database capacity monitoring (hard disk capacity), network (LAN and WAN) velocity, memory usage, etc. For further information, see Section 7 of this Guide.

- service performance targets (for in scope services):

> response and resolution times

• Governance:

- roles (as appropriate) with contact details (as necessary):

> Process Owner

> System Owner

> client QA

> supplier QA/QM

> service access points (e.g., service desk/call management)

> SMEs (e.g., Engineering, IT, etc.)

> service users

> contract manager

> service manager

> third parties

- Tools:
  - service desk
  - asset management
  - maintenance management
  - backup and restore
- Documentation and Records:
  - types of documents and records required:
    > system documentation to be kept up to date:
      -- requirements and design specifications
      -- test specifications
      -- operating and maintenance manuals
    > audit trail of tasks executed to the system:
      -- service requests and reports
      -- fault reports
      -- maintenance schedules and records
      -- calibration schedules and records
      -- change control/configuration records
    > service manual
    > service performance metrics

> training records

> archiving of documentation

- Ownership and responsibility for:
  - configuration management
  - document distribution management
  - documents and records during service provision
  - documents and records following contract exit
  - format of documents and records (electronic /paper)
  - document templates
  - retention periods for service/support records
- Resources:
  - client and supplier resource requirements:
    > management and supervision (on-site and remote)
    > service delivery, including hours of operation
    > contract management
    > service management
    > quality and security
    > physical resources
    > IT Infrastructure
    > storage
    > offices
- Escalation and Complaints:
  - dispute, resolution and arbitration procedures
  - escalation procedures
  - complaints procedures
- SOPs and Training:
  - What SOPs are needed to manage/deliver the support services within the user and supplier organizations?

- How do SOPs interface?
- What training is required to manage/deliver the services within the user and supplier organizations and how often?

• Service Management and Service Performance Monitoring:

- review meetings
- report requirements
- service performance metrics
- service performance incentives and penalties
- audit requirements
- onsite management and supervision requirements
- remote access requirements
- service continuity requirements

6.8 Scalability

The level of definition in the SLA and the complexity of the governance model may be scaled according to the scope, complexity, and impact of the services provided. The scalability of each support service is described in the relevant process section.

7 Performance Monitoring

7.1 Introduction

GAMP® 5 defines Performance Monitoring as "that part of overall preventive maintenance that obtains performance data that is useful in diagnosing system problems. It provides trends that may indicate performance problems, which can be used as part of CAPA to reduce application or system down time."

The purpose of monitoring performance is to enable the delivery of a consistent and timely service to system users; this aligns closely with ITIL®, which looks at Performance Monitoring as a sub-process of Performance Management in the context of the continuous improvement of Capacity Management (see Appendix 2).

Planning for Performance Monitoring may have commenced during the Project Phase (e.g., during specification and verification, which would incorporate the definition of critical process parameters).

This section is related to Appendix O3 of GAMP® 5(Reference 7, Appendix 4).

7.2 Scope

The scope of this guidance applies to business critical and GxP regulated automated systems.

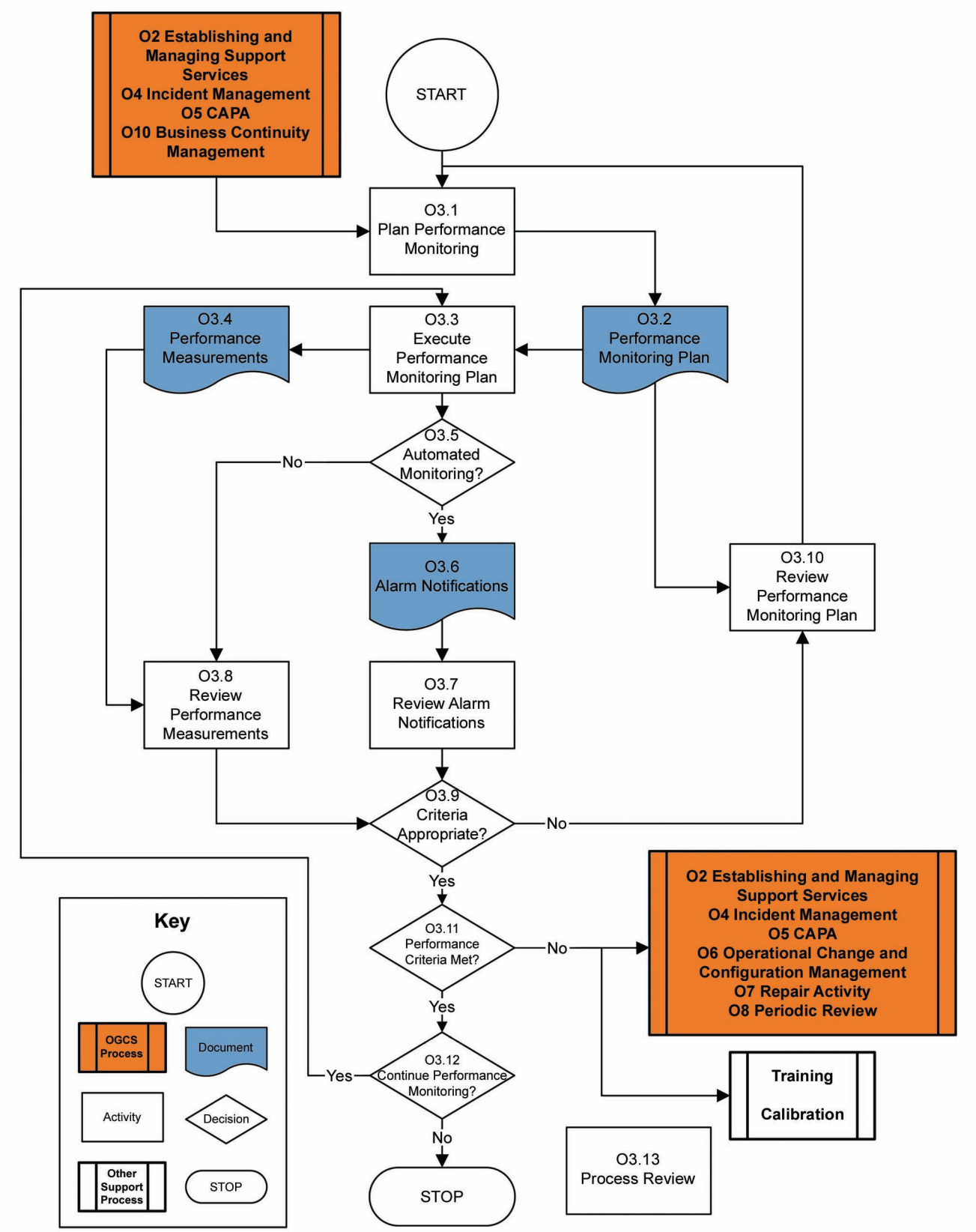
7.3 Roles and Responsibilities

Table 7.1 provides an indicative example. Organizations should allocate roles and responsibilities based on organizational structure and the specific system.

Table 7.1: Roles and Responsibilities for Performance Monitoring

Role	RACI Role	Responsibilities
Process Owner	I	• informed of issues with the computerized system highlighted by the performance monitoring process
System Owner	A	• accountable for the application of the Performance Monitoring Process as applied to system(s) under their ownership • accountable for analysis of performance metrics • accountable for the reporting of performance issues
Platform Support (SME)	R	• responsible for collection of performance metrics • responsible for responding to alarm signals
Application Support (SME)	R	• responsible for collection of performance metrics • responsible for responding to alarm signals
System Administrator (SME)	R	• responsible for collection of performance metrics • responsible for responding to alarm signals
Supplier	C	• consulted when establishing performance metrics • informed about performance metrics results in order to drive supplier CAPA processes
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

7.4 Performance Monitoring Process Flow Diagram



7.5 Process Narrative

Process Step/Decision/Record	Description
O3 Performance Monitoring	**An operational process which is part of overall preventative maintenance that obtains performance data that is useful in diagnosing system problems.**
O2 Establishing and Managing Support Services **O4 Incident Management** **O5 CAPA** **O10 Business Continuity Management**	Operational processes which may trigger **O3 Performance Monitoring**.
O3.1 Plan Performance Monitoring	Determine and document how **O3 Performance Monitoring** is to be conducted, which performance metrics are to be monitored, and how the metrics are to be interpreted to provide indications of process performance over time. The system or process parameters selected for measurement should be decided by assessing the potential risk to patient safety, product quality, or data integrity if the component fails or exhibits deteriorating performance. Risks to data integrity (reliability and authenticity) and availability also should be considered in relation to product quality or patient safety. The output is the Monitoring Plan. The performance requirements should have been defined in the Requirements Specification and should differentiate between GxP and non-GxP metrics. Performance monitoring may be triggered by **O2 Establishing and Managing Support Services, O4 Incident Management, O5 Corrective and Preventive Action,** and **O10 Business Continuity Management**.
O3.2 Performance Monitoring Plan	The Monitoring Plan is the agreed mechanism by which performance metrics will be gathered and processed. Where real-time warnings of performance deviation are required, the Monitoring Plan may be automated. For manual systems, the Monitoring Plan will detail a schedule of process performance reviews. This may be a separate document or part of a broader plan.
O3.3 Execute Performance Monitoring Plan	Depending on whether the monitoring process is automated, execution of the plan will either initiate automatic collection of performance metrics or schedule reviews of Performance Measurements in order to gather required metrics.
O3.4 Performance Measurements	Records of measured parameters can occur in many formats, depending upon the nature and frequency of measurement. Records vary from system generated logs of measured values to manual records maintained in control logs or equipment logbooks. Data can be the original observations or derived.
O3.5 Automated Monitoring?	If monitoring is automated, alarms are automatically triggered by the monitored parameter deviating from preset limits. If monitoring is not automated, then parameters are monitored manually.
O3.6 Alarm Notifications	Automated alarm notifications can take many forms, e.g., audible or visual alarms, message on system console, emails, text alerts, printed lists, or logs of alarm conditions.

7.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O3.7 Review Alarm Notifications	This activity reviews alarm notifications, i.e., all instances of deviations from preset limits. The purpose is to determine whether the alarm frequency is predictive of performance deterioration, and therefore, whether preset criteria are adequate for intended purpose based on practice.
O3.8 Review Performance Measurements	The purpose of the review is to summarize raw performance data to facilitate detection of trends in the data that may be useful in predicting process performance deterioration or process or service interruption.
O3.9 Criteria Appropriate?	Criteria should be sufficiently sensitive to process variability in order to be capable of providing an early warning of potential performance problems. Sensitivity should not be sufficiently high to yield a high level of false warnings.
O3.10 Review Performance Monitoring Plan	If the performance criteria are inadequate for purpose, e.g., insensitive to process or service deterioration or failure, the Performance Monitoring Plan should be reviewed in order to confirm purpose and suitability of performance metrics. The Performance and Monitoring Plan should be revised, as required.
O3.11 Performance Criteria Met?	If the performance metrics are fit for purpose and performance criteria are met, then the process or service is considered to be operating as intended. If the performance criteria are not met then depending upon then process affected external processes are triggered to manage a solution to resolve performance deterioration.
O2 Establishing and Managing Support Services **O4 Incident Management** **O5 CAPA** **O6 Operational Change and Configuration Management** **O7 Repair Activity** **O8 Periodic Review**	Operational processes that could be triggered by process step O3.11
Training **Calibration**	Other support processes that could be triggered by process step O3.11
O3.12 Continue Performance Monitoring?	Decision whether to continue with **O3 Performance Monitoring**. If no, the process stops. If **yes**, the process feeds back into step O3.3.
O3.13 Process Review	Reviews should be conducted to ensure that the process is operating as expected.

7.6 Procedural Guidelines and Considerations

7.6.1 Plan Performance Monitoring

The system or process component to be monitored will depend upon the purpose of the plan. Component examples include:

- specific applications and systems
- process parameters
- alarms
- instrumentation
- network infrastructure
- servers
- workstations and PCs
- control systems
- environment (e.g., temperature and humidity)
- logs/security/event histories

The system or process parameters selected for measurement should be determined by assessing the potential risk to patient safety, product quality, or data integrity should the component fail or exhibit deteriorating performance. Risks to data integrity (reliability and authenticity) and availability also should be considered in relation to product quality or patient safety and keeping the business running.

Examples of parameters that may be measured for automated systems include:

- specific applications and systems:
  - monitoring of application error messages
  - response times
  - download and upload times
  - number of users on the system
  - instrument failure and downtime
  - software failure
  - deviations from allowable range for critical process parameters
- network:
  - availability of components (e.g., server, router)

  - network load
  - broadcasts
  - class of traffic (FTP/HTTP/other communication protocols)
  - physical and logical security breaches (including attempted malicious attacks, e.g., from viruses, worms)
  - computer room temperature and humidity
- servers/workstations/PCs/control systems:
  - CPU utilization
  - cache utilization
  - interactive response time
  - number of transactions per time unit
  - average job waiting time
  - disk capacity
  - disk fragmentation
  - I/O load
  - system error messages
  - hardware status
  - existence of critical batch jobs
  - alarms (and over-ride histories)
  - physical and logical security breaches (including attempted malicious attacks, e.g., from viruses, worms)
  - printer report queues
  - scan rates and logging frequency

The frequency of measurement should reflect the criticality of the monitored process. Automated control systems operating in real-time or enterprise systems may require more automated monitoring than manual or departmental systems. Consideration should be given to the effect automated monitoring may have on the performance of the system.

Where real-time monitoring is required and the process is critical to product quality or patient safety, action or warning limits should be set to automatically signal a process deviation in order to trigger intervention.

Gathering performance data automatically can rapidly result in information overload; only key performance metrics and data useful for determining the root cause of performance deterioration should be collected routinely. Root cause projection analysis can be a useful strategy for determining which metrics should be gathered routinely. For alarmed parameters, only records related to out of specifications values may need to be retained (report by exception approach). The use of system logs for recording performance histories (data) can be useful in diagnosis of root causes.

For manual or Operational processes, it may not be feasible or desirable to set action or warning limits. Trends of measurements over time may be more useful as an indicator of changes in performance, e.g., consistent reduction in response time over time, increase in bandwidth usage over time.

Trends in performance metrics may be used to predict future constraints on service delivery.

Notification mechanisms should be appropriate to the urgency with which the alarm condition needs attention. An alarm raised as the result of an imminent failure of a critical process activity directly affecting product quality or business continuity may warrant immediate attention, as opposed to one arising from exceeding network loading limits.

Examples of notifications include:

- audible or visual alarms
- messages on system console
- warnings – approaching alarm state
- emails
- text alerts
- pager alerts
- printed lists or logs

Qualification of specific notification mechanisms may be appropriate where notification reliability is critical to maintaining product quality, patient safety, or other system uptime requirement driver.

Personnel receiving the alarm signals should have a clear understanding of their responsibilities.

Planning also should include the steps which should be taken in the event of receiving an alarm or warning signal to initiate restoring the process or component to acceptable performance.

External processes may include:

- repair/maintenance/calibration
- change control
- incident management
- CAPA

Monitoring mechanisms should not alter GxP records. If these mechanisms alter other application/system data, verification of this should be considered based on risk.

7.6.2 Periodic Review Considerations

For a specific system:

- Does a Performance Monitoring Plan exist?

- When was it last reviewed?
- Have the identified metrics been collected to the defined schedule?
- Have any trend analyses been conducted over the collected data?
- Did the analyses result in changes to the system or its supporting documentation and SOPs?
- Has performance of the system improved or at least remained constant since the last review?

7.7 Records and Record Content

7.7.1 The Monitoring Plan

The Monitoring Plan should assist the collection and interpretation of performance metrics. Performance metrics may be derived from recorded measurements or transaction logs.

A tabular format is recommended for ease of use.

The Monitoring Plan should identify:

- the system or process being monitored
- the parameters measured
- the frequency of measurement
- alarm, warning and action limits
- tool (automated systems) or process (inspection/review) used for monitoring
- notification mechanism
- person or system/process to notify
- operator intervention procedure
- where and how performance metrics are documented
- reference to in-house policy for retention time for performance metrics records

The Monitoring Plan also should reference how mechanisms and tools are controlled and managed, and any specification and verification activities required based on risk to patient safety, product quality, and data integrity.

Monitoring records may be stored in various formats. For automated systems, raw data and alarm/warning states usually are recorded automatically in system log files for inspection.

Where a system log file is not automatically maintained, a manual process (governed by an SOP) for recording the alarm conditions or other performance metrics should be employed.

Performance monitoring records may be within the scope of a Records Retention Policy and a risk assessment should be performed to determine the level of impact which the performance records have on decisions supporting patient safety, product quality, or data integrity.

7.8 Scalability

Factors for consideration:

- limiting monitoring to systems that have a high impact on product quality or patient safety as determined by the use of an appropriate risk assessment

8 Incident Management

8.1 Introduction

An incident is any unplanned occurrence which prevents (or may prevent) or delays users, the system, an operation, or a service from proceeding with an assigned task. (See also Appendix 2).

The process aims to categorize incidents to direct them to the most appropriate resource or complementary process to achieve a timely resolution.

This may result in an immediate local resolution. In other cases, incidents may need to be escalated for longer term corrective and preventive action. Therefore, there is a relationship between the incident management and CAPA processes.

Incidents and their resolutions usually are tracked using an incident log to monitor the performance of both the process and the automated system within which the incident occurred.

The process is intended to provide a high-level structure that will be supported by detailed SOPs, and associated tools, which give guidance on the escalation and evaluation scenarios.

This process may be supported by software tools.

This section is related to Appendix O4 of GAMP® 5 (Reference 7, Appendix 4).

8.2 Scope

The Incident Management process is intended to provide effective support for unexpected events to users of laboratory, process control, and IT systems.

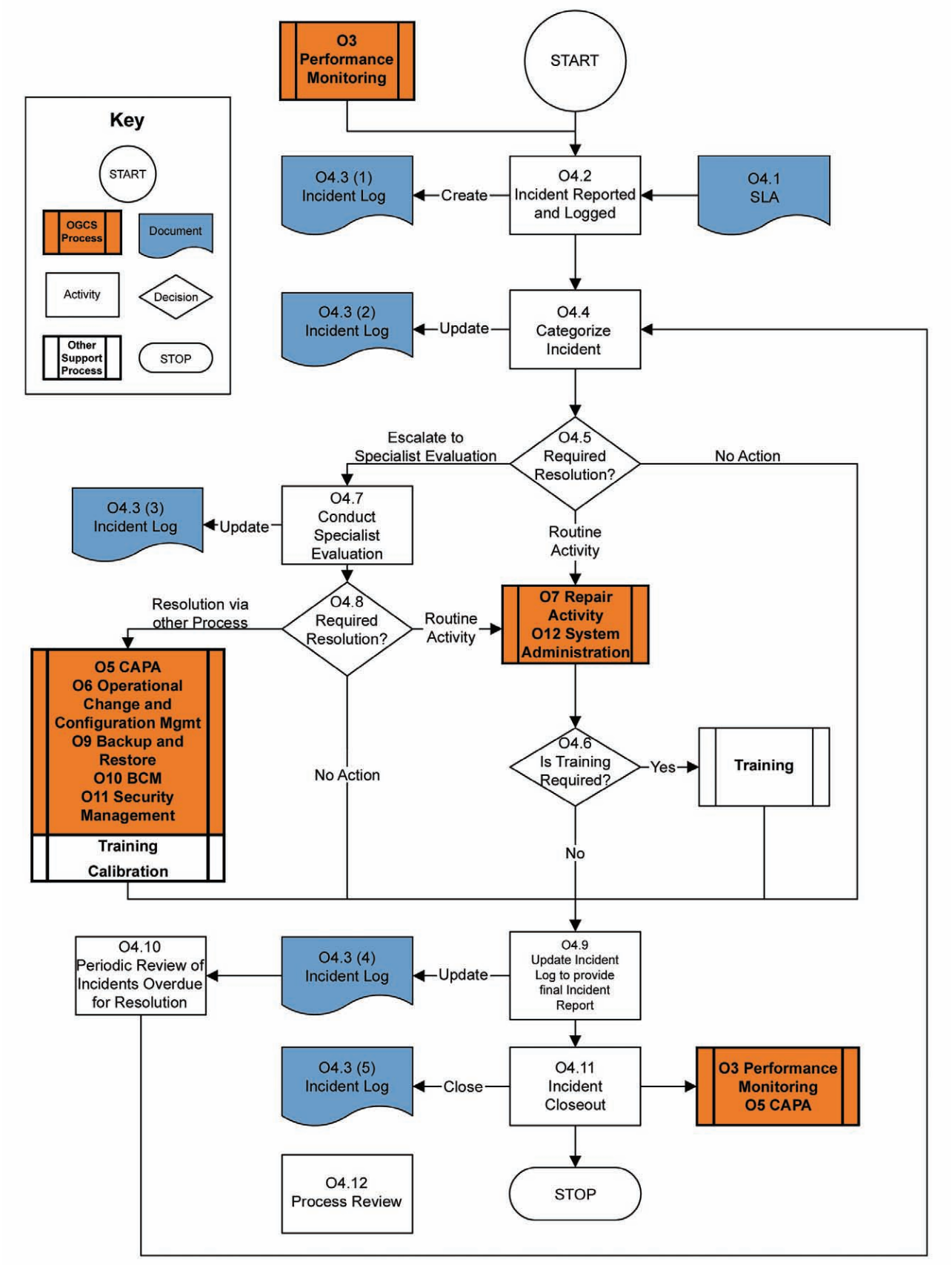
8.3 Roles and Responsibilities

Table 8.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 8.1: Roles and Responsibilities for Incident Management

Role	RACI Role	Responsibilities
Process Owner	C	• May need to be consulted when a resolution is proposed • Should be informed of incidents in accordance with defined escalation procedures • Should be informed of the status of incidents including metrics
System Owner	A	• Responsible for implementing and following the incident management process • Responsible for assignment of priority to incident resolution • Responsible for the timeliness of resolution • Should be involved in the decision to escalate or, as a minimum, inform the support personnel of the required timescale for resolution
End User	C	• Should notify service desk on detection of the incident • May be consulted or informed on status • Should be informed of implementation of resolution
System Administrator (SME)	R	• Can resolve simple issues under the System Administration SOP, e.g., reset locked account • May be involved in the decision to escalate to specialist evaluation
Quality Unit	C	• Should conduct audits to ensure the process is being followed and the relevant documents are generated • May be consulted when a resolution is proposed • May need to be consulted when other processes are triggered, e.g., Change Control, Restore Data
Application Support (SME)	R	• Responsible for following the incident management process • Will support the evaluation of the incident and assignment of priority • May be involved in the decision to escalate to specialist evaluation • Will make any approved changes or corrections to the system (together with others) • May include or involve the supplier
Platform Support (SME)	R	• Responsible for following the incident management process • Will support the evaluation of the incident and assignment of priority • May be involved in the decision to escalate to specialist evaluation • Will make any approved changes or corrections to the system (together with others) • May include or involve the supplier
Supplier	C	• May be consulted to assist the evaluation and resolution of an incident
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

8.4 Incident Management Process Flow Diagram



8.5 Process Narrative

Process Step/Decision/Record	Description
O4 Incident Management	**An operational process which categorizes incidents and directs them to the appropriate resource or complementary process to achieve a timely resolution.**
O3 Performance Monitoring	A potential input to trigger **O4 Incident Management**.
O4.1 SLA	SLAs may have an input with respect to the speed of response of service provision.
O4.2 Incident Reported and Logged	An incident is an unplanned occurrence which prevents (or may prevent) or delays users, the system, an operation, or a service from proceeding with an assigned task. A fault or incident report can be generated in several ways, e.g., via a '**Service Desk**'. For simplicity, this **Incident Management** process refers to the **Service Desk** as a generic method of logging and escalation although it is recognized that for less complex systems a simple log book may suffice. A procedure (outside the scope of this Guide) or SLA is required to govern the operation of the **Service Desk**, including out-of-hours cover. An incident typically is logged in the first instance by a **Service Desk**. The **Service Desk** should create an Incident Log entry and communicate the status to the originator.
O4.3 (1) Incident Log (Create)	Create an entry in the Incident Log. For further information, see Section 8.7 of this Guide.
O4.4 Categorize Incident	The incident should be evaluated and categorized (including an incident which is categorized as an emergency.)
O4.3 (2) Incident Log (Update)	The Incident Log should be updated with the results of the evaluation and categorization. (If the incident is categorized as an emergency this update may occur after action has been taken for resolution, but should be completed in a timely manner.)
O4.5 Required Resolution?	The incident, as documented in the Incident Log, should be subjected to an initial evaluation, which will result in one of the following courses of action: • **No Action** • **Resolution by Routine Activity** • **Escalate to Specialist Evaluation**
No Action	Move to Step O4.9 'Update Incident Log to provide final Incident Report'
Resolution by Routine Activity:	
O7 Repair Activity **O12 System Administration**	The **O12 System Administration** process may be invoked where the incident may be remedied or rectified by a simple direct action under the authority of the System Administration SOP. It also may include more 'Maintenance' oriented solutions, such as **O7 Repair Activity**.
O4.6 Is Training Required?	On completion of the administration or repair activity, the effect of the change or repair should be considered to determine whether training of users or support personnel is required.
Training	Where training is required, control passes to the Training SOP and Training Plan.

8.5 Process Narrative (continued)

Process Step/Decision/Record	Description
Escalate to Specialist Evaluation:	
O4.7 Conduct Specialist Evaluation	When escalation is required, a specialist evaluation will be required, conducted by an SME group of necessary disciplines to determine cause and resolution. For GxP-related incidents resolution, an action plan will be required, approved by the Quality Unit.
O4.8 Required Resolution?	The specialist evaluation will result in three possible courses of action: 1. **No Action** 2. **Routine Activity** 3. **Resolution via other Process** (could include a 'workaround' solution)
O4.3 (3) Incident Log (Update)	The Incident Log should be updated with the outcome of the specialist evaluation.
Resolution via Other Process:	
O5 CAPA **O6 Operational Change and Configuration Management** **O9 Back Up and Restore** **O10 Business Continuity Management** **O11 Security Management**	Resolution of the escalated incident may invoke other processes. **O4 Incident Management** has a strong inter-relationship with **O2 Establishing and Managing Support Services** process, since the efficient operation of the **O4 Incident Management** process relies heavily on the existence of well-written SLAs and support procedures, which are generated under this process.
Training **Calibration**	Resolution of the escalated incident may invoke any one or more support processes such as Training and Calibration.
O4.9 Update Incident Log to provide final Incident Report	The outcome of the completed incident process should be recorded in the Incident Log, or may be recorded in a separate document (Incident Report). It should contain information leading to a conclusion about the success of the resolution of the incident. Where No Action has been taken, the log also should be updated to record this decision, along with a justification reason.
O4.3 (4) Incident Log (Update)	Incident Log is updated.
O4.10 Periodic Review of Incidents Overdue for Resolution	Regular review (defined period) of incidents overdue for action to ensure each is addressed in a timely manner. Feeds back into O4.4.
O4.11 Incident Closeout	Incidents should be closed out. The closeout, usually by signature indicating that all required actions have been completed, should be recorded in an Incident Log.
O4.3 (5) Incident Log (Close)	The Incident Log is closed.
O3 Performance Monitoring **O5 CAPA**	A review of incidents to reveal problems or trends should be an input to **O3 Performance Monitoring** and **O5 CAPA**.
O4.12 Process Review	Reviews of the **O4 Incident Management** process and achievements against performance measures and customer expectations should be undertaken at a suitable frequency to ensure that the process remains under control. For further information, see Section 8.6.3 of this Guide.

8.6 Procedural Guidelines and Considerations

8.6.1 Procedure Considerations

A process or tool for reporting faults/incidents should be available. It should provide a method of logging the fault/incident and allow escalation and scalability depending on criticality of the system and severity of the fault/incident.

Communication: the level of communication to the original fault reporter (and other affected personnel) should be scaled according to the level of the incident, and the likely time to resolution.

Incidents can be categorized and should be pre-defined by an organization based on risk to patient safety, product quality, and data integrity. A standard categorization should be applied across systems. Example indicative categories include:

- Emergency – system stopped with impact on GxP or business critical process
- High – system availability and functionality affected, affecting on one or more users
- Low – system available and usable but performance or some non-critical functionality impaired

Incidents may be categorized based on type rather than priority, e.g.:

- Application
- Infrastructure

Procedural measures are different for the two categories. Measures typically will be system dedicated for application incidents and generic for infrastructure incidents.

- Organizations may choose to implement a categorization approach based on a combination of priority and incident types.

The incident should be evaluated and recorded, either as a discrete record or as part of an ongoing Incident Log form. The evaluation should determine what the impact of the incident was, what caused the incident, and how it is proposed to resolve the incident.

Possible courses of action following initial evaluation include:

- **No Action** – during the course of logging an incident, the incident reporter or an experienced user may correct the issue, or the incident may be a repeat of a previously reported incident that is already in the process of being resolved, which requires a cross reference to the previous incident record.
- **Routine Activity** – an incident may be remedied by the action of a Service Desk operator or evaluator if they have System Administrator rights under the authority of a System Administration SOP, e.g., resetting a user account, solving authorization and print problems, or a Repair Activity, such as like for like replacement of a component or re-calibration of an out-of-tolerance instrument. This feeds into one of the operational processes **O7 Repair Activity** or **O12 System Administration**, where such an action would be physically implemented, i.e., control passes to this other procedure for implementation. (SLAs may govern the provision of the repair activity.)
- **Escalate to Specialist Evaluation** – an incident may require re-assigning to a specialist group (SMEs) or department. Dedicated groups may cover particular applications or infrastructure, e.g., ERP, LIMS, AER or WAN, LAN, or email:

- Escalation to a specialist group involves determining, which group is most applicable. This relies on a clear definition of the problem by the User, and on clear definitions, available to the evaluator, of the responsibilities of each specialist group. If an escalated incident is routed to an inappropriate department, the receiving department is expected to correct the error by promptly re-routing the incident to the appropriate group.

Where escalation to Specialist Evaluation is required, possible outcomes include:

- No Action (as above)

- Routine Activity (as above)

- **Resolution via other process** – the incident requires complex action involving other processes and people, e.g., changes to an application, or intervention by a third party supplier. Processes may be governed by SLAs, which are controlled by **O2 Establishing and Managing Support Services**. (Examples of processes to which control may be passed are **O5 CAPA, O6 Operational Change and Configuration Management, O9 Backup and Restore, O10 Business Continuity Management, Training, Calibration**):

  - These processes may involve both an in-house support group and one or more layers of third party supplier. For example, an incident determined to be caused by a bug may be referred to the contract support provider for that application. In the event of a complex bug, the contract support provider may in turn need to refer the problem to the original coding house for the module in question.

  - In the event of **Disaster Recovery**, frequent status reports should be sent to the original User and to affected key users and sites.

  - An incident given the classification of 'Emergency' may result in emergency changes being made to the system. The 'emergency' route through the **Change Management** process may be used, e.g., the change may proceed without approval from the Change Review Board, and documentation may be generated retrospectively.

Is Training necessary? If an incident is triggered by user error, **Training** may be a solution. Alternatively, an incident may involve a change either to an application or an SOP, either of which would require training before implementation.

Incident Logs should be updated at significant points during the Incident Management process, e.g., at evaluation and categorization, at definition of resolution, at the point of hand-off of control to another supporting process, or on completion of implementation of the solution. The final report may be a separate document or a completed Incident Log entry and should include a conclusion about the success of the resolution.

Incident Close Out: the incident record should be closed only after other nested processes, (e.g., CAPA, Change Management) have been closed in the appropriate sequence. An incident may be set to a 'Holding' status, while the nested processes are executed. Alternatively, it may be possible to close an incident after hand-off to another process, provided cross-referencing between the two records is adequate.

- Where non-critical activities associated with an incident need to be completed, it may be permissible to close an incident, as long as there is an assured process for tracking these activities to completion. This may be preferable to leaving incidents open for extended periods. Electronic systems may manage this situation automatically.

- An incident can initiate CAPA or Change Control processes.

- If an incident initiates a Change Control process, it may be appropriate to close out the incident or assign a 'Holding' status. Resolution will be managed via the Change Control process. The Change Request should cross-reference the Incident Log number. On completion of the change, the incident record also should be closed.

8.6.2 Periodic Review of a System's Incidents Considerations

- Does the Incident Log exist?
- Is each Incident Log entry complete?
- Does the incident's Evaluation Record exist?
- Has the record been updated as the incident progressed through the process?
- Does the Incident Report exist?
- Have all related actions been completed?
- Was timely incident closure recorded in the Log?
- Are there any trends associated with the particular applications/systems?
- To what extent was the supplier involved?

8.6.3 Process Review Considerations

The choice of metrics should be considered, e.g., simply tracking the time taken from the initial incident through to incident closeout compared to the User's desired response time does not take into account differing complexities of resolutions. For example, the amount of work involved to reset a user account should not be compared to the amount of work involved for an external support provider to complete a software module change. A weighting factor on the target time to resolution may provide a solution.

The use of 'customer surveys' should be considered. These can be simple, e.g., selecting three incidents per month at random, and calling the User to ask:

- Did the Service Desk respond in a helpful, professional manner?
- Were you satisfied with the time it took to resolve the problem?
- Were you kept sufficiently informed of progress?
- Are you happy with the resolution provided?

If the user answers 'No' to any of these questions, then a more detailed investigation into the handling of the incident should be initiated. This may lead into the **O5 CAPA** process as an improvement suggestion for the **O4 Incident Management** process.

An analysis of the Root Cause categories for incidents should be undertaken to look for trends, which may give rise to possible improvement suggestions and corresponding preventive actions.

Monitoring of these metrics may be governed by a separate Process Review activity or may be included as part of the **O4 Incident Management** process itself.

8.7 Records and Record Content

Incident Logs and accompanying records should contain following information, as a minimum:

- unique reference number for the incident
- date and time of the incident
- user name and contact details
- date and time of initial incident report
- software application/infrastructure, environment, and module (or hardware type and failure mode)
- unique equipment or system ID and name
- description of incident
- incident priority (emergency, high priority, or low priority)
- user's desired response time (unless priority is emergency)
- name of the service desk operator who took the call, together with date and time
- evaluation of the incident including:
  - What was the impact of the incident on patient safety, product quality, data integrity, business?
  - What was the cause of the incident (may relate back to description of the incident)?
- a unique Incident Report Number (when a separate document is used)
- a description of the resolution and the processes applied (by SOP reference)
- reference to any supporting documentation, e.g., Change Request number, test protocol identifier
- a root cause category, e.g.:
  - system or application not working correctly:
    - integral to the system or application
    - external influence, e.g., data centre failure
- system or application working in accordance with documented requirements, but still not meeting the business or user needs
- training issue
- user access issues
- other
- related actions not yet completed, e.g., training on updated procedures, and a due date for their completion

- an audit trail of the actions taken and the persons involved
- conclusion about the success of the resolution
- closeout approval from at least an SME

8.8 Scalability

Incidents should be addressed according to the system's impact and severity of the incident. An **example** model is presented in Table 8.2. This example is intended to be illustrative only and not definitive.

Table 8.2: Scalability Model

<table>
<tr><td></td><td colspan="3">Incident Management (Incident Priority)</td></tr>
<tr><td></td><td>Emergency</td><td>High Priority</td><td>Low Priority</td></tr>
<tr><td>Low Impact System</td><td>No level of incident would be considered an Emergency</td><td colspan="2">Simple log of incidents and resolutions. Approval by SME(s) of resolution and implementations recommended.
Formal evaluation of the incident optional.</td></tr>
<tr><td>Urgency</td><td></td><td>LOW</td><td>VERY LOW</td></tr>
<tr><td>Medium Impact System</td><td colspan="3">Log entry should contain full details of the incident and proposed resolution. Formal evaluation of the incident is recommended. Approval by System Owner and Quality Unit of proposed resolutions and completion of actions required</td></tr>
<tr><td>Urgency</td><td>HIGH</td><td>MEDIUM</td><td>LOW</td></tr>
<tr><td>High Impact System</td><td colspan="3">Log entry should contain full details of the incident and proposed resolution. Formal evaluation of the incident is required. Approval by System Owner and Quality Unit of proposed resolutions and completion of actions required.</td></tr>
<tr><td>Urgency</td><td>VERY HIGH</td><td>VERY HIGH</td><td>HIGH</td></tr>
</table>

9 Corrective and Preventive Action

9.1 Introduction

The purpose of a Corrective and Preventive Action (CAPA) process is:

- to establish a means of capturing and tracking corrective and preventive actions for processes and systems
- to provide a tool to contribute to the assessment of the 'fitness for purpose' of processes and systems
- to prevent occurrence of potential failures and recurrence of actual failures/non-conformances
- to drive continuous improvement of processes

This section is related to Appendix O5 of GAMP® 5 (Reference 7, Appendix 4).

9.2 Scope

The CAPA process captures those incidents and failures escalated from the incident management and periodic review processes. These should be tracked from initial occurrence, through impact assessment to resolution and implementation of the correction, recognizing that the control of the resolution and implementation of the correction may be managed by other processes. The CAPA process also should accommodate the situation in which a failure needs both corrective action (to fix a failure) **and** additional preventive action (to avoid the failure occurring again). It also needs to capture instances where a potential failure is recognized so that they also may be tracked through impact assessment to the implementation of preventive actions with control via other processes.

In the context of this Guide, Problem Management (ITIL® terminology) may be included in the scope of CAPA.

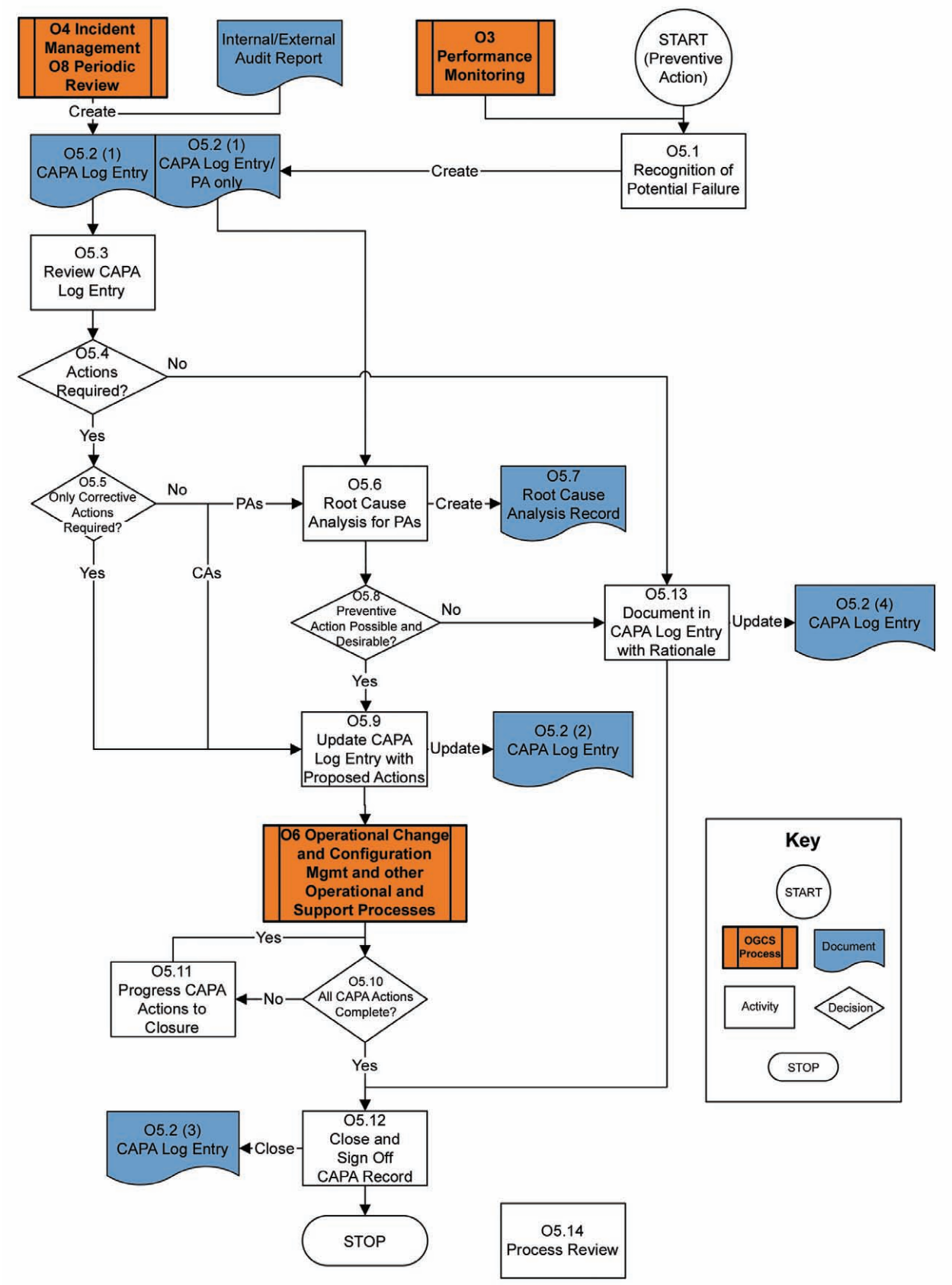
9.3 Roles and Responsibilities

Table 9.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 9.1: Roles and Responsibilities for Corrective and Preventive Action

Role	RACI Role	Responsibilities
Process Owner	R	• responsible for each allocated CAPA event, including: - approval of required action - implementation of action - approval of resolution • ensure that adequate and appropriate resources and support are provided to the resolution of each allocated CAPA event • may be responsible for logging CAPA events
System Owner	R	• responsible for each allocated CAPA event, including: - approval of required action - implementation of action - approval of resolution • ensure adequate and appropriate resources and support are provided to the resolution of each allocated CAPA event • may be responsible for logging CAPA events
Quality Unit	A	• accountable for the CAPA process and ensuring that it is maintained, and that those who interface with the CAPA system are trained in the principles of CAPA • responsible for reviewing CAPA records and ensuring that each instance is managed to resolution • act as regulatory compliance SME, as required • responsible for the approval of the resolution and closure of each CAPA event • may be responsible for logging CAPA events
Subject Matter Expert (SME)	R	• responsible for investigating the CAPA event, and developing, documenting, and implementing the resolution. A team of SMEs may be assigned to manage CAPA events. SMEs may be taken from the following disciplines: business process, engineering, IT, supplier, quality, validation. • may be responsible for logging CAPA events
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

9.4 Corrective and Preventive Action Process Flow Diagram



9.5 Process Narrative

Process Step/Decision/Record	Description
O5 Corrective and Preventive Action (CAPA)	**An operational process for investigating, understanding, and correcting discrepancies while attempting to prevent their reoccurrence, and for recognizing potential discrepancies to prevent their occurrence.**
Internal/External Audit Report	Internal or External Audit report findings may, following a risk assessment, initiate Corrective Actions.
O3 Performance Monitoring **O4 Incident Management** **O8 Periodic Review**	Outputs from these operational processes may be an input to **O5 CAPA** requiring a CAPA Log Entry to be initiated. Where performance criteria are not being met **O3 Performance Monitoring** may identify areas for improvement and initiate a CAPA Log Entry leading to proposed preventive actions. **O4 Incident Management** may generate an incident resolution proposal which requires the implementation of either preventive or corrective actions. Observations or non-conformances found during **O8 Periodic Review** also may lead to an input to **O5 CAPA**. Completion of any **O5 CAPA** actions also may require cross-referencing back to the process, which triggered the CAPA Log Entry in order to 'close the loop'.
O5.1 Recognition of Potential Failure (Preventive Action)	Employees should feel empowered to offer suggestions for process/system improvements or to report areas of potential failure. These should be formally documented and identified uniquely. Improvement suggestions are intended to relate to preventive actions; each will initiate a CAPA Log Entry.
O5.2 (1) CAPA Log Entry/PA only CAPA Log Entry (Create)	A corrective action or preventive action record in the CAPA Log. This can be recorded using a manual/paper system or an e-CAPA management system. If multiple corrective or preventive actions are identified, then consider whether this requires a single CAPA record or one for each action identified.
O5.3 Review CAPA Log Entry	The CAPA Log Entry should be reviewed by a team, which includes the Owner (Process and System), probably Quality Unit, IT, or Engineering. Suggestions raised at step O5.1 should be evaluated to determine whether there is scope for improvement, i.e., prevention of the potential failure. This may involve a risk assessment and evaluation or a root cause analysis. The evaluation should be documented. The decision whether to implement the preventive action will be based on the outcome of the evaluation. It may be helpful to assign a priority to the CAPA Log Entry based on the impact of the affected system and the criticality of the specific functionality involved, to allow a scalable approach to CAPA management. For further information, see Section 9.8 of this Guide.
O5.4 Actions Required?	The team determines if any actions are required. If no, proceed to O5.13 to update the CAPA Log Entry with the rationale. If 'Yes,' proceed to decision O5.5 to determine if it is only corrective actions that are required.

9.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O5.5 Only Corrective Actions Required?	A Corrective Action will fix the error. A Preventive Action will investigate the cause and implement a solution to prevent the same error occurring again, wherever possible. A team determines what actions are required. All Corrective Actions will proceed to O5.9 Update CAPA Log with Proposed Actions with Root Cause Analysis is conducted for preventive actions at O5.6 Root Cause Analysis for preventive actions. It may not be possible or desirable to try to correct an observation/issue, but there may be opportunity to improve the process to prevent the same situation occurring again.
O5.6 Root Cause Analysis for PAs	Use this process to investigate why/how the issue occurred. It will require a multidisciplinary team and should be documented, identifying the possible causes, and potential solutions.
O5.7 Root Cause Analysis Record	A formal record, uniquely identified, of the analysis (and evaluation) of the root causes of the issue. This record should be retained as part of the CAPA 'packet'. It should be signed by the System Owner.
O5.8 Preventive Action Possible and Desirable?	Determine whether the potential solutions identified in the Root Cause analysis (and evaluation) should be implemented.
O5.9 Update CAPA Log Entry with Proposed Actions	If corrective or preventive actions have been identified, the CAPA Log Entry should be updated to record the details of the proposed actions. Urgent corrective actions may need to be recorded in advance of the preventive actions to allow the resolution to be expedited. Where necessary, make cross–reference to the log ID to which control will be passed.
O5.2 (2) CAPA Log Entry (Update)	The CAPA Log Entry is updated with the proposed corrective and preventive actions. Approval of the proposed resolution should be added to the record.
O6 Operational Change and Configuration Management and Other Operational and Support Processes	Where corrective actions or preventive actions are required, one or more of these pre-defined processes will be initiated. They may run in parallel or with interdependencies. Where system or process changes are required, **O6 Operational Change and Configuration Management** is triggered. Once implemented, consideration should be given to including this changed aspect of the system in the **O3 Performance Monitoring** parameters as a means of determining the effectiveness of the solution.
O5.10 All CAPA Actions Complete?	Review the work done to date in response to the CAPA request to determine whether all avenues (using the pre-defined processes) have been executed/implemented and all documentation completed, signed, and filed.
O5.11 Progress CAPA Actions to Closure	Review the status of CAPA actions to identify those which have not been completed and progress any outstanding actions to completion and closure.
O5.12 Close and Sign off CAPA Record	Completion and sign off ensures that all actions and process steps have been completed, and where necessary, signed so that all corrective actions and preventive actions required are traceable from source to completion. This should include, where necessary, cross references to other evidential records, e.g., Change Management records.

9.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O5.2 (3) CAPA Log Entry (Close)	Approval for the closure of the CAPA Log Entry should be added to the record. Retain the completed CAPA Log Entry and any accompanying records for the prescribed retention period.
O5.13 Document in CAPA Log Entry with Rationale	Where it is determined that no corrective actions are required from step O5.4, the CAPA Log Entry should be updated with the rationale for the lack of corrective actions. (There may be preventive actions – see step O5.5) If no preventive actions are identified (following review at step O5.9), this should be recorded in the CAPA Log Entry along with an explanation for this outcome.
O5.2 (4) CAPA Log Entry (Update)	The CAPA Log Entry is updated. Approval of the proposed rationale for taking no action should be added to the record.
O5.14 Process Review	The CAPA Log should be reviewed periodically to ensure that all CAPA entries are progressed to resolution and closure. This may be undertaken by the same body of people who constitute the Change Review Board (see Section 6.2 of this Guide). Opportunities for improvement identified in these reviews may become inputs to **O5 CAPA**.

9.6 Procedural Guidelines and Considerations

A procedure should be established to address the process described above. It should include content describing the scope and applicability of the CAPA program and who is responsible, accountable, consulted, and informed about the activities included in the process. Additionally, consideration should be given to defining and documenting:

- How will the CAPA log be maintained?
- Is it:
  - Paper-based:
    - > Where is it kept?
    - > Who has access?
  - Database or Spreadsheet application:
    - > Is it adequately specified, verified, and controlled?
- How will cross referencing to other processes be achieved?
- Will any root cause analysis records be an integral part of the CAPA record or separate from it?
- Where an event has both Corrective and Preventive Actions will this be one CAPA Log Entry or more?

9.6.1 Periodic Review Considerations

- Does the CAPA Log exist?
- Does the Root Cause Analysis Record exist?
- Have the records been updated throughout the CAPA process?
- Have all related actions been completed?
- Was the CAPA record completion recorded in the CAPA Log?
- Was the CAPA process effective – has there been any reoccurrences of similar incidents, can improved performance be demonstrated?

9.6.2 Process Review Considerations

Monitor the activity and 'health' of the CAPA process (the number of CAPA incidents raised, in progress, completed etc) may be beneficial. CAPA metrics should be chosen carefully, as the integrity of the process may be affected by inappropriate measures, e.g., setting an objective to reduce the number of CAPA incidents may cause reduced reporting rather than improving performance.

9.7 Records and Record Content

The CAPA log and accompanying evidential record should contain the following information, as a minimum:

- Unique tracking number
- Name of system to which the CAPA is being applied
- Cross reference to Incident record ID
- Name of person making the CAPA entry and the date
- Description of the issue (that requires the CAPA action), i.e., what is wrong
- Whether it is a Corrective Action or a Preventive Action or both
- Reference to the record of the Root Cause Analysis (Preventive Actions)
- Description of the proposed resolution (including the benefits) or a rationale for why no corrective/preventive actions are required
- Name of the person to whom tracking the resolution has been assigned (i.e., owner of this CAPA entry; this may be different from the person reporting the issue)
- Approval of the proposed resolution or rationale for no action (e.g., by System Owner, SME(s), and Quality Unit)
- Cross references to other log entries to which control has been passed for execution of the resolution (e.g., Change Log ID where the Change Management process will be used to fix an issue)

- Description of what was implemented and when (e.g., new document version with its effectivity date, training plan ID, new/updated support service), unless recorded by another referenced operational process or other support process record. **Note:** Where other records have been generated to report these changes consistency with the CAPA log should be guaranteed.

- Evidence that the resolution was verified if resolution was managed within the CAPA process itself. (If resolution was handed off to another process, the verification should be included in those records.)

- Closure signature (by System Owner and Quality Unit) to agree that all proposed actions associated with this issue have been completed. Where resolution has been handed off to another process or other processes, it may be that the System Owner and Quality Unit need to approve and close the lower level process. When this is true, it may only be necessary for an SME to close the CAPA record.

9.8 Scalability

An example approach scalability is shown in Table 9.2. This example is intended to be illustrative only, and not definitive.

9.8.1 CAPA Priority

CAPA Log Records are reviewed and assigned a CAPA Priority of High, Medium, or Low according to the Table 9.2:

Table 9.2: Scalability of CAPA Priority

	CAPA Priority		
	High	**Medium**	**Low**
Low Impact System	No CAPA action will be assigned a High Priority	No CAPA action will be assigned a Medium Priority	All CAPA actions will be assigned a Low Priority
Medium Impact System	No CAPA action will be assigned a High Priority	Only critical functionality can be assigned Medium Priority	May be assigned to critical functionality or other functionality
High Impact System	Only critical functionality can be assigned High Priority	May be assigned to critical functionality or other functionality	No CAPA action will be assigned a Low Priority

However, where CAPA is triggered by an incident, the priority assigned to the CAPA actions should be the same as that applied to the incident.

The CAPA Priority is used to determine the rigor of supervision and control applied to the CAPA process for that CAPA Log Entry as shown in Table 9.3.

9.8.2 Rigor of Control

The rigor of the controls applied to the process is scaled based on CAPA Priority.

Table 9.3: Rigor of Control

	CAPA Controls
Low CAPA Priority	• Simple log of corrective action issues and resolutions • SME(s) review of resolution and implementation proposals recommended • Inclusion of preventive actions is optional • Use of Root Cause Analysis (or other tool) optional
Medium CAPA Priority	• CAPA Log should include both corrective actions and preventive actions • Use of Root Cause Analysis (or similar tool) recommended • System Owner and Quality Unit review proposed resolutions and completion of required actions
High CAPA Priority	• CAPA Log must include both corrective actions and preventive actions • Use of Root Cause Analysis (or similar tool) is required • System Owner and Quality Unit review and approve proposed resolutions and completion of required actions

10 Operational Change and Configuration Management

10.1 Introduction

Throughout the life of a system, changes may be required to adapt the system to a change of use, to meet new regulatory requirements, or to implement continuous improvements and 'bug-fixes,' etc. Change Management is fundamental to allowing a system to evolve, while maintaining control of that system. The operational change and configuration management process for a system should be linked to or be part of an overall site change management process.

A system is defined by its components, e.g., hardware, application software, operating software, infrastructure, any associated equipment or instruments, and by its technical and verification documentation. Collectively the status of these *configuration items* forms the *configuration* of the system.

The status and history of the configuration items may be contained in a controlled document, called either the Configuration Item List or the Configuration Status Account. This Guide uses the term 'Configuration Item List.'

Change Management is the process which controls the ongoing evolution of system components by ensuring that changes to components are recorded, evaluated, authorized, and managed (including personnel, training, and cultural aspects of implementing a change).

Configuration Management controls the coherence of important information and ensures that:

a. A system can be described in terms of the status of its configuration items in its current or in any desired prior state at any given point during the Operation Phase.

b. Important information, e.g., drawings, source and compiled code, specifications, is available to key personnel at latest revision with all previous versions clearly marked as superseded and archived appropriately.

Configuration Management is triggered by the Change Control process, where a change is proceeding and impacts on configuration items. Configuration Management also can be triggered by O4 Incident Management, O12 System Administration, and M9 Document Management (where affected documents are also configuration items).

This section is related to Appendix O6 of GAMP® 5 (Reference 7, Appendix 4).

10.2 Scope

This guidance applies to changes to any component of a system while in operational use or during system fault or error handling, such as:

- application software
- operating system software
- firmware, hardware
- infrastructure
- master and configuration data
- controlled documentation

- instrumentation

For those changes to the infrastructure with the potential to affect many systems, a prior review and recommendation process should have been performed, which may trigger a system-level impact assessment. Infrastructure change management is discussed in the GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Reference 8, Appendix 4).

Following a risk-based approach, some activities may be deemed out of scope of this guidance, e.g., 'like-for-like' replacements and operational/administrative activities such as user management, where O7 Repair Activity and O12 System Administration can be applied.

For significant changes, the impact assessment may initiate a new project; in which case the verification and validation approaches described in GAMP® 5 (Reference 7, Appendix 4) should be followed.

10.3 Roles and Responsibilities

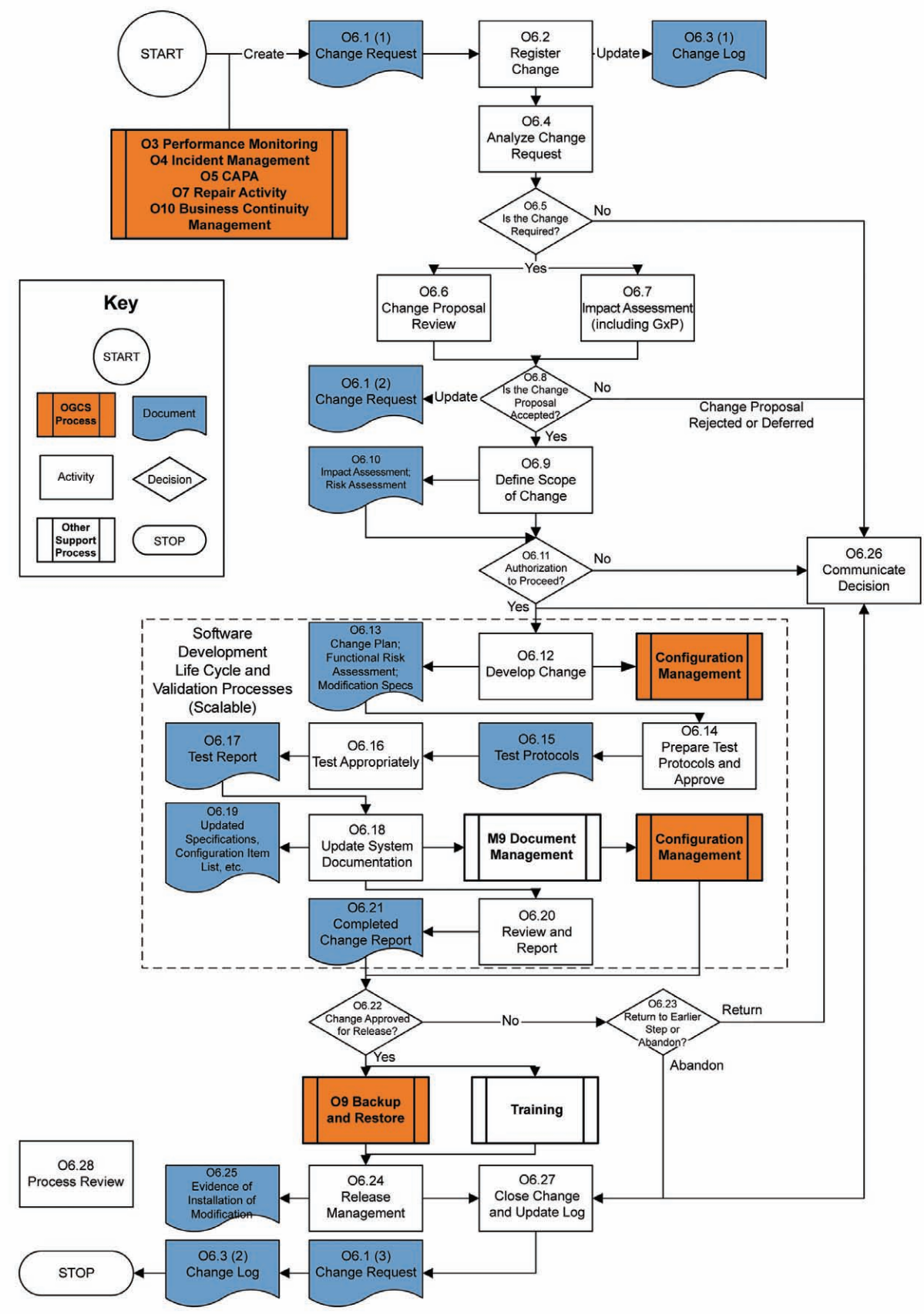
Table 10.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Note: only one role should be accountable for a process. In Table 10.1 two processes (Operational Change Management and Configuration Management) are covered; therefore, two roles have been designated as accountable – the Process Owner for the Operational Change Management process and the System Owner for the Configuration Management process.

Table 10.1: Roles and Responsibilities for Operational Change Management and Configuration Management

Role	RACI Role	Responsibilities
Process Owner	A	• owns the Operational Change Management process, and is accountable for its implementation • reviews and approves changes as appropriate
System Owner	A	• responsible for implementing the Operational Change Management process • owns the Configuration Management process and is accountable for its implementation • reviews and approves changes as appropriate
End User	I	• will be informed about proposed changes • may request changes • may need retraining after a change
Quality Unit	R	• will be consulted on proposed changes • reviews and approves changes as appropriate
Platform Support (SME)	R	• responsible for (as appropriate): - assessing change proposals - designing possible solutions - implementing approved solutions - verifying solutions • responsible for Configuration Management activities as appropriate
Application Support (SME)	R	• responsible for (as appropriate): - assessing change proposals - designing possible solutions - implementing approved solutions - verifying solutions • responsible for Configuration Management activities as appropriate
System Administrator (SME)	R	• will be informed of proposed changes • responsible for Configuration Management activities as appropriate
Supplier	C	• may need to be consulted on proposed changes • may act as SME and may provide product and documentation updates • may need to be informed during the Configuration Management process
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

10.4 Operational Change Management Process Flow Diagram



10.5 Operational Change Management Process Narrative

Process Step/Decision/Record	Description
O6 Operational Change and Configuration Management	**An operational process which ensures that changes to all system components are effectively managed and documented throughout the operational life of the system.**
O3 Performance Monitoring **O4 Incident Management** **O5 CAPA** **O7 Repair Activity** **O10 Business Continuity Management**	These Operational processes may lead to the generation of an operational change request. **Note:** the change request also may come from other sources, e.g., user suggestions, platform, or other hardware changes (security patches, technical updates, etc.). Other 'parent' changes within the **Change Management** System also may result in system changes as part of a larger Change Plan.
O6.1 (1) Change Request	The document containing the request/requirement for the change. The change request may be a paper or electronic document, and will be created by an individual recognized as competent to raise a change request. The format of the change request will be defined within the controlling procedure.
O6.2 Register Change	The change will be assigned a unique identification reference which will be entered onto a change log. This log may be maintained manually by a change coordination function or may be automatically generated within an electronic change management system. The basic process for operational **Change Management** should be defined and managed. It should be as simple as possible, i.e., the number of Handovers should be minimized. A software tool that allows electronic approvals can be beneficial.
O6.3 Change Log (1)	A register of all change requests for a given system or application.
O6.4 Analyze Change Request	Personnel competent to review the change request (e.g., the System Administrator/Change Manager in conjunction with the System Owner) should assess the change request to establish the nature and scope of the change if it should proceed and with what urgency or priority. Where appropriate, the technical impact of the change should be assessed to inform any subsequent change review and approval process. This decision will depend on the nature of the change requested and the scope of the change management system.
O6.5 Is the Change Required?	The outcome of this review is a decision as to whether or not the change is required, i.e., is the change beneficial and appropriate. If 'Yes,' the change proceeds to a more formal review. If 'No,' the originator of the change should be informed that the change has not been accepted and the rationale for this decision and the Change Log updated accordingly.

10.5 Operational Change Management Process Narrative (continued)

Process Step/Decision/Record	Description
O6.6 Change Proposal Review	The formal review of the proposed change should be reviewed by the 'stakeholders' of the change. A Change Review Board may be constituted from a number of different disciplines, e.g., the System Owner, Process Owner, Quality Unit, and relevant SMEs. The change may be reviewed at a regular meeting of the Change Review Board or by use of a 'workflow' for change review and approval within an electronic system. This review should consider the need for the change, the priority/urgency of the change, the viability of the proposed change, the high-level impact of the change, the cost/benefit ratio for the change. The change may be reviewed by representatives from the implementation Project team who are likely to have the required system and cross-functional knowledge to make informed decisions. In some organizations, the detailed scope of the change may be included in the review. For further information, see step O6.9.
O6.7 Impact Assessment (including GxP)	The potential impact of the change is evaluated. An assessment regarding whether the change has a GxP impact should be conducted to determine the workflow/levels of approval required after this point and the impact on existing validation documentation. Changes may be assigned as low, medium, or high impact. For further information, see Section 10.10 of this Guide.
O6.8 Is the Change Proposal Accepted?	Each system should have a designated Process Owner or Change Manager responsible for ensuring that all changes to the system are implemented in a controlled manner. Each Change Request raised should be reviewed for impact and its disposition (accept or reject) determined by management. A minimum of two people normally are required to accept or reject a change and for higher levels of GxP critical systems one of these should represent Quality Assurance. The outcome of this review is a decision regarding whether the change request is accepted or rejected – possibly for resubmission at a later stage. If the change proposal is accepted, the Change Request is updated at step O6.1 (2). If the change proposal is rejected or deferred, the requester of the change should be notified of the decision and the justification for the decision.
O6.1 (2) Change Request (Update)	The acceptance of the proposed change is recorded on the Change Request form.

10.5 Operational Change Management Process Narrative (continued)

Process Step/Decision/Record	Description
O6.9 Define Scope of Change	This step may be carried out by the Change Review Board or by the person responsible for the change or by SMEs. Consideration should be given to which configuration items may be impacted by the change. The output of this stage will be an impact or risk assessment document and a high level identification of the actions required to implement the change and to appropriately mitigate all identified impacts. This assessment may take place before the change is submitted to the Change Review Board. The benefit of this approach is that a detailed change proposal is available for review; the disadvantage is that if rejected, the SME resource required to carry out a detailed functional risk assessment may be wasted.
O6.10 Impact Assessment; Risk Assessment	The output from the 'Define Scope of change' activity – this should report the potential impact of the change on system components (e.g., data, personnel, platform, application software, other hardware, validation and qualification documentation, user documentation, or training). It is recommended that a standard form or checklist is used to ensure that all elements of the system are considered.
O6.11 Authorization to Proceed?	Following completion of the detailed assessment, a further review of the change documentation should occur before the change proceeds to the development stage. This should be performed by personnel with the technical competence to assess the change (e.g., peer reviewer), but also should involve approvals from other reviewers (e.g., Quality, Business and other SMEs) where appropriate. Although changes which have received Change Review Board endorsement normally would be expected to proceed there may be new issues, identified by the detailed impact assessment (e.g., technical feasibility, effect on other systems) which may prevent the change proceeding in the proposed form. If the change does not receive this authorization, the 'stakeholders' of the change should be identified and alternative solutions that will achieve a similar outcome also may need to be considered.

10.5 Operational Change Management Process Narrative (continued)

Process Step/Decision/Record	Description
O6.12 Develop Change	The change can move forward to be technically developed. This will require a detailed investigation into the requirements of the change in order that the necessary modifications to the system can be specified at the appropriate level of detail. GAMP® 5 categories of hardware and software should be part of the consideration, as well as the "novelty and complexity" of the change. To distinguish the new specification document from the initial validation documentation this is designated as a 'Modification Specification.' For a simple change, the change proposal form may contain sufficient details; for more complex changes, the modification specification may be within the change plan or may be a separate document. The scope of the change may affect several existing functions; therefore, a regression analysis should be performed at a functional level to establish the technical impact of the change and define the test plan. Other outputs from previous impact or risk assessments also should be considered to create a detailed implementation plan for the change. From this step until O6.20, the actions will be governed by a (pre-existing, Project Phase) process for software development life cycle. Updates to the original system documentation should be identified as part of the Change Plan; this is further discussed at step O6.18. This step will trigger the **Configuration Management** process.
Configuration Management	**Change Management** and **Configuration Management** are intertwined, as most of the changes that need to be managed in conjunction with a computer system are changes to the configuration. A well-defined process should be used, which emphasizes thorough and effective planning, management, and communication of changes. As the change is developed the effect on the components of the system should be considered. **Configuration Management** controls should be established and followed to ensure that the change is implemented correctly.
O6.13 Change Plan; Functional Risk Assessment; Modification Specifications	Outputs from the 'Develop Change' activity. These should include (as part of the Change Plan) a Backout Plan in case the change needs to be rolled back after implementation. Where appropriate, the need for training should be considered in the impact/risk assessment and be incorporated into the change plan.
O6.14 Prepare Test Protocols and Approve	All changes should be tested appropriately before implementation. Based on the 'modification specification' document, a detailed testing protocol should be developed. Where the change involves modification to code, there should be independence between the development of the change and the authoring and approval of the test specification. Decisions regarding scope, rigor, and location of testing should be technically justified, based on risk, and documented. Where appropriate, 'Regression testing' may be triggered to ensure that there are no unintentional consequences associated with the change. For further guidance, refer to Appendix D5 on Testing of Computerized Systems in GAMP® 5 and the GAMP® Good Practice Guide on Testing of GxP Systems (Reference 7, Appendix 4).

10.5 Operational Change Management Process Narrative (continued)

Process Step/Decision/Record	Description
O6.15 Test Protocols	Test Protocols should be subject to independent peer technical review and approval (prior to execution) and other reviews and approvals dependent upon the scope and nature of the change (for example all changes affecting a high impact GxP component should be reviewed and approved by a quality representative).
O6.16 Test Appropriately	The approved test protocols are executed and results are collected. If deviations are encountered during testing, these should be resolved and related evidence appended to the test results.
O6.17 Test Report	The output from the 'Test Appropriately' stage will be the executed test protocol with approval signatures from the tester and peer reviewer(s) as appropriate. For more complex changes, a Test Report may be produced.
O6.18 Update System Documentation	Once the change has been successfully tested, System Documentation should be updated as defined in the Change Plan. Any 'live' document within the Validation package may need to be updated. For commercial systems, all required documents should be updated by the Supplier before a change is released to customers. For internally developed systems, a risk-based approach may allow documents to be updated as part of a regular update after the change has been released.
O6.19 Updated Specifications, Configuration Item List, etc.	The output from the 'Update System Documentation' stage will be updated life cycle and qualification/validation documentation, as appropriate. It may not be practical to re-issue documentation for re-approval for every minor change. Organizations should take a risk-based approach, and where appropriate, indicate criteria (e.g., maximum interval/number of minor changes) between formal updates.
M9 Document Management	The change control process uses the predefined management process **M9 Document Management** to govern the updating of the system documentation. Where documents which are configuration items are changed, the **Configuration Management** process will be triggered.
Configuration Management	As the system documentation is updated the Configuration Item List should be updated and superseded documentation suitably archived.
O6.20 Review and Report	A review should be performed to ensure that all the elements of the Change Plan required in advance of the release of the change have been completed and that there are no outstanding unresolved issues or incomplete actions. Significant changes may require a separate report to summaries the results of the testing, minor changes may have the results reported as part of the change documentation.
O6.21 Completed Change Report	The output of the 'Report and Review' stage will be the completed Change Report.

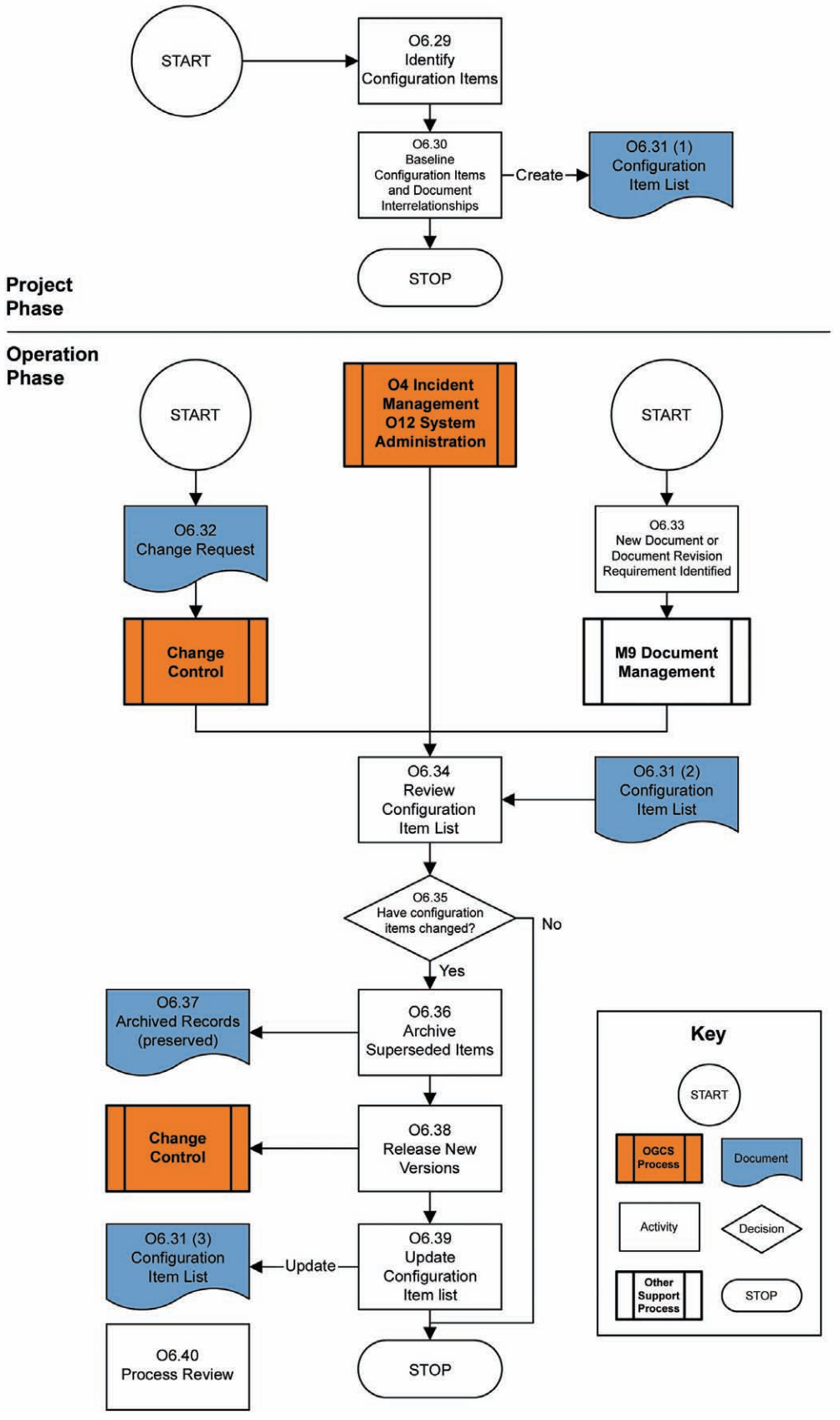
10.5 Operational Change Management Process Narrative (continued)

Process Step/Decision/Record	Description
O6.22 Change Approved for Release?	The Change Report should be passed to the Process Owner and the System Owner for final review and approval of the change. Where the change impacts GxP, the Quality Unit should be included in the approval. **Note:** for medical devices, FDA 21 CFR Part 820 (Reference 1, Appendix 4) has a more formal requirement: "Each manufacturer should establish and maintain procedures for the identification, documentation, validation or where appropriate verification, review, and approval of design changes before their implementation."
O6.23 Return to Earlier Step or Abandon	In the event the change is not approved for release, analyze the reason for rejection. It may be that further testing and documentation is required or the decision may be taken to back out the change. If the change is abandoned, communicate the decision, take out or reverse any actions carried out, conduct testing where required, close the change and update the change log.
O9 Backup and Restore	Backup is the operational process of copying records, data, and software to protect against loss of integrity or availability of the original. Restore is the subsequent restoration of records, data, or software to their original configuration when required.
Training	**Training** will be required if the change introduces new functionality, significantly affects the use of the system, or how the system is technically administered. Procedures or work instructions may need to be updated, training materials prepared, and training sessions delivered. It may be beneficial if the system has an separate 'training instance' where instruction can be given and familiarity with the change can be gained in advance of implementing the change into the production environment. Otherwise, training may need to be delivered immediately after the change has been made live.
O6.24 Release Management	The change can now be implemented. For internally developed systems, this means that the change can be applied to the production environment by an appropriate installation verification process. Commercial systems also will require a formal Release Management process to distribute the new release and support materials to customers (For further information, see Section 10.8.4 of this Guide).
O6.25 Evidence of Installation of Modification	Evidence that the change has been successfully installed should be collected.
O6.26 Communicate Decision	In the event that a change proposal is rejected or deferred or authorization to proceed withheld, the decision and its justification should be communicated to the change originator.

10.5 Operational Change Management Process Narrative (continued)

Process Step/Decision/Record	Description
O6.27 Close Change and Update Log	If there are non-critical activities to be completed associated with the change, it may be permissible to close the change as long as there is an assured process for tracking these activities to completion elsewhere. This may be preferable to leaving changes in an incomplete status for extended periods. Electronic systems may manage this situation automatically. For further information on change closure, see Section 10.8.5 of this Guide.
O6.1 (3) Change Request	Change Request is closed.
O6.3 (2) Change Log	Closure of the Change Request should be recorded in the change log.
O6.28 Process Review	A process to detect overdue changes is required as an integral part of the process. Timeliness can be defined in multiple ways, e.g., by defining change urgency/criticality levels with associated target action timelines or by agreeing on proposed/negotiated change implementation dates etc. The Change Review Board should review Change Logs to ensure that they are closed out on completion of the change. Where appropriate, a post implementation review of changes also may be performed.

10.6 Configuration Management Process Flow Diagram



10.7 Configuration Management Process Narrative

Project Phase (not in scope of operation phase, but an essential precursor to it)	
Process Step/Decision/Record	**Description**
O6.29 Identify Configuration Items	**Configuration Management** is the process by which the coherence of important information within a project is controlled. The information should not be placed under configuration control until it is at an appropriate level of maturity, as the process of **Configuration Management** brings with it complexity, time impacts, and extra work. Configuration Management tools are available which can support the Configuration Management process and maintain Configuration Item Lists automatically.
O6.30 Baseline Configuration Items and Document Interrelationships	Having identified the items that need to be placed under **Configuration Management**, these items should be baselined at key points in the project. A comprehensive baseline should be established prior to the **O1 Handover** process where the system moves from the Project Phase into the Operation Phase.
O6.31 (1) Configuration Item List	The Configuration Item List should contain sufficient level of detail that, in the event of a disaster, the system could be re-constituted from the information contained within the account, and for documentation and software, from secure copies of the Configuration Items (these may be secure master copies or back-up copies as mandated by the **O9 Back-Up and Restore** process).
Operation Phase	
Process Step/Decision/Record	**Description**
O6.32 Change Request	A paper or electronic document, created by an individual recognized as competent to raise such a request, and containing the request/requirement for the change.
Change Control	The **Change Control** process feeds into the **Configuration Management** process at the point where the change is developed, and again at the point where the system documentation is updated to reflect the change.
O4 Incident Management **O12 System Administration**	**O4 Incident Management** and **O12 System Administration** processes may trigger **Configuration Management**.
O6.33 New Document or Document Revision Requirement Identified	During the operational life of a system, a requirement may arise to either revise an existing document, e.g., to reflect a new way of working or to create a new document.
M9 Document Management	The **Document Management** process will control the creation or revision of a document, up to and including the approval and issue of the document.
O6.31 (2) Configuration Item List	The current version of the Configuration Item List.
O6.34 Review Configuration Item List	The current version of the Configuration Item List is used to evaluate whether the changed items are Configuration Items. (An example of this would be the Access Control List, which is not a Configuration Item, and is managed under a different process e.g., the Security Management SOP for the system.)

10.7 Configuration Management Process Narrative (continued)

Operation Phase	
Process Step/Decision/Record	**Description**
O6.35 Have Configuration Items Changed?	If any configuration items in scope are changed, then further **Configuration Management** activities are triggered. If no configuration items in scope are changed, then **Configuration Management** is not required and the process ends without further expenditure of effort. This does not necessarily end or otherwise impact the **Change Managemen**t and/or **Document Management** processes which lead in to this process. The implementation of the change also may create new Configuration Items which also should be considered.
O6.36 Archive Superseded Items	The output from either the **Change Control** process or the **Document Management** process is an updated system element. If the element is a Configuration Item, the previous version becomes superseded. The superseded item should be clearly and indelibly identified as superseded. Where appropriate, the prior version should be and archived securely under the **Archiving** process. This applies mainly to documentation and software elements, as it is not normally necessary to archive defunct hardware. Consideration should be given to establishing a formal software library (similar to the Definitive Software Library in ITIL®). There may be specific issues to address when archiving software components, e.g., if source code is archived, a relevant compiler also should be archived.
O6.37 Archived Records (Preserved)	The superseded items become preserved data.
O6.38 Release New Versions	New versions of the configuration items are released.
Change Control	The **Configuration Management** process hands over to the **Change Control** process as the new versions of components are released – see step O6.22. The Configuration Item List may include a distribution list for some Configuration Item. This list should be used to ensure that new versions are distributed to relevant parties or areas.
O6.39 Update Configuration Item List	After the installation of the changed item into the production (effective) environment, the final step in the process is to update the Configuration Item List, showing: • the new Issue or Version of the item • the date of issue or release • a reference to the Change Request or document generation process
O6.31 (3) Configuration Item List (Update)	The updated Configuration Item List becomes the current version, but the previous information from the last version of the account must not have been lost to guard against the eventuality that it may become necessary to 'roll-back' the system to a previous version.

10.7 Configuration Management Process Narrative (continued)

	Operation Phase
Process Step/Decision/Record	**Description**
O6.40 Process Review	As part of the process review activity, the System Owner should review the Configuration Item List periodically to confirm that: • the List is current and up-to-date • the List is stored securely and is readily accessible • any referenced Change Requests can be matched to a Change Log entry • the List is subject to version control (and only the latest issue is available for distribution)

10.8 Procedural Guidelines and Considerations

10.8.1 Types of Changes

Organizations should define when in a system life cycle that the transition from project change control to operational change control should be made. Defining this transition point can be complicated (e.g., during the phased Handover of a system) and needs to consider the possible return of an operational system (i.e., after acceptance and release) to a project development life cycle for a major change.

Significant changes should be reviewed, impact and risk assessed, authorized, documented, tested, and approved before implementation. However, the following changes may be exempted or handled by other processes:

Like-for-like Replacements: this type of change applies to equipment and instruments and also to the infrastructure components included in the computerized system. Such changes can be controlled by suitable standard maintenance procedures.

Like-for-like changes may not be easy to assess and careful consideration should be given to their impact. For example, individual PLC input cards could look quite different physically, but be identical in operation. Alternatively, components that appear to be “100%” identical may require updated/new drivers. SME input should be obtained and where there is doubt, a change control should be raised. See also **O7 Repair Activity**.

Standard Changes: where there are controlling procedures and responsible personnel to implement the changes, these may be managed by System Administration function, discussed in O12.

Emergency Changes: these changes should be subsequently reviewed, tested, documented, and approved in a timely fashion according to the appropriate procedure. The same process steps should be followed, but they may not happen in the usual order. What constitutes an emergency change should be clearly defined. This route may be triggered by **O4 Incident Management**, depending on the level of escalation of the incident.

For high impact systems, involvement and prior approval of the change by the Quality Unit should take place wherever this is practical and no personnel are in danger.

A major risk related to handling emergency changes is that documentation of actual events and associated activities is not created for subsequent review. The emergency change process should include provisions to ensure that the changes are thoroughly documented within a reasonable time frame.

Where appropriate, the process for emergency changes also should include a detailed communication plan to operators to notify that a change is implemented without testing and that additional checking/verification of system outputs may be required.

Changes should not be allowed to escalate to emergency status through the accumulation of internal failures or delays.

Temporary Changes: these are changes which are planned to be in place for a 'limited' period (as defined by the user organization). Temporary changes should be documented to make them clearly visible to personnel who need to know they remain. Particular attention should be given to the reversal of temporary changes to ensure that they are 'rolled back' and properly reviewed through the formal change management process before being made permanent.

Global Changes: for additional information related to managing change in globally implemented computerized systems, see the GAMP® Good Practice Guide: Global Information System Control and Compliance (Reference 7, Appendix 4).

10.8.2 Change Management Systems

Changes should be recorded in a single change management system. An automated comprehensive enterprise change management system capable of managing all change records (logs and supporting documentation) is beneficial, as local and global application and infrastructure teams can then use the same tools and search the same data. An additional benefit is that records management is substantially easier. Organizations may not have access to such tools; therefore, change records may be held in various 'fragmented' systems and media.

If an electronic change management system is to be used, consideration should be given to the level of validation required to ensure that there are sufficient controls established to demonstrate its effective use and operation.

10.8.3 Reviewing Changes

A change is reviewed in the first instance by competent personnel, such as a System SME. Consideration should be given to the need, justification, and priority for the change, the scope and potential risk of the change, the completeness of the change request, the viability of the change, criteria for implementation (e.g., service window or upgrade), the cost/benefit of the change, and the possibility that the same change has been requested previously.

If the change is accepted at the first line review, it can be submitted to the Change Review Board. The Change Review Board exists to review changes and return an 'accept' or 'reject' verdict. The Change Review Board should have documented:

- the scope and purpose of the change review board
- roles and responsibilities
- processes for the impact assessment (product and business) and disposition of submitted changes
- frequency of meetings
- appointment of deputies, etc.

When change proposals are reviewed by the Change Review Board, their decisions should be documented.

10.8.4 Release Management

The process for executing a change should adhere to the formal release management practices of the organization. Changes may be released to users in different ways:

- **Delta release:** execution of a single change in the production environment. Full documentation accompanies the delta release.

- **Emergency release:** correction to a small number of known problems. Release is often in advance of documentation delivery; otherwise similar to delta.

- **Full release:** multiple changes are built, tested, and distributed together. Regression testing is part of the process. Version upgrades are an example of a full release.

- **Package release:** at least two releases (delta or full) in combination. Multiple version upgrades are an example.

Generally, a release strategy for a given change is based on urgency and timing. Cost also should be considered, as full or package releases are considered to be more efficient and more compliant with regulatory expectations, as documentation and testing usually are better than for changes that have been implemented gradually.

Communication is considered an important part of change execution. Groups implementing a change should communicate what was done and how operation of a computer system will be affected to all affected sites. 'Suspension of service' and 'return to service' should be included in a communication plan.

Global Systems Release management may require specific elements of planning which potentially will have broad ramifications. Rollout may not be preformed simultaneously at all sites; the impact on the need and the ability to share data between sites should be evaluated. Communication plans should inform users of the impact and schedule for major changes. Sites need to be made aware of requirements for installation of changes.

It may be difficult to find a time to shut a system down to execute the change that does not negatively impact business users somewhere, especially if the system is global. For distributed systems, it may be possible to replicate the change (or otherwise execute it) on various instances at less intrusive times. For systems that may replicate back to a centralized database; however, this may cause difficulties if the change includes alteration of the database architecture.

These issues should be considered, documented, and addressed during planning of the change execution process.

Documentation efforts should accommodate expectations of the sites.

For further information, refer to the GAMP® Good Practice Guide: Global Information Systems Control and Compliance (Reference 7, Appendix 4).

Where a rollback is executed, it should be approached methodically, and some testing should be performed to verify that the rollback worked as expected. The verification/test process for the rollback may require user participation.

10.8.5 Change Close Out

When a change has been implemented and a system returned to service, change documentation should be closed out. Organizations should ensure that all tasks are complete. Tasks which may be incomplete include:

- updating specification documents (URS, FS, SDS, or System Description) affected by the change

- obtaining required sign-offs

- ensuring retention of change documentation (including test results)

- Closure of change requests as 'implemented' or 'not implemented'. Closure of an 'implemented' change request may present difficulties, e.g., if the change implementation requires a long time to complete for multiple instances. Change requests that are not executed should be closed out.

- final updating of the change log

The change procedure should define clearly that all parts of the process should be completed, and internal controls, such as audits, should be used as confirmation. If an automated change tool is used, organizations should consider automated alert notices for changes that have not been closed and are past their scheduled implementation dates.

10.8.6 Configuration Management

At the start of the project, elements of a system under development which should be Configuration Items should be identified; examples include:

- specification documentation, e.g., URS, FS, HDS, SDS
- application software, e.g., source code, executable, configuration files, service packs
- other software, e.g., drivers, operating systems
- application specific firmware
- hardware, e.g., PLCs, PCs, servers, communication interfaces
- manuals, e.g., operating instructions, maintenance manuals
- databases
- security patches
- other patches (e.g., bug fixes)

Configuration Items should be established at a level of detail appropriate to the effective management and control of a system and its components.

For documentation under Configuration Management, a Distribution List (i.e., personnel who hold the controlled copy which should be updated) should be maintained.

Typically, Process Control Systems (DCS, PLC, or SCADA) have a large number and variety of system components; the Configuration Item List for such also may include:

- modules, e.g., phase modules, equipment modules
- version of HMI utilities
- PLC – make, model, additional interface modules, etc.
- PLC code e.g., ladder logic
- version of PLC programming environment
- version of utilities for run-time setup or configuration of systems (variable speed drive controllers, flow-meters, etc.)
- piping and instrumentation diagram
- operating instructions
- maintenance instructions

- valves
- instruments
- pumps, filters, heat exchangers (depending on type of process)
- detailed mechanical drawings
- electrical schematic and layout drawing
- general assembly drawing
- component data sheets
- static data (e.g., process parameters and settings)

For some DCSs, there is no way of utilizing a version number for some configuration changes. In some cases, this can be managed only using the built-in change management system (e.g., VCat in Delta V).

For PLC systems, this should be implemented by using manually inserted version numbers embedded in the code, such that it resides in the controller. This also makes the data available to be read remotely on a SCADA HMI, which should be verified as part of a change control release.

The **Configuration Management** process may be different for IT infrastructure components. In a modern IT environment with shared infrastructures, a simple Configuration Item list may not be capable of showing all the relationships between various system components. A Configuration Management System approach as suggested by ITIL® is a potential solution.

10.8.7 Configuration Item List and Configuration Status Accounting

Consideration should be given to the relationships between different Configuration Items. If traceability or documentation matrices have been generated, these should provide a clear representation of the interrelationships between the requirements, design specifications, and protocols. Other relationships also should be considered and documented as appropriate.

The method used to maintain a Configuration Item List and where it is stored should consider:

- an organization's procedures and policies
- the complexity of a system, i.e., a typed list may be sufficient for a simple system, but insufficient for a complex DCS
- the accessibility for key users
- the security of storage required

A risk-based approach should be used to determine the level of detail recorded for each component. For example, does a component need to be documented using just the model or version number or by a unique identification number, e.g., a serial number? This level of accounting can be extremely resource intensive and may prevent a like-for-like replacement during repair.

The use of Configuration Management tools should be considered for managing records, establishing a baseline, and maintaining the Configuration Item List.

10.8.8 Process Review Consideration

10.8.8.1 Operational Change Management

The Operational Change Management process should be reviewed by the Change Management Process Owner to ensure that it is being followed correctly. Items for review may include:

- Does a Change Log exist?
- Is the Change Log a complete and up-to-date listing of all change requests related to the system?
- Are impact/risk assessments completed as part of the change control process?
- Does the output from the risk assessment determine the activities that are required to implement the change?
- Has a change plan been developed to implement the change?
- Has a functional risk assessment been performed to determine the technical scope of the change?
- Is a document specifying the modifications to be made to the system available?
- Are the executed test protocols available for inspection and have they been executed according to good testing practice?
- Have the executed protocols been signed off before the change is made live?
- Are life cycle documents updated as changes are applied?
- Are changes reviewed once testing is complete and before implementation?
- Is adequate and appropriate evidence of the successful installation of system modifications collected?
- Are closed changes recorded as such in the Change Log?
- Have any exceptions been found during the routine reviews of the Change Logs?

10.8.8.2 Configuration Management

The Configuration Management process should be reviewed by the System Owner to ensure that it is being followed correctly. This would typically involve:

- review of the Configuration Item List against the current system
- identification of updated items in the system and retrieval and verification of change-related documentation

10.9 Records and Record Content

10.9.1 Change Logs

Information contained in a change log should include, e.g.:

- unique equipment or system ID

- unique identification reference for the change
- date change request received
- current software version
- person who raised the change request
- the current status of the change
- references to any associated changes

10.9.2 Change Management Records

The minimum content of change records (change requests) should include:

- unique equipment or system ID
- identity of the requester
- relationship to other changes
- details of the impact assessment
- impact (minor/significant/major)
- test strategy (based on risk and impact)
- priority (low/medium/high/urgent)
- change plan (not always necessary for minor changes, based on risk)
- approval to execute change
- status: proposed, scheduled, executed, cancelled, completed
- date (and time where relevant) that the change was implemented
- follow up tasks completed, e.g., documentation, post-execution monitoring if required
- closure of the change record
- for dedicated lines: batch/lot number, name, etc., of the first product(s) released with the change implemented (this information should support subsequent complaints tracking)

Change records should be available to personnel who are troubleshooting a problem to both Process and System Owners and to the Quality Unit in case of regulatory audit. The records may have to be available to personnel at different sites. Paper-based systems are considered an inefficient solution for maintaining change records.

Responsibility and accountability should be assigned. Process Owners have ultimate responsibility for change records, but may delegate this, e.g., to the owner of a change control tool.

Quality Units should audit change control records. Change control records may be audited by regulators and local System Owners should understand the communication channels which allow rapid access to change control records.

The length of time for which change control records should be retained may be determined from a combination of regulatory and business considerations. A risk-based approach to record retention may help to minimize archive and retrieval costs.

10.9.3 Change Plan

A detailed Change Plan may be appropriate for guiding a change process and should include:

- Roles, responsibilities, and key resources required to complete a change – who needs to supply what (e.g., software, hardware, documents, test environments, simulations, configuration tools, test tools licenses, sample data, and access accounts?
- a timescale with key milestones identified
- validation documents and specifications to be updated
- tests to be conducted
- method of making and verifying a change and releasing it to the production environment (or of verifying a process and repeating it in a production environment)
- (where applicable) method of separating test and production environments (e.g., separate test rig, or install onto production system but separate by time or a combination?) and a method for isolating test data from production data
- pre-requisites before a change is applied (i.e., state of equipment, backups/archive updates, other safety considerations)
- the effect on users, e.g., training plans
- personnel to whom to communicate the change (distribution list)
- a Backout Plan

The distinction between a Change Plan and a Validation Plan is one of scale and scope.

10.9.4 Backout Plan

The Backout Plan (also called a rollback plan) should be risk-based and address the possibility that the change has to be rolled back. It may include:

- an impact assessment and escalation process
- whether workarounds are available while problems are being investigated or whether a rollback is required
- What is the impact across the environment?
- Decision making process with clearly defined roles and responsibilities

Backout Plans should consider effects for differing scenarios (e.g., rollback is required after a period of live running, compared to rolling back at the point of installation) on:

- system data

- GxP data
- transitions between test and production environments
- documentation
- personnel
- production disposition

Where a rollback is not possible, a risk assessment should be performed to identify how the risk of irreversible harm should be managed. It may be beneficial to clone a live system and test a change on the clone.

A Backout Plan does not justify reducing the amount of testing planned for a change.

10.9.5 Configuration Item List

For each configuration item, a Configuration Item List should contain:

- item description
- document number, part number, or module number
- current issue or version
- issue or release date
- location of master record (for documents and software items)
- change history of the configuration item

10.10 Scalability

10.10.1 Change Management

This section describes an **example** approach to the scaling of change management. This example is intended to be illustrative only and not definitive.

System Impact

Using the methodology of GAMP® 5 Appendix M3: Science Based Quality Risk Management the System Impact (Reference 7, Appendix 4) is determined as Low, Medium, or High.

Change Impact

An initial impact assessment is performed for the change to determine the rigor with which the change is to be managed. Changes may be assigned as Low, Medium, or High Impact. For example:

Change Classification	Change Characteristics
Low Impact change	• simple change – low complexity • low technical impact on the system • no impact on patient safety, product quality, or data integrity
Medium Impact Change	• medium complexity change • has limited technical impact on the system • may have potential impact on patient safety, product quality, or data integrity
High Impact Change	• complex change • has significant potential technical impact on the system • may have significant potential impact on patient safety, product quality, or data integrity

Change Rigor is then determined from the table of System Impact versus Change Impact, see Table 10.2.

Table 10.2: System Impact versus Change Impact

		Change Impact		
		Low Impact Change	**Medium Impact Change**	**High Impact Change**
System Impact	**Low Impact System**	L	L	M
	Medium Impact System	L	M	H
	High Impact System	M	H	H

Where:

L = Low Change Rigor

M = Medium Change Rigor

H = High Change Rigor

10.10.2 Configuration Management

The initial definition of the Configuration Item List occurs during the Project Phase, but may change significantly during the Operation Phase.

Only those items that need to be controlled should become Configuration Items, because of the level of work involved in Configuration Management.

- Too few Configuration Items, i.e., not capturing all the essential elements of the system and the system is not adequately controlled and could not be re-created in the event of a disaster or a rollback.

- Too many Configuration Items, i.e., making Configuration Items of elements which are not essential and do not need this level of control and the process generates excessive work without adding value.

A risk-based approach may be used to determine the scope of the items which need to become Configuration Items. For a High Impact system, more of the validation documentation and operational elements may be included as Configuration Items. Similarly, for a Low Impact system of low complexity, it may be considered sufficient to document the model number and version of the system, and rely on a Supplier's Configuration Management processes.

Table 10.3: Change Rigor

	Change Control	Configuration Management
Low Change Rigor	• Risk Assessment is a checklist. • Change Plan and Modification Specification can be limited/documented as part of a change. • Test plan must be pre-approved, but does not need Quality Unit approval. • Testing needs only to verify that the change has been successful. It may be possible to omit some steps, e.g., the Change Review Board or the collection of test evidence.	• Few Configuration items affected. • Quality Unit involvement usually not required.
Medium Change Rigor	• Follows full flow of Change Control • Testing may be limited to areas directly impacted by the change. • Quality Unit involvement may be minimal.	• Affected configuration items may include specifications and system components. • Quality Unit involvement for deployment to live system is required as a minimum.
High Change Rigor	• Follows full flow of Change Control. Risk assessment will include functional level. Testing with evidence is required and will likely include regression testing. Quality Unit may be full partners. Change Plan will include a Backout Plan. Validation planning may be appropriate. • High Impact Change may indicate project sized change (becomes a development project) or a single discrete but highly significant change. • Quality Unit should review and approve the change, where required.	• Detailed specifications, operating manuals, test specifications; static data, etc. may be affected. Significant work may be required to update all affected items, issue, and replace previous versions. • High level of Quality Unit involvement required.

11 Repair Activity

11.1 Introduction

Repair activity is the process by which non-functional systems are returned to a functional state. This process uses a decision making process to scale the level of response and documentation associated with the repair activity.

This section is related to Appendix O7 of GAMP® 5 (Reference 7, Appendix 4).

11.2 Scope

This guidance applies to the physical act of repairing or replacing a defective system component, typically instrument, equipment, or hardware related. It sits below the higher-level procedures governing the provision of repair activity, e.g., O2 Establishing and Managing Support Services, and can be triggered by O4 Incident Management, O5 CAPA, or Calibration processes.

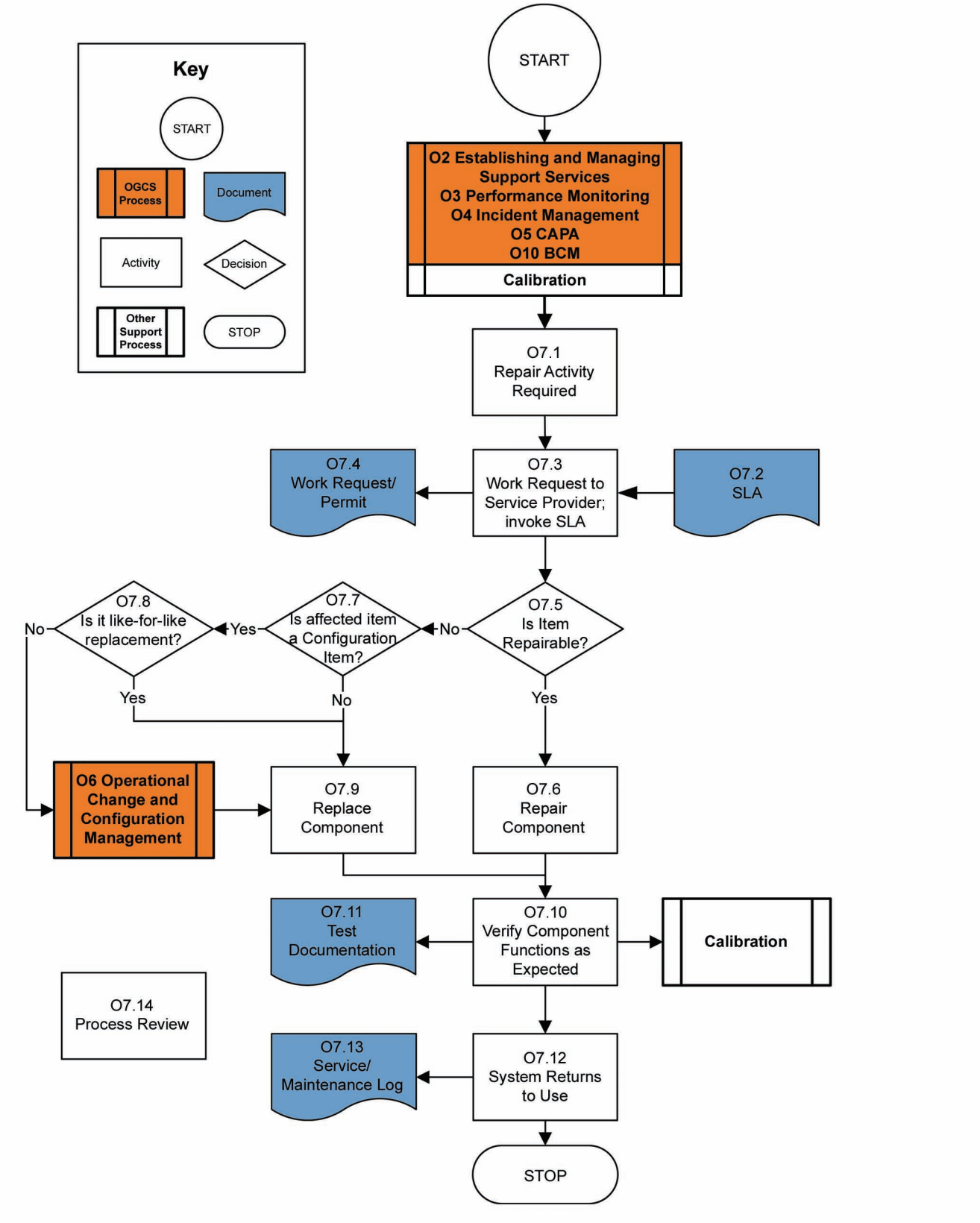
11.3 Roles and Responsibilities

Table 11.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 11.1: Roles and Responsibilities for Repair Activity

Role	RACI Role	Responsibilities
Process Owner	I	• informed where repair activities may impact process
System Owner	A	• accountable for the implementation of the repair process while maintaining system availability • identifies those components eligible for repair or replacement • maintains a spares list
Platform Support (SME)	R	• responsible for planning, making, and documenting the repair in accordance with the defined process, as appropriate
Application Support (Technical/SME)	R	• responsible for planning, making, and documenting the repair in accordance with the defined process, as appropriate
Quality Unit	C	• may be consulted on appropriate procedures and documentation requirements
Supplier	C	• may need to be consulted during the repair or diagnostic activity
End User	I	• needs to be informed of potential impacts on system availability
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

11.4 Repair Activity Process Flow Diagram



11.5 Process Narrative

Process Step/Decision/Record	Description
O7 Repair Activity	**The operational process of managing repair or replacement of a failed or defective component, which may be a configuration item.**
O2 Establishing and Managing Support Services **O3 Performance Monitoring** **O4 Incident Management** **O5 CAPA** **O10 Business Continuity Management**	These operational processes may trigger a Repair Activity.
Calibration	Calibration of a component may trigger the need for a repair activity.
O7.1 Repair Activity Required	Evaluation of the incident determines that a repair is needed.
O7.2 SLA	An SLA governs the provision of repair. The SLA has been previously established under the **O2 Establishing and Managing Support Services** process.
O7.3 Work Request to Service Provider; invoke SLA	Under the terms of the SLA, the service provider is informed of the need for repair or maintenance.
O7.4 Work Request/Permit	Work Request or Permit is raised to execute the repair work. For further information, see Section 11.7.1 of this Guide.
O7.5 Is Item Repairable?	An evaluation by the support provider to determine if the item can be repaired or if a replacement is necessary. If the item cannot be repaired, the process moves to step O7.7.
O7.6 Repair Component	Defective part is repaired according to Work Request/Permit. Workflow now moves to step O7.10.
O7.7 Is affected item a Configuration Item?	If the item is not on the Configuration Item List, the replacement can proceed. If the item is on the Configuration Item List, it should be determined if the replacement is like-for-like.
O7.8 Is it like-for-like replacement?	If the replacement is not like-for-like (i.e., the component is traced and documented by serial number or an identical component is not available), **O6 Operational Change and Configuration Management** is triggered. The key question is: will the status of the component change as a result of the repair or replacement? For further information on like-for-like changes, see Section 10.8.1 of this Guide. If the replacement is like-for-like, it can proceed.
O6 Operational Change and Configuration Management	Where a like-for-like replacement is not available for a Configuration Item, Change Control is invoked. Details of the changed component are recorded in the Hardware Specification if needed. The Configuration Item List is updated.

11.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O7.9 Replace Component	Components that cannot be repaired are replaced.
O7.10 Verify Component Functions as Expected	Test to demonstrate fitness for purpose using e.g., a checklist or standard form (Good Engineering Practice). Testing activities should be based on impact, risk, and complexity of the repair; the need for regression testing also should be considered.
Calibration	For analytical equipment systems, a calibration confirmation or performance test is required.
O7.11 Test Documentation	Depending on the level of GxP criticality of the system, formal test documentation may be created and should be retained.
O7.12 System Returns to Use	Released after testing, the system returns to use. Users are notified.
O7.13 Service/Maintenance Log	Service and Maintenance Log is updated. This may include either a reference to testing documentation or confirmation that informal testing was completed (depending upon type of repair activity and affected item). Records of service or maintenance may include independent reports as well as a Log entry.
O7.14 Process Review	A regular review of the process should be performed by the System Owner, Process Owner, and SMEs, as appropriate, to ensure that the SLA is being followed and achieved, and that it is still aligned with business needs. Work Requests, Permits, Test Documentation, and Service and Maintenance Logs should be reviewed regularly by the System Owner to look for trends and exceptions.

11.6 Procedural Guidelines and Considerations

11.6.1 General Considerations

The Repair Activity process may involve making a physical change to a validated system outside of the Change Management process. This means that the Repair Activity process has the potential to impact significantly on control of a system if not applied appropriately.

The Repair Activity procedure should:

- Be clear as to what constitutes repair activity.
- Identify when Change Management process needs to be invoked.
- Ensure Good Engineering Practice is followed, including a risk-based approach to testing.
- (Where appropriate), identify rollback/disaster recovery procedures.

11.6.2 Periodic Review Considerations

For a particular system, following repair:

- Is adequate and appropriate test documentation available to confirm that the repaired component functions as intended?
- Are Service and Maintenance log and reports available for review?

11.7 Records and Record Content

11.7.1 Work Request/Permit

A work request or permit should be raised to trigger the execution of the repair work. It should contain:

- unique identifier
- reference to Incident Log Reference Number or CAPA Log Entry Number
- system identity
- component identity or description
- description of the work to be undertaken (and reference to relevant procedures)
- cross references to other required documentation (see below)
- an indication of the priority to be given to the repair

Internal SOPs may require the provision of Engineering Health and Safety documentation, e.g., method statements and risk assessments, isolation certificates, etc. as a precursor to the issuing of the work permit.

11.7.2 Service Reports

A Service Report (typically part of the Service/Maintenance Log) will be created as a result of the Repair Activity. In addition to the information contained in the original work request, it will typically include:

- user name and contact details of the person undertaking the repair
- description of work undertaken, parts used, and testing performed
- details of any related work to be undertaken, e.g., change control or documentation update

11.8 Scalability

Guidance on the extent to which the Repair Activity operational process can be used is indicated in Table 11.2 System Impact versus ‘Repair Complexity.’

Table 11.2: System Impact versus 'Repair Complexity'

	→ Increasing 'Repair Complexity' →		
	Repair	**Like-for-Like Replacement**	**Different Component Used**
Low Impact System	Test repair on completion.	Test system on completion.	Change Control is invoked. Use Checklist or Form to Confirm system is satisfactory.
Medium Impact System	Test repair on completion.	Use Checklist or Form to confirm system is satisfactory.	Change Control is invoked. Documented testing of functions most affected by the component.
High Impact System	Use Checklist or Form to confirm repair is satisfactory.	Document testing of functions most affected by the component.	Change Control is invoked. Regression analysis performed, followed by formal testing. Update specifications. Verify system functionality prior to acceptance and release.

12 Periodic Review

12.1 Introduction

As defined in GAMP® 5:

"Periodic reviews are used throughout the operational life of a system to verify that it remains compliant with regulatory requirements, fit for intended use, and satisfies company policies and procedures. The review should confirm that, for all the components of a system, the required support and maintenance processes are established and that the expected regulatory controls (Plans, Procedures, and Records) are established and in use."

Therefore, Periodic Review is a critical Operational process – without Periodic Review it is not possible to demonstrate that control has been maintained throughout a system's life cycle.

A frequent output of Periodic Review is the identification of Corrective Actions (part of CAPA) which will improve the control and operation of the system.

This section is related to Appendix O8 of GAMP® 5 (Reference 7, Appendix 4).

12.2 Scope

The scope of Periodic Review may be a single regulated system or a group of similar regulated systems. Where corrective actions have been identified, a follow-up review may focus only on specific components of a system.

The scope of a Periodic Review includes the application and also may include an evaluation of the compliance status of an entire system, i.e., training and competence of end users and support SMEs, controls of segregation of responsibilities, etc.

Where appropriate, the Periodic Review of a system may be completed as part of a broader activity, such as periodic review of a manufacturing process.

Supplier audits are outside the scope of this Guide; however, there may be circumstances where a system in the Operation phase may require that the supplier be re-audited or that a new supplier of support services is audited for the first time. GAMP® 5 Appendix M2 Supplier Assessment should be followed.

Where the production environment is supported by other controlled environments, they also should be within the scope of Periodic Review. The Periodic Review should consider the controls in place to ensure that these other controlled environments are equivalent to the production environment. The review also should consider the process by which software changes are promoted to the production environment.

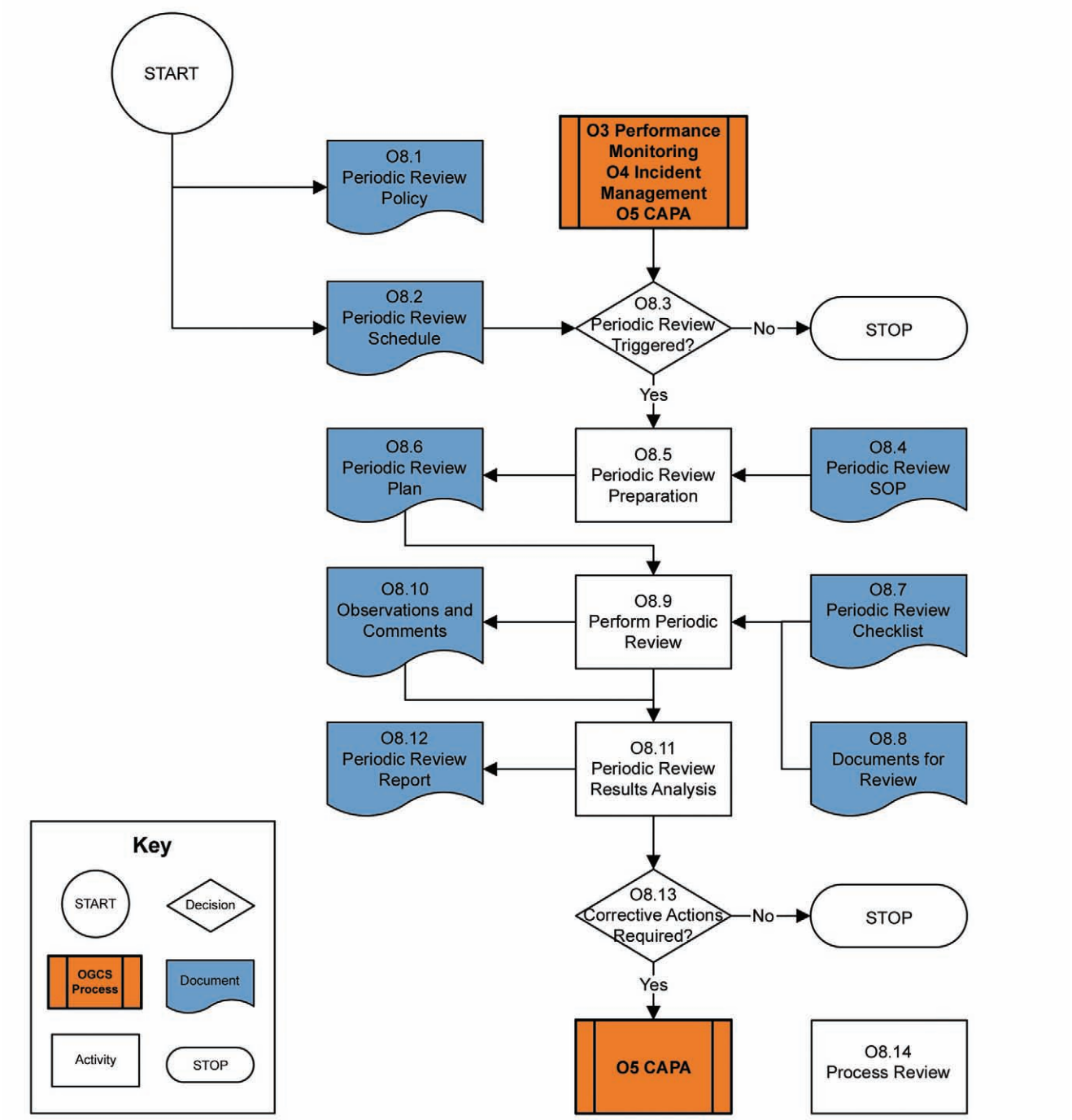
12.3 Roles and Responsibilities

Table 12.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 12.1: Roles and Responsibilities for Periodic Review

Role	RACI Role	Responsibilities
Process Owner	A	• accountable for ensuring that Periodic Reviews are conducted according to schedule and procedure • attends the review • responds to the Reviewer's questions or directs the Reviewer to the appropriate person • accountable for the completion of any agreed remedial activities, including appropriate reviews and approvals of Periodic Review report
System Owner	R	• attends the review • makes system documentation available as necessary during the review • assists with the execution of any remedial activities.
Reviewer/Auditor (SME)	R	• conducts the review in coordination with the Quality Unit • must be familiar with the procedure and the relevant regulations • must be competent to conduct the review for the system • prepares and issues a report of the findings
End User	C	• may attend the review • responds to questions put by the reviewer
System Administrator	C	• may attend the review • makes system documentation available as necessary during the review • assists with the execution of any remedial activities
Application Support (SME) and Platform Support (SME)	C	• may attend the review • makes system documentation available as necessary during the review • assists with the execution of any remedial activities
Quality Unit	C	• may attend the review • reviews and agrees all remedial activities • assures that Periodic Reviews are scheduled, performed, and documented
Supplier	C	• may be consulted prior to the review • may attend the review • makes system documentation available as necessary during the review • assists with the execution of any remedial activities
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

12.4 Periodic Review Process Flow Diagram



12.5 Process Narrative

Process Step/Decision/Record	Description
O8 Periodic Review	**The operational process which verifies that GxP regulated systems remain compliant with regulatory requirements, are fit for intended use, and satisfy organizational policies and procedures.**
O8.1 Periodic Review Policy	A high level document which may be a separate policy or contained within other policy documents, i.e., Validation Master Plan or Quality Management System, which defines the policy of the regulated organization with respect to Periodic Reviews.
O8.2 Periodic Review Schedule	This document is a schedule of reviews generated by the application of the Periodic Review policy to the organization's systems and processes.
O3 Performance Monitoring **O4 Incident Management** **O5 CAPA**	The operational processes which may trigger a requirement for a Periodic Review.
O8.3 Periodic Review Triggered?	A Periodic Review is required – the triggering process should allow sufficient time for the review to be organized to ensure that all key personnel are able to participate and that there is sufficient preparation time, i.e., to identify and locate required records.
O8.4 Periodic Review SOP	This generic procedure determines how the review will be performed, what documentation/checklists will be required, and identifies reviewers and approvers of the Periodic Review Report.
O8.5 Periodic Review Preparation	To ensure a successful Periodic Review appropriate preparations should be made, the objectives and scope of the review should be defined, participants identified and briefed, checklists prepared, and facilities be available for inspection. If an external Reviewer/Auditor is involved, the briefing should include this individual.
O8.6 Periodic Review Plan	This is optional. For a comprehensive review of a large complex system, there will be many components; a thorough review will need careful preparation if it is to be successful. For a routine review of a low risk priority system, a plan may not be required if a suitable procedure and checklist are already available.
O8.7 Periodic Review Checklist	To ensure consistency of review in terms of scope and level of detail, it is recommended that checklists for review topics are prepared. There may be variants of the checklist for different classes of systems, e.g., laboratory systems, or automation systems. A checklist will be of use to inexperienced Reviewers/Auditors, but should not constrain the review from 'drilling down' into areas where deviations have been identified. This approach may help to determine the size of an issue, i.e., is it a chance finding or a systemic problem – possibly affecting several systems (e.g., a problem with the operational change and configuration management process)?
O8.8 Documents for Review	Documents (procedures and control records) are inputs into the Perform Periodic Review activity.

12.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O8.9 Perform Periodic Review	The Periodic Review is performed. Responsible persons should participate in the review.
O8.10 Observations and Comments	The Reviewer/Auditor records findings according to the checklist and any other observations and comments relevant to the review.
O8.11 Periodic Review Results Analysis	The Reviewer/Auditor analyzes the findings and may seek further information from the Process Owner, System Owner, etc. Factual questions arising during the Periodic Review may require further investigation.
O8.12 Periodic Review Report	The Reviewer/Auditor creates a report. The structure of the report may be based on that of the checklist. Depending on the complexity of the system and nature of the Periodic Review, the report may be a separate document or an appropriately approved checklist. A statement of the overall outcome of the review regarding the compliance state of the system should be documented. All deviations or issues of concern identified during the review should be reported along with an indication of how they will be addressed. There is also an opportunity to recognize good practice when it is observed.
O8.13 Corrective Actions Required?	Deviations may require corrective actions. The organization may wish to perform a risk assessment of the recommendations before committing to perform corrective actions. If no CAPA actions are identified, the Periodic Review is complete.
O5 CAPA	Once committed to, corrective actions can be managed to resolution via the CAPA process. An outcome of the Periodic Review may be the identification of the need to perform a follow-up review of a system or of a particular support process.
O8.14 Process Review	The Process Owner should ensure that Periodic Reviews are conducted according to schedule and following the appropriate procedure. The Quality Unit should assure that Periodic Reviews are performed according to schedule and following the procedure and checklist, that observations and comments are formally documented, and that resulting corrective actions are progressed to resolution through O5 CAPA.

12.6 Procedural Guidelines and Considerations

12.6.1 General Considerations

Before Periodic Reviews of a system can occur within an organization, the related policy, procedure, document templates, and checklists should be prepared with appropriate SME involvement. The availability of the Periodic Review SOP should be verified prior to acceptance and release.

Participants in the review should have received training regarding the process to be followed.

The role of the Reviewer/Auditor is considered critical. Depending on the policy and maturity of approach of the regulated organization, the performance of the review could be assigned to an internal colleague (e.g., a member of the Quality Unit) or to a suitably qualified and experienced external resource.

Periodic Reviews should involve key participants. Where possible, a 'round table' meeting should be held. For large global systems, this may not be feasible. It may be necessary for the reviewer or review team to collect evidence remotely, and to provide an opportunity for participants to comment on observations independently. The Review Report can be reviewed separately with the Process Owner and the System Owner.

The strategy for conducting a Periodic Review should be agreed prior to the Periodic Review. Two approaches are:

1. 'Vertical' Review: a system is selected and a detailed review of the evidence supporting the establishment and maintenance of control is performed. This review may involve the supplier and support providers for the system.

2. 'Horizontal' Review: the extent to which control processes are applied consistently is subject to review. This type of process review may involve more than one system and may involve providers of support services to an organization.

Providing a formal 'certificate' for each 'horizontal' process with a definitive expiry date, may make effective use of reviewer resources. Vertical reviews then verify that 'horizontal' processes are certificated and in date. A risk-based approach (such as that described in Section 12.8.2 of this Guide) should be used to determine the extent to which 'horizontal' reviews can be used to support Periodic Reviews.

12.6.2 Triggering a Periodic Review

End users should be involved in the implementation and ongoing operation of a system. A review process that is triggered by end user feedback may be beneficial. Processes to collect feedback regularly and to perform trending analysis should be established. In addition to a Periodic Review Schedule, reviews may be triggered by Performance Monitoring, Incident Management, and CAPA.

12.6.3 Periodic Review Preparation

The effectiveness of preparation activities can affect significantly the outcome of a review.

The objectives, team composition, and review agenda should be agreed prior to a Periodic Review. Key individuals (e.g., Process Owner, System Owner, SMEs, System Administrator, and Quality Unit) should participate in a Periodic Review. Prior to a Periodic Review, the Reviewer/Auditor should inform key individuals that the following records and information (where applicable) should be available for the Periodic Review:

- the Validation Plan and Validation Report for the system
- the status of outstanding actions arising from the Validation Report
- System Specification and Verification documentation
- previous periodic review report
- other audit reports
- the status of any outstanding actions arising from prior reports and reviews
- operational and maintenance SOPs and related records
- calibration records
- configuration item list
- change management information (the level of changes that a system has been subject to and the nature of those changes)

- changes in the scope of use of the system
- list of system users and training records
- performance monitoring records
- equipment log books (e.g., for laboratory systems)
- incident logs
- backup and restore logs
- security and access control information
- where applicable and depending on the regulated company's approach, documents demonstrating compliance with specific regulations, such as 21 CFR Part 11 (Reference 1, Appendix 4) or EU GMP Annex 11 (Reference 2, Appendix 4)

Periodic reviews also should consider the 'fitness for use' of a system. This should consider its medium and long term viability, e.g., whether components of the system or its support hardware or software, are likely to become obsolete. This could initiate plans to obtain hardware spares or system retirement and replacement. This should be identified early in the process, as replacing a control system could take a significant amount of time.

Appendix 3 contains a list of control records identified elsewhere in this Guide.

12.6.4 Performing a Periodic Review

Performing a Periodic Review includes:

1. Opening Meeting
2. Review
3. Closing Meeting
4. Report of the Findings

These may be separate activities for large complex systems, but may be combined into one continuous activity for simple/small systems. Depending upon the complexity of the system andthe complexity of the review, opening and closing meetings may not be required.

12.6.4.1 Opening Meeting

The Reviewer/Auditor should introduce the review at the opening meeting, which should be attended by the System Owner, System Administrator, Quality Unit representative, and other invitees, as required. The purpose of this meeting is to introduce reviewers (if necessary), re-iterate the objectives of the Periodic Review, how long it is expected to take, and who is required or expected to participate, in addition to other relevant background information.

12.6.4.2 Review

A Periodic Review typically will include how a system is operated, current procedures relevant to the system, and evidence that procedures are being followed. The review also should consider the extent of use of the system, whether it is still required, and whether it is being used as intended.

12.6.4.3 Closing Meeting

Following the Periodic Review, a closing meeting should be held where the Reviewer/Auditor can identify adverse findings. This allows discussion and may clarify misunderstandings or misinterpretations. The System Owner, System Administrator, Quality Unit representative, and other invitees (as required) should have opportunity to comment before a Periodic Review is closed. It is preferable to do this final review 'face to face' with review participants present, but it may be performed electronically, (e.g., by the circulation of a draft report of the findings).

12.6.4.4 Report of the Findings

The Reviewer/Auditor should publish a Periodic Review Report of the findings of the review which should be submitted to the Process Owner, the System Owner, and the Quality Unit for approval. The minimum output should be a documented justification of the continued acceptability of use of systems under review.

12.6.4.5 Remediation Action Planning

Where corrective actions are identified and agreed, these actions are managed through to resolution by **O5 CAPA**.

The timeline for corrective actions should be commensurate with the criticality of adverse findings, coordinated with other activities concerning the system (e.g., scheduled upgrade), and should recognize the exposure of non-compliance.

12.6.4.6 Monitoring

All corrective action owners should be accountable for ensuring that each task is brought to closure, which may involve coordination with change control procedures, SOP update procedures, and training procedures.

A follow-up meeting or a series of follow-up meetings should be scheduled to review and progress the corrective actions against 'target completion dates.' The meetings should ensure that corrective action items are closed and should address the progress of any outstanding corrective actions.

12.6.5 Periodic Review and Internal Quality Audits

A regulated organization may perform Internal Quality Audits of processes in addition to Periodic Reviews of systems. These may include operational and support processes which may be wholly or in part not specific to an individual system.

Where a support process can be demonstrated with confidence to be implemented consistently across the regulated site/organization, the Internal Quality Audit results for that site/organization can be used to mitigate the depth of Periodic Review. A risk-based approach should be adopted to ensure that sufficient evidence is available to assure that high risk systems are under control. For further information, see Section 12.8.2 of this Guide.

The following operational processes are likely to be system independent:

O3 Performance Monitoring

O4 Incident Management

O5 CAPA

O6 Operational Change and Configuration Management

O8 Periodic Review

O9 Backup and Restore

Other operational processes are generally system specific, but also may contain elements which are system independent:

O1 Handover

O2 Establishing and Managing Support Services

O7 Repair Activity

O10 Business Continuity Management

O11 Security Management

O12 System Administration

O13 Archiving and Retrieval

D7 Data Migration

M10 System, Retirement, Decommissioning, and Disposal

12.7 Records and Record Content

12.7.1 Periodic Review Policy

The Periodic Review Policy is a high level commitment to perform Periodic Reviews. The policy also may address:

- how the policy will be achieved
- the approach to be taken
- how the frequency/scope of reviews will be determined

12.7.2 Periodic Review Schedule

The Periodic Review scheduling strategy for each system may be included or referenced in the Validation Master Plan. The schedule can be in spreadsheet form and should involve all systems at the regulated site/organization. The key elements of the schedule are:

- system name and description
- system version
- Process Owner
- System Owner
- System Administrator
- risk category (High, Medium, Low)

- release history
- date of last Periodic Review
- planned intervals between periodic reviews for that system
- expected date of next Periodic Review
- reference to last Periodic Review Report

12.7.3 Periodic Review SOP

This Periodic Review SOP should be generic to all systems within a regulated site/organization.

Typically, sections may include:

- Principle
- Purpose
- Scope
- Responsibilities
- Procedure to be followed
  - Preparation
  - Execution
  - Review and Remediation
  - Documentation and sign-offs
  - Periodic Review Checklist

12.7.4 Periodic Review Plan

A Periodic Review Plan normally is required only where the scale and complexity of the intended Periodic Reviews requires detailed definition and pre-planning prior to execution.

12.7.5 Periodic Review Checklist

The Periodic Review SOP should contain or reference an appropriate checklist or set of standard questions to guide the review. The use of a checklist to be completed during a Periodic Review provides an agenda, ensures that all review topics are considered, and promotes consistency between Periodic Reviews.

For a list of the control records identified in this Guide, see Appendix 3; these may be helpful in the preparation of the Periodic Review checklist. The Appendices also includes a list of external factors (e.g., change in regulations) that also may to be considered.

12.7.6 Periodic Review Report

The following information should be considered in the Periodic Review Report:

- system covered
- scope of review
- list of participants
- list of deviations
- list of corrective actions (proposed and confirmed)
- status of actions (open or completed)
- summary of compliance status

12.8 Scalability

The frequency and depth of Periodic Reviews can be determined by using a risk-based approach, which considers relevant factors such as impact, complexity, and novelty of a system.

12.8.1 Frequency of Periodic Review

12.8.1.1 Initial Review

The first Periodic Review for a new or significantly upgraded system should be performed within a relatively short time period of it being handed over for operational use. If there are any unanticipated problems with the performance or support provision for a system, these should be identified as rapidly as possible and remedial actions instigated.

12.8.1.2 Ongoing Review

Several models could be adopted to determine the interval between successive reviews.

A scalable approach can be used to ensure that high impact systems receive more frequent reviews than low impact systems. For further information, see GAMP® 5 Appendix M3 (Reference 7, Appendix 4).

Table 12.2 is presented as an **example** for guidance only; regulated organizations should set a frequency of Periodic review appropriate to the risks to patient safety, product quality, and related records. Typically, only critical systems will receive annual Periodic Review.

Table 12.2: Frequency of Periodic Review

System Impact	Frequency of Periodic Review
Low	Periodic Review should be conducted at least once every 3 years.
Medium	Periodic Review should be conducted at least once every 2 years.
High	Periodic Review should be conducted at least once every year.

Periodic Reviews also may be triggered by other operational processes, i.e., CAPA, Performance Monitoring, and Incident Management.

12.8.2 Depth of Review

The Depth of Periodic Review can be determined by adopting a risk-based approach. Factors which may be considered include:

- GAMP® Category of the system (See GAMP® 5 Appendix M4)
- Outcome of the previous review
- Level of change to the system since the previous review

Different levels of review can be defined, e.g., a three level model may be adopted:

Level 1: Checklist only

A Level 1 Periodic Review is intended to be effective and efficient. The Reviewer/Auditor should confirm that the required Plans, Procedures, and Records are in place and have been subject to the expected level of review and approval. The status of actions identified at a previous review should be evaluated and recorded. A separate Periodic Review Report is not produced; review findings, observations, and actions arising are recorded directly onto the checklist.

Evidence from Internal Quality Audits related to operational and support processes is accepted – which may not be specific to the system being reviewed.

A checklist only review will not normally evaluate the quality and content of the documentation. Evidence does not need to be retained; however, the Reviewer should seek and observe objective evidence to support the findings.

A separate Periodic Review Report is not produced; review findings, observations, and actions arising are recorded directly onto the checklist.

Level 2: Intermediate

The objective of a Level 2 Periodic Review is to perform a review appropriate to the impact and complexity of the system (linked to GAMP® Category) of the system. The reviewer confirms that the required Plans, Procedures, and Records are in place and have been subject to the expected level of review and approval. The status of actions identified at any previous review should be evaluated and recorded. Areas where there have been significant changes are examined in detail, e.g., major system upgrades or changes in scope of use of the system.

The review may evaluate the quality and content of the documentation. The Reviewer should seek and observe objective evidence to support the findings and relevant evidence may be retained.

Evidence from Internal Quality Audits related to supporting processes may be accepted – wherever possible it should be specific to the system being reviewed.

The findings of the review will be documented in a Periodic Review Report.

Level 3: Detailed

The objective of a Level 3 Periodic Review is to perform a comprehensive review of all components of the system. Examples of Plans, Procedures, and Records specific to the system are obtained and are reviewed in depth by the Reviewer to confirm that the content is aligned with the controlling procedures. The status of actions identified at any previous review should be evaluated and recorded.

A 'challenge testing' approach is adopted. The Reviewer should seek and observe objective evidence to support the findings and relevant evidence may be retained.

Evidence from Internal Quality Audits related to supporting processes may be accepted, but should be specific to the system being reviewed.

The findings of the review should be documented in a Periodic Review Report.

Table 12.3 is presented as an example for guidance only; regulated organizations should set a depth of review appropriate to the risks to patient safety, product quality, and related records. Where a review identifies or indicates suspected issue, further reviews should be performed to determine the extent of the problem and to identify root causes.

Table 12.3: Depth of Periodic Review

	Depth of Periodic Review			
System Impact	GAMP® Category			
	1	**3**	**4**	**5**
Low	Level 1	Level 1	Level 2	Level 2
Medium	Level 2	Level 2	Level 2	Level 3
High	Level 2	Level 3	Level 3	Level 3

13 Backup and Restore

13.1 Introduction

The purpose of the Backup and Restore Process is to ensure the accurate and reproducible copying of digital assets (data and software) to protect against loss of original data and subsequent accurate restoration of assets when required, i.e., restore activity, disaster recovery.

This section is related to Appendix O9 of GAMP® 5 (Reference 7, Appendix 4).

13.2 Scope

Data and software employed by business critical and GxP regulated automated systems, e.g.:

- System Software
- Application Software (including 3rd Party Software)
- Firmware
- Configuration Data
- GxP-Regulated Data and Metadata
- Audit Trail
- Critical Business Data

A distinction is made between data backup and data archive.

- Backup is performed for short term duplication of ‘current’ applications and data on external media to prevent loss.
- Archiving is the process of deleting ’old’ applications and data (i.e., applications and data that are no longer expected to be used) from the original storage location (usually hard drives) after storage on external media.

The need for an effective backup and restore process applies equally to all systems, from a stand-alone instrument to an enterprise-wide application.

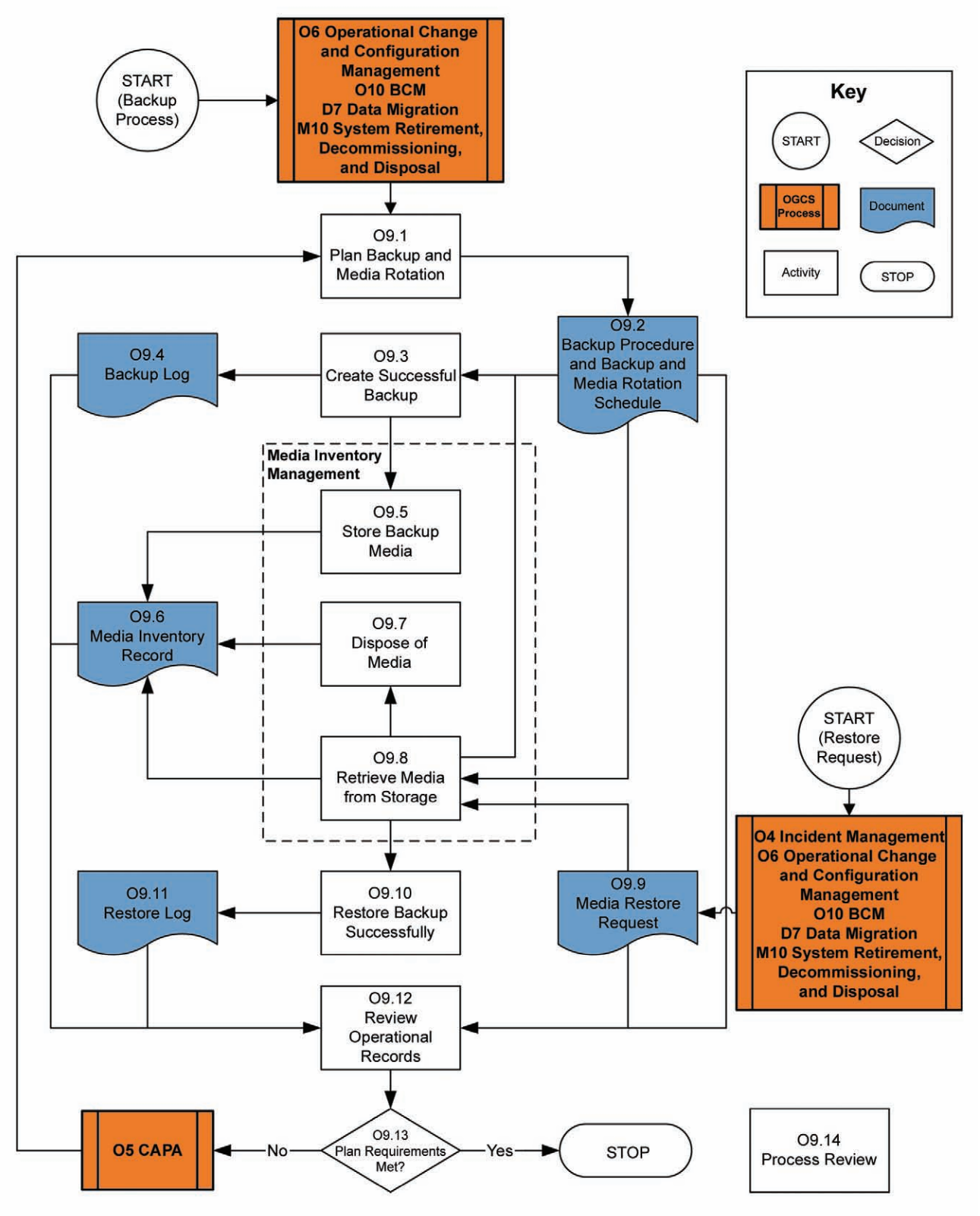
13.3 Roles and Responsibilities

Table 13.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 13.1: Roles and Responsibilities for Backup and Restore

Role	RACI Role	Responsibilities
System Owner	A	• accountable for establishing a Backup and Restore Process • accountable for the application of the Backup and Restore Process to system(s) under their ownership. • accountable for Review of Backup and Restore records • accountable for ensuring that the Backup and Restore Process meets the Business's system availability requirements
Platform Support (SME)	R	• responsible for executing the Backup and Restore process • responsible for the reporting of Backup and Restore issues • responsible for the resolving of Backup and Restore issues
Application Support (SME)	C	• consulted on Backup Schedule • remain informed in the event of Restoration Activity
Quality Unit	C	• may be consulted on critical GxP restoration activities
System Administrator (SME)	I	• remain informed of Backup Schedule • remain informed in the event of Restoration Activity
End User	I	• remain informed in the event of Restoration Activity
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

13.4 Backup and Restore Process Flow Diagram



13.5 Process Narrative

Process Step/Decision/Record	Description
O9 Backup and Restore	**Backup is the operational process of copying records, data, and software to protect against loss of integrity or availability of the original. Restore is the subsequent restoration of records, data, or software to their original configuration when required.**
O6 Operational Change and Configuration Management **O10 Business Continuity Management** **D7 Data Migration** **M10 System Retirement, Decommissioning, and Disposal**	The Backup process may be triggered by: **O6 Operational Change and Configuration Management, O10 Business Continuity Management, D7 Data Migration, M10 System Retirement, Decommissioning and Disposal.**
O9.1 Plan Backup and Media Rotation	The schedule for conducting backups and the rotation of backup media should be planned and based on a documented evaluation of the GxP and business criticality of data managed by the automated system.
O9.2 Backup Procedure and Backup and Media Rotation Schedule	The plan will specify a schedule for conducting backups, (including the requirement for 'ad hoc' backups as necessary) and rotating media. The storage locations of the backup media also will be specified.
O9.3 Create Successful Backup	Backups can be created automatically or manually. Manual backups should be executed by following a repeatable process. Backups should be assessed to verify successful completion. Criteria for deciding to repeat the backup should be documented in the event of a backup failure.
O9.4 Backup Log	The backup log can be system generated or manually generated. The log should record all backup attempts and outcomes. The backup log should reference any follow up required because of backup failure.
O9.5 Store Backup Media	Backup media should be stored in a secure location to prevent physical loss or accelerated environmental deterioration. One set of media should be stored at a location that is geographically separated from the servers.
O9.6 Media Inventory Record	The media inventory record should record usage of media, its age, generation, and location.
O9.7 Dispose of Media	Damaged or out-of-specification media should be securely disposed of according to an established process. Data confidentiality should be maintained. The media inventory should be updated accordingly.
O9.8 Retrieve Media from Storage	Media is retrieved for reuse according to criteria established in the schedule and the inventory log updated.
O4 Incident Management **O6 Operational Change and Configuration Management** **O10 Business Continuity Management** **D7 Data Migration** **M10 System Retirement, Decommissioning, and Disposal**	The Restore process may be triggered by: **O4 Incident Management, O6 Operational Change and Configuration Management, O10 Business Continuity Management, D7 Data Migration, M10 System Retirement, Decommissioning, and Disposal.**

13.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O9.9 Media Restore Request	A media restore request should be used to initiate a restore. The request should arise from the Incident Management or Business Continuity Management processes. The Media Inventory record should be updated accordingly.
O9.10 Restore Backup Successfully	Backups can be restored automatically or manually. Manual restores should be executed by following a repeatable process. A log of all restores should be maintained with their outcome.
O9.11 Restore Log	The restore log can be system or manually generated. The log should record all restore attempts and outcomes. If logs are automatic, manual review is required.
O9.12 Review Operational Records	A review of all backup and restore operational records is undertaken to verify that the backup and restore process is operating as planned. The review frequency will depend upon data volumes, criticality of data, and frequency of data updates.
O9.13 Plan Requirements Met?	On review of the backup and restore records, if there is evidence to suggest that the process is not meeting its planned requirements, corrective actions (see **O5 CAPA**) should be taken to reduce the risk of data loss.
O5 CAPA	If there is evidence to suggest that the process is not meeting its planned requirements, corrective actions should be taken to reduce the risk of data loss.
O9.14 Process Review	The System Owner should undertake regular reviews of the **O9 Backup and Restore** process to ensure that the backup and media rotation schedule is being met and that backup and restore logs and media inventory records are being maintained.

13.6 Procedural Guidelines and Considerations

13.6.1 Backup Media

Backup should be performed onto suitable media and media should be used in accordance with the recommendations of the manufacturer. When choosing storage media, the following should be considered:

- recommended service life
- acceptable environmental conditions for storage
- verification and rewrite requirements
- security of storage

The type of media used should be documented.

Electronic media deteriorates over time and media should be stored in accordance with the manufacturer's specifications.

13.6.2 Creating Successful Backups

Backups can be created automatically or manually. Manual backups should be executed by following a repeatable process.

Execution of the backup may be system specific and consideration should be given to how specific aspects will be addressed in the context of a generic procedure, e.g., use of system specific work instructions.

In addition to verification during the Project Phase, backup (and restore) processes should be tested to demonstrate that they operate reliably throughout the Operation Phase. This testing should be documented.

The backup process should include verification that the process has functioned correctly; verification mechanisms, such as Cyclic Redundancy Check (CRC) or file header comparison, may be appropriate.

Should a backup fail, criteria for deciding to repeat the backup should be documented, e.g., manual backup following two failed automatic backups.

There should be a defined escalation process to manage backup incidents or exceptions.

A log of all backups attempted, with outcomes, should be maintained.

Backup media should be uniquely identified and the following information should be clearly and securely associated with the backup media, either on the label itself, or in a separate log with unique identification codes linking the log entries and the backup media:

- creation date
- system/data designation
- version/baseline identifier (if applicable)
- backup type (i.e., daily differential backup or weekly full backup)
- current generation number (if applicable) and copy number (if applicable)
- date of first usage (of media if applicable)
- date of backup
- identity of operator (if performed manually)
- expiry date (date backup can be disposed)
- data backup tool including software/firmware version (if applicable)

13.6.3 Managing Media Inventory

In addition to local storage of backup media, for speed of restoration, a copy of the backups should be stored in a secure, geographically distinct location. The degree of geographic separation should take into account the likelihood of atmospheric and geographical hazards impacting both server and storage locations.

The backup media should be physically secured and protected from fire, water, and other hazards, including access by unauthorized personnel, whether physically or remotely (i.e., by hacking).

Where controls of physical media are required, the value of a record of inventory transactions to record all deposits, retrievals, and disposals should be considered.

Media close to their expiry date should be marked for data cleansing and disposal.

Damaged or out-of-specification media should be securely disposed of according to a documented process.

Inventory reconciliation should be carried out on a regular basis. The frequency of reconciliation should reflect the impact of data loss on business activities or regulatory responsibilities as a result of misplaced or damaged media or use of media close to expiry date.

13.6.4 Restoring Backups Successfully

Backups can be restored automatically or manually. Manual restores should be executed by following a repeatable process.

Restore requests by end users should be appropriately documented, because restoring data is a GxP-relevant process. A log of all restores should be maintained with their outcomes.

The technical part of the restore process may be system specific and consideration should be given to how this is addressed in the context of a generic procedure, e.g., use of system specific work instructions.

The restore process should be tested during the Operation Phase to demonstrate that it operates reliably. For software, the restored application should enable access to data, prevent data corruption, or integrate with other systems. For critical systems, the restoration of data from archives should be tested.

For the safe storage and restoration of GxP data for which the host system is either no longer in use or no longer is compatible, a data migration approach considered preferable, rather than the retention of “obsolete” equipment.

Periodic Review of critical archived data may be required, even if the host system (and possibly the entire production facility) is no longer in use. This may have been addressed in the system retirement plan, and should be reviewed to ensure the plan is still viable.

Media restore will be triggered by an incident. The restore should be managed by a formal process, e.g., by means of an approved request. The potential impact of restored data should be documented, e.g., re-synchronization of data may be required in the case of inter-dependant systems. Possible risks associated with the data to be restored should be evaluated, as required.

A full backup, prior to the restore, may mitigate further data loss should a restore fail.

Any failure of the restore process should trigger an incident which should trigger the CAPA process. The root cause of failures to restore data or systems should be established and documented.

The media inventory should be updated to indicate the purpose of media removal.

13.6.5 Periodic Review Considerations

For each system, a review of operational backup and restore records should be undertaken to verify that the backup and restore process is being performed according to schedule and following the procedure.

Considerations include:

- Does the backup process continue to be appropriate to system impact and data criticality?

- Have all backups been successful, if not, are failures explicable, and is the level of failures acceptable?
- Has there been any requirement to restore records or the system from backup, if so, was it successful?

The impact of any data restore activities executed to repair known incidents of data corruption should be evaluated in terms of the data integrity of scheduled backups already in the inventory media cycle. Controls to prevent any risk of propagating incidents of data corruption via the backup cycle should be reviewed.

On review of the backup and restore records, if there is evidence to suggest that the process is not meeting requirements, corrective actions should be initiated to reduce the risk of data loss.

13.7 Records and Record Content

13.7.1 Backup and Restore Procedure

A Backup and Restore procedure should be established and approved by the Quality Unit.

Where a Backup and Restore procedure is applicable to many systems, it should consider:

- the generic nature of the Backup and Restore procedure
- specific requirements of software backup versus data backup
- automated and manual system differences

System specific elements may be covered in system specific procedures or work instructions.

13.7.2 Planning Backup and Media Rotation Schedules

The schedule for backup should consider the volume of data, frequency of data update, data type, the resources required to support the update, and impact of data loss on business activities.

Both data and software should be backed up. Software backups are more likely to be event driven in that they are used to baseline a software system configuration for recovery after catastrophic system failure or faulty change implementation.

When data is to be backed up, the virtual drive and file directory coverage should be clearly defined.

Typically, a mixture of differential, incremental, or full backups is employed on the following basis:

- daily
- weekly
- monthly
- quarterly
- annually

The choice between differential and incremental backups will depend on the potential need to restore intermediate versions of updated files between full backups.

At least two generations of backup should be maintained, i.e., the current backup and the immediately preceding one. Typically, three generations are used.

Once all generations have been used, the oldest generation should be overwritten using the latest backup.

13.7.3 Backup Log

Information recorded in the backup log, which should be securely associated with the backup media, should include:

- detail of what is being backed up (data/system/software version)
- data backup type (full, incremental, differential)
- interval since last backup
- backup media
- life cycle status of the backup media
- data backup tool (including software/firmware version,if applicable)
- date/time of backup
- identity of person performing the backup
- location of backup

13.8 Scalability

A risk assessment may be required to determine the impact of loss of data to ensure that GxP records are adequately protected.

Other factors for consideration:

- Automation: automation of the backup process should be considered when the number of systems requiring backup poses a significant risk to the successful execution of the planned Backup Schedule or management of the media inventory.
- Data volumes: as data volumes increase the amount of system resources required to backup data may impact on system performance and capacity. There may be a need to tailor the backup regularity to accommodate the frequency of data updates, e.g., data that is archived will require less frequent backup than transactional data.

14 Business Continuity Management

14.1 Introduction

Business Continuity Management (BCM) encompasses the steps required to restore critical business processes following a disruption, while continuing to provide product or services to the Process Owner. Inadequate recovery plans may jeopardize the survival of an organization; a significant number of organizations have failed following a major disaster.

The Business Continuity Plan (BCP) will identify the triggers for invocation of the recovery plan, people to be involved and required communication, as well as the interim processes to maintain the process previously performed with the use of the system.

A disaster is an unplanned event that has the potential to impact process and data integrity or restrict access to or performance of the system for a prolonged duration.

Disaster Recovery Planning (DRP) is a sub-set of Business Continuity Management that focuses on regaining access to an IT system, including software, hardware, and data following a disaster.

The Business Continuity Plan and Disaster Recovery Plan prepared by an organization should be periodically tested to demonstrate that critical services and processes can continue, and that there is a process for the timely resumption of essential business functions.

This section is related to Appendix O10 of GAMP® 5 (Reference 7, Appendix 4) as applied to systems in their Operation Phase.

14.2 Scope

This guidance describes the operational process for DRP and BCM. The guidance is generic and scalable; generally the failure of a critical system will compromise the associated business process and require both the BCM and DRP to be invoked.

BCM is a regulatory requirement for high impact systems, which support critical regulatory or life-saving processes. Systems which execute a time-critical regulatory process, e.g., Lot Recall, Pharmacovigilance, are of particular regulatory concern.

The scope of this section excludes more significant Business Continuity events, such as breakdown of a major production facility, loss of the main office building, pandemic outbreaks, etc. Although the principles are identical, these are outside the scope of this Guide and covered elsewhere, e.g., in specialist business continuity management standards and associated publications.

14.2.1 Fail-Over and Fail-Back

The term ‘Fail-Over’ is used in this Guide; this is intended to mean “handover to the alternative business process.” This will be the process defined in the BCP and may be a manual or paper form based method or an alternative system or other solution that assures business continuity.

‘Fail-Back’ is the reinstatement of the interrupted process after a successful recovery.

14.3 Roles and Responsibilities

Table 14.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Note: only one role should be accountable for a process. For business continuity management, the ultimate accountability lies with the Process Owner; however, there are two key aspects to business continuity management:

1. business continuity planning (process orientated)

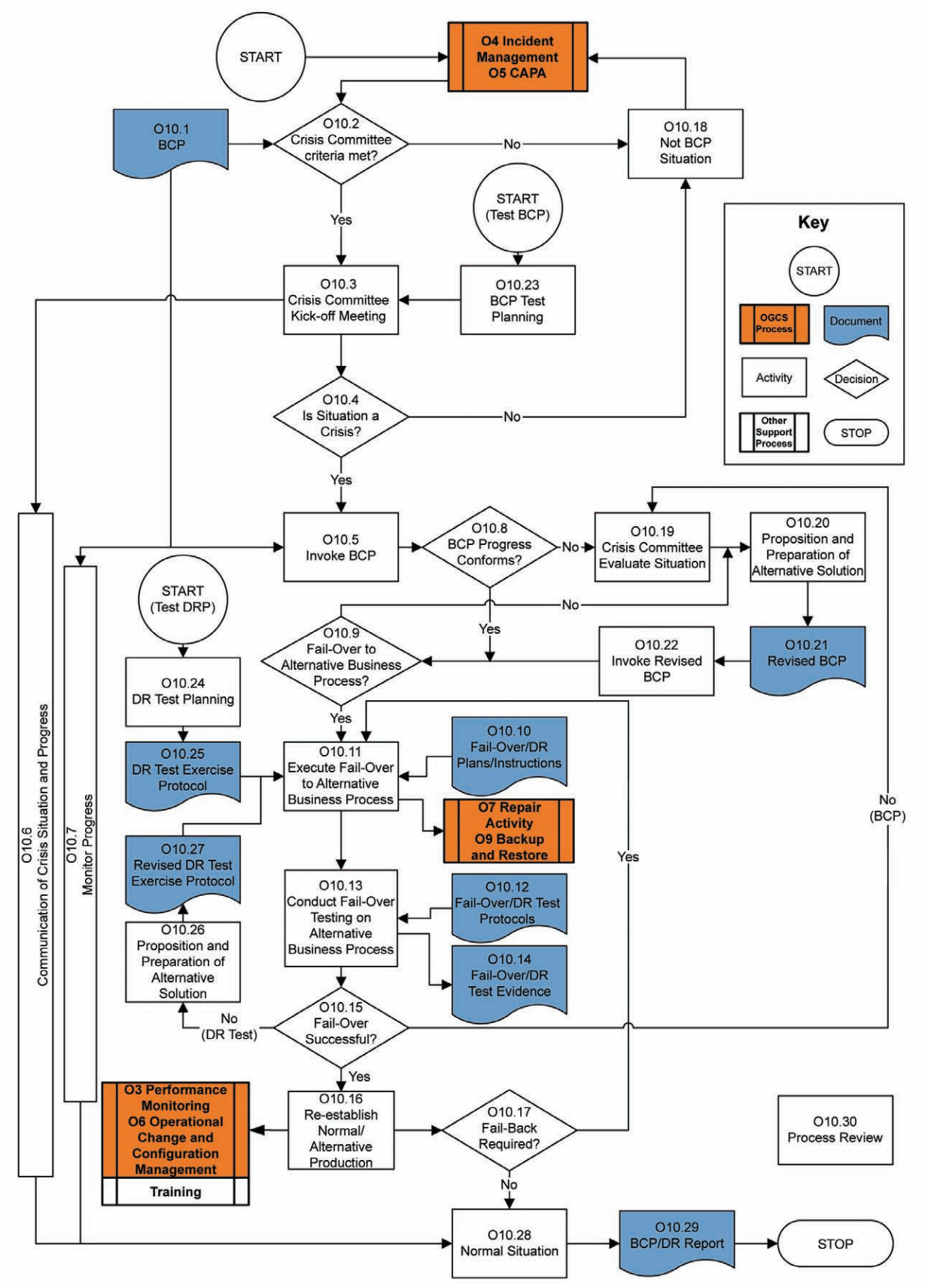
2. disaster recovery planning (system orientated)

To highlight the different orientation of the Process Owner and System Owner, each has been made accountable for their respective aspects.

Table 14.1: Roles and Responsibilities for Business Continuity Management

Role	RACI Role	Responsibilities
Process Owner	A	• accountable for establishing BCM processes for business processes under their ownership • accountable for ensuring that BCM and Disaster Recovery processes meet an organization's requirements and mitigate risks • accountable for the periodic testing of BCM processes • consulted on resolution of BCM and DR issues
System Owner	A	• accountable for DR processes for system(s) under their ownership • responsible for supporting the execution of BCM process(es) for systems under their ownership • responsible for executing periodic DR tests for system(s) under their ownership • responsible for producing records associated with the DR and BCM process, e.g., BCM plans/reports, Fail-Over/DR Plans/ Instructions, DR Test Protocols/Reports, Fail-Over/DR Test Protocols, and Fail-Over/DR Test Evidence • responsible for the reporting of DR and BCM issues • consulted on resolution of DR and BCM issues
Platform Support (SME)	R	• responsible for executing the DR and BCM processes related to platform support • responsible for the reporting of DR and BCM issues related to platform support • consulted on resolution of DR and BCM issues
Application Support (SME)	R	• responsible for executing DR and BCM processes assigned to application support • responsible for the reporting of DR and BCM technical issues related to application support • consulted on resolution of DR and BCM issues
System Administrator (SME)	R	• responsible for executing DR and BCM processes assigned to the System Administrator • responsible for the reporting of DR and BCM technical issues
Quality Unit	C	• consulted during the establishment of BCM and DR processes and plans • review of BCM and DR test evidence • consulted on resolution of DR and BCM Issues
Supplier	C	• may be consulted during the establishment of BCM and DR processes and plans • may be consulted on resolution of DR and BCM issues
End User	I	• remain informed of the DR and BCM process
Where R=Responsible, A=Accountable, C=Consult, I = Inform See Appendix 1 for definitions.		

14.4 Business Continuity Management Process Flow Diagram



14.5 Process Narrative

Process Step/Decision/Record	Description
O10 Business Continuity Management	**An operational process which encompasses the steps required to restore business processes following a disruption, while continuing to provide product or services to the customer. It includes steps often described as Disaster Recovery.**
O4 Incident Management **O5 CAPA**	Operational processes that may lead to the invoking of Disaster Recovery and the BCP are **O4 Incident Management** and **O5 CAPA**.
O10.1 BCP	The BCP will be prepared and available for reference throughout the process.
O10.2 Crisis Committee criteria met?	A review should be performed after the initial reporting of the incident to ensure that situation meets the criteria for reporting to the Crisis Committee.
O10.3 Crisis Committee Kick-off Meeting	A kick-off meeting of the Crisis Committee will be held. The situation will be reviewed by the Committee.
O10.4 Is Situation a Crisis?	The Crisis Committee will evaluate the incident and ensure the situation meets the criteria of a crisis if the BCP is invoked.
O10.5 Invoke BCP	The BCP will be invoked according to the instructions contained in the document.
O10.6 Communication of Crisis Situation and Progress	Communication of the crisis situation and progress reporting should be conducted according to the BCP or related SOP.
O10.7 Monitor Progress	Throughout invoking the BCP, the Crisis Committee will monitor the progress of the BCP.
O10.8 BCP Progress Conforms?	The progress of events against the BCP deliverables and timings will be assessed by the Crisis Committee to determine if it is acceptable to the regulated organization.
O10.9 Fail-Over to Alternative Business Process?	If progress against the BCP is acceptable or if a revised BCP has been invoked, the decision should be taken regarding whether a Fail-Over should be conducted to the new business processes. This may include reverting to new systems or physically moving locations.
O10.10 Fail-Over/DR Plans/ Instructions	The steps required for Fail-Over should be outlined in a detailed set of instructions. For IT applications, the specific instructions associated with an application may be contained in a DRP or procedure.
O10.11 Execute Fail-Over to Alternative Business Process	The Fail-Over to alternative business processes will be executed according to the relevant Fail-Over/Disaster Recovery Instructions. Fail-Over may include system restoration activities.
O7 Repair Activity **O9 Backup and Restore**	Where relevant as outlined in the Fail-Over/Disaster Recovery Plans/ Instructions, **O7 Repair Activity** and **O9 Backup and Restore** may be invoked when failing-over to the new business process.
O10.12 Fail-Over/DR Test Protocols	Fail-Over or Disaster Recovery Test Protocols should be prepared and available for execution to ensure the failed-over or recovered processes are functioning correctly and according to specifications.
O10.13 Conduct Fail-Over Testing on Alternative Business Process	Testing of the Fail-Over should be conducted on the alternative business processes according to the procedures specified in the Fail-Over Test Protocols.

14.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O10.14 Fail-Over/DR Test Evidence	Test evidence will include the executed test protocol with approval signatures from the tester and peer reviewer, as appropriate. If deviations have been encountered during the testing, these should be resolved and appended to the test results.
O10.15 Fail-Over Successful?	The Fail-Over must be successful before the re-establishment with normal/ new production. If Fail-Over was not successful during a real BCP situation, go to O10.19. If Fail-Over was not successful during a Disaster Recovery Test exercise, go to O10.26 Once the Fail-Over has been deemed successful, normal/alternative production can be re-established. If manual work has been undertaken while an automated system has been unavailable, the input of manual data will need to be addressed when the automated production resumes.
O10.16 Re-establish Normal/ Alternative Production	Normal or alternative operation is re-established.
O3 Performance Monitoring **O6 Operational Change and Configuration Management**	**O3 Performance Monitoring** and **O6 Operational Change and Configuration Management** should be used to control the process of the normal or an alternative system for acceptance and release.
Training	The support process **Training** may be used to control the process of the normal or an alternative system for acceptance and release.
O10.17 Fail-Back Required?	Does the system need to be failed-back to its original state? This is appropriate if the Fail-Over has been executed to temporary systems or locations. If 'yes,' the flow returns to step O10.11.
O10.18 Not BCP situation	The incident or situation does not meet the criteria of a crisis and the BCP does not need to be invoked. The incident should be managed according the relevant Operational processes: **O4 Incident Management** or **O5 CAPA**.
O10.19 Crisis Committee Evaluate Situation	From step O10.8: If the BCP process is not conforming to the activities specified in the BCP plan, the Crisis Committee will evaluate the situation and reasons for non-conformances.
O10.20 Proposition and Preparation of Alternative Solution	The Crisis Committee will prepare alternative solutions.
O10.21 Revised BCP	The BCP should be revised according to the solutions put forth by the Crisis Committee.
O10.22 Invoke Revised BCP	The revised BCP will be invoked according to the instructions contained in the document.
O10.23 BCP Test Planning	If **testing** the BCP, this is the starting point for the test exercise.

14.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O10.24 DR Test Planning	If **testing** the Disaster Recovery Plan, this would be the starting point for the test exercise. DRP is a subset of BCP and normally involves the recovery of IT applications or infrastructure.
O10.25 DR Test Exercise Protocol	A Disaster Recovery Test Exercise Protocol should be prepared, reviewed, approved prior to the execution of the disaster recovery test.
O10.26 Proposition and Preparation of Alternative Solution	If the Fail-Over has not been successful during the Disaster Recovery test exercise, the relevant parties should propose and prepare alternative solutions.
O10.27 Revised DR Test Exercise Protocol	After an alternative solution has been proposed and prepared, the Disaster Recovery Test Exercise Protocol will be updated to reflect the new solution.
O10.28 Normal Situation	Following successful DR or execution of the Business Continuity Plan, the business will be informed that normal operating conditions have been restored.
O10.29 BCP/DR Report	Following the return to normal business, the results of the BCP, BCP test, or DR test will be reported.
O10.30 Process Review	The BCM process should be subject to internal review to ensure it remains effective and aligned with business needs.

14.6 Procedural Guidelines and Considerations

14.6.1 Business Continuity Plan (BCP)

Overview

A Business Continuity Plan should be prepared and available for reference throughout any crisis. The BCP will be invoked according to the instructions contained in the document.

The BCP should be subject to independent business/technical review and approval and other reviews and approvals dependent upon the scope and nature of the system, department, or site.

The BCP should be written on a business process level and contain the following information:

- event/disaster scenarios
- Business Continuity strategies, including:
  - selection of alternative strategies for recovery/Fail-Over
  - specification of business process Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO):
    > Recovery Point Objective (RPO) – the point in time to which data must be restored following a failure or disaster loss, e.g., a restore to the previous night's back up will not include today's transactions – is this acceptable?
    > Recovery Time Objective (RTO) – the time within which the business process must be restored following a failure or disaster.

- immediate steps to be taken to minimize further impact
- interim processes required to manage disruptions
- prioritization for system restore in the event that the disruption involves failure/unavailability of multiple systems
- where manual processes are involved to allow the business to continue to operate, how any associated electronic records/data will be synchronized once the electronic systems have been restored
- where recovering from a disaster, how any records (data, system changes, configuration changes) will be reinstated since the last backup

• required personnel and responsibilities, including:

- Key Contacts, e.g., Process Owner, System Owner, Suppliers, Quality Unit should be listed with their contact details.

• Crisis Committee

- criteria for reporting to the Crisis Committee
- representatives:
  > Chair (e.g., Process Owner)
  > the parties involved in the Crisis Committee Kick-off Meeting
  > The core Crisis Committee should include representatives from areas of the business, such as Environmental, Health and Safety, Security, Utilities, Engineering, HR/Communications.
  > Depending on the nature of the crisis, other Technical Advisors may be required at the meeting, such as representatives from Production, IT, Laboratories, Facilities, etc.

• criteria for a crisis and invoking the BCP

• stage timings and escalation process:

- Define the maximum allowable time to conduct evaluations and key activities in the Disaster Recovery and Business Continuity Management process before escalation occurs.
  > For example, the BCP should define the maximum length of time that the Crisis Committee is allowed to evaluate the incident to ensure the situation meets the criteria of a crisis. If the maximum time is exceeded and the Crisis Committee is not able to reach a decision, the Crisis Committee should declare the incident a crisis and the next stage of the process is invoked.
- A description of the escalation process and responsibilities

• progress tracking

• communication of the crisis situation and progress reporting

The BCP should be periodically reviewed to keep it aligned with business imperatives and all references to roles/ personnel should be kept up to date.

A copy of the BCP should be held in a secure location that can be accessed in the event of a disaster.

14.6.2 Considerations for DR and BCP

An Impact Assessment should be conducted to determine the potential business impact from computerized system failure and subsequent computerized system outage.

For each computerized system, the types of service failure should be reviewed:

- loss of access to system (e.g., fire, physical destruction)
- degradation of service performance
- loss of data
- loss of data integrity and confidentiality

For each failure, consider the potential risk from the failure, e.g.:

- health, safety, and environment
- regulatory or legal compliance
- business operation

When considering the potential risks, consideration should be given to the consequence of prolonged failure.

The potential threats (including likelihood) to the computerized system should be considered:

- human error/accident
- fire/flood/earthquake/other adverse natural event
- power/electrical failure
- failure to comply with policies and procedures
- accident
- software or hardware failure
- system/component obsolescence
- removal/loss of media (disk, memory stick, mobile device)
- deliberate malicious acts – sabotage/hacking/theft/terrorism

The Business Continuity Strategy should consider measures for minimizing the threats and vulnerabilities to the computerized system and also Recovery Mechanisms.

Potential risk reduction mechanisms include:

- review appropriateness of backup and recovery procedures

- review of security controls
- review of the long term viability of the system
- failure and backup systems, e.g., Uninterruptable Power Supplies, Standby systems, etc.
- avoiding single supplier agreements
- failure detection systems, e.g., infrastructure failure alerts, hardware failure alarms, system diagnostics

Potential recovery options include:

- recovery of data and software from backup and archive
- recovery of systems and software from configuration management records
- use of other available systems (e.g., laboratory systems, products systems, etc.)
- for high criticality systems, the option of a redundant (parallel system)
- identification of critical spares (including obsolete items if necessary)
- reconfiguring network access
- using manual processes until computerized systems re-established
- relocating essential personnel and their required resources to other on site or off site premises
- consideration of system replacement

14.7 Records and Record Content

14.7.1 Fail-Over/Disaster Recovery Plans/Instructions

The steps required to Fail-Over or recover the system should be outlined in a detailed set of instructions. For IT applications, the specific instructions associated with an application may be contained in a Disaster Recovery plan or procedure.

Although the information to be contained in a Fail-Over or Disaster Recovery Plan will be dependent upon a system, the following information should be considered:

- Principle
- Scope
- Responsibilities
- Procedure:

  - recovery – instructions, interdependencies, and pre-requisites to recover:
    - > hardware (servers, workstations, handheld/mobile devices, etc.)

  - > software (operating systems, applications, databases, patches, service packs, etc.)
  - > data
  - > communication plan
- configuration changes
- synchronization (environments, databases, etc.)
- post recovery checks
  - > Fail-Over/Disaster Recovery Test Protocols to be executed
  - > evidence to be collected
- acceptance and release:
  - > communication plan

14.7.2 Fail-Over/Disaster Recovery Test Protocols

For critical processes, Fail-Over or Disaster Recovery acceptance testing criteria should be understood, and where appropriate, test protocols should be prepared and available to ensure that the failed-over or recovered process is functioning correctly and according to specifications.

Protocols should be subject to independent business/technical review and approval, along with other reviews and approvals dependent upon the scope and nature of the system, department, or site.

For further information, see the GAMP® Good Practice Guide: Testing of GxP Systems (Reference 8, Appendix 4).

If an alternative Fail-Over disaster recovery solution has been identified during the Business Continuity Management testing Process, the Fail-Over/Disaster Recovery Test protocol should be updated, reviewed, and approved to reflect the new solution.

14.7.3 Fail-Over/Disaster Recovery Test Evidence

Fail-Over/Disaster Recovery test evidence will be generated as a result of the execution of test protocols. Evidence will include the executed test protocol with approval signatures from the tester and peer reviewer as appropriate. If deviations have been encountered during the testing, these should be resolved and appended to the test results.

Executed test protocols should be available for inspection.

Test protocols should be executed according to good testing practice.

Executed protocols should be approved before acceptance and release of the new system.

14.7.4 Disaster Recovery Test Exercise Protocol

A Disaster Recovery exercise should be conducted according to the procedure specified in a Disaster Recovery test exercise protocol. Protocols for the DR exercise should be prepared and available for execution to ensure the failed-over process is functioning correctly and according to specifications.

Protocols should be subject to independent business/technical review and approval, along with other reviews and approvals (e.g., Quality Unit) dependent upon the scope and nature of the system, department, or site.

Protocols should be prepared, reviewed, and approved prior to the execution of the disaster recovery test exercise. The following information should be considered in the DR test exercise protocol:

- Scope and Objectives
- Method – including Disaster Scenario
- Logistics and Requirements, including:
  - location and exercise dates
  - date of the disaster
  - preparations for the exercise
  - facility
  - hardware and network requirements
  - data restoration and backup media
  - data deletion
  - participants and contact information
- Timetable
- Testing
- Reporting

For further information, see the GAMP® Good Practice Guide: Testing of GxP Systems (Reference 8, Appendix 4).

If an alternative Fail-Over solution has been proposed during the exercise, the Disaster Recovery Test protocol should be updated, reviewed, and approved to reflect the new solution.

14.7.5 BCP/DR Report

A communication to the Business should be sent out immediately after the successful resolution of the disaster to state that normal service is resumed.

Following the return to normal business, the results of the BCP, BCP test, or DR test should be reported. The report should include all findings, deviations, lessons learnt, and recommended changes to the BCP. The content of the BCP/DR report should be communicated to affected stakeholders.

If, as a result of recommendations in the report, the BCP is changed, it should be re-tested to ensure that the changes work as intended and do not cause unexpected affects elsewhere.

14.7.6 Periodic Review Considerations

For all Systems:

- determine if a Disaster Recovery plan is required and established
- determine if a Disaster Recovery testing schedule has been established
- determine if Disaster Recovery testing has been carried out according to the schedule

For Medium/High Impact Systems:

- review records and corrective actions

14.8 Scalability

The scalability or rigor of the Disaster Recovery and Business Continuity Management process depends on System Impact. For an example see Table 14.2. This example is intended to be illustrative only, and not definitive.

Table 14.2: Rigor of the Disaster Recovery and Business Continuity Management

	Disaster Recovery	Business Continuity Management
Low Impact System	DR Plan, DR Instructions (Back-Up and Restore) available, Disaster Recovery test frequency and type based on risk	No action
Medium Impact System	DR Plan, DR Instructions available, DR Test protocols available, Disaster Recovery test frequency and type based on risk	System included in BCP
High Impact System	DR Plan, DR Instructions available, DR Test Protocols available, Disaster Recovery test frequency and type based on risk	System included in BCP, Event/Disaster Scenarios Considered, Fail-Over Options Considered

The frequency of Disaster Recovery testing for a system should be risk-based and take account of business and technological changes.

Disaster recovery test types also should be chosen based on risk, and consider the criticality and complexity of the system.

Various disaster recovery test methods are available, including:

- Paper Test: This is a paper walk through of the plan that involves key personnel in the plan's execution. During the exercise, personnel involved should work out what may happen in a particular type of service disruption. This may involve a walkthrough of the entire plan or just a portion of the plan. A paper test usually precedes a parallel test.
- Parallel Test: This type of test usually involves a local version of a full test where actual resources are used in the simulation of a disaster. Parallel tests are performed regularly on different aspects of the BCP and can be a cost-effective way to gradually obtain evidence about how effective the plan is. It also provides a means to improve the BCP in increments.
- Full Operational Test: This is one step away from an actual service disruption. The organization should have thoroughly tested the plan on paper and locally as a parallel test (i.e., within an equivalent, but non-operational environment) before endeavoring to completely shut down operations.

15 Security Management

15.1 Introduction

The Security Management process defines the controls required for securing a computerized system in an operational environment. The process ensures that all activities, controls, and documentation required for security of the system have been defined and ownership has been identified.

Security procedures should be periodically verified to ensure that the security system is appropriate to meet organization policy and regulatory compliance requirements.

This section is related to Appendix O11 of GAMP® 5 (Reference 7, Appendix 4).

See GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Reference 8, Appendix 4) for further details on Infrastructure Security. See also ISO 17799 (Reference 4, Appendix 4) for further details on information security management.

15.2 Scope

The primary function of Security Management is to protect the safety of information. The levels of protection applied are dependent upon the value of the information with respect to confidentiality, integrity, and availability. Security management involves physical, logical, technical, and procedural controls to ensure that only authorized users and administrators perform permitted activities that ensure the confidentiality, integrity, and availability of both system and data is assured.

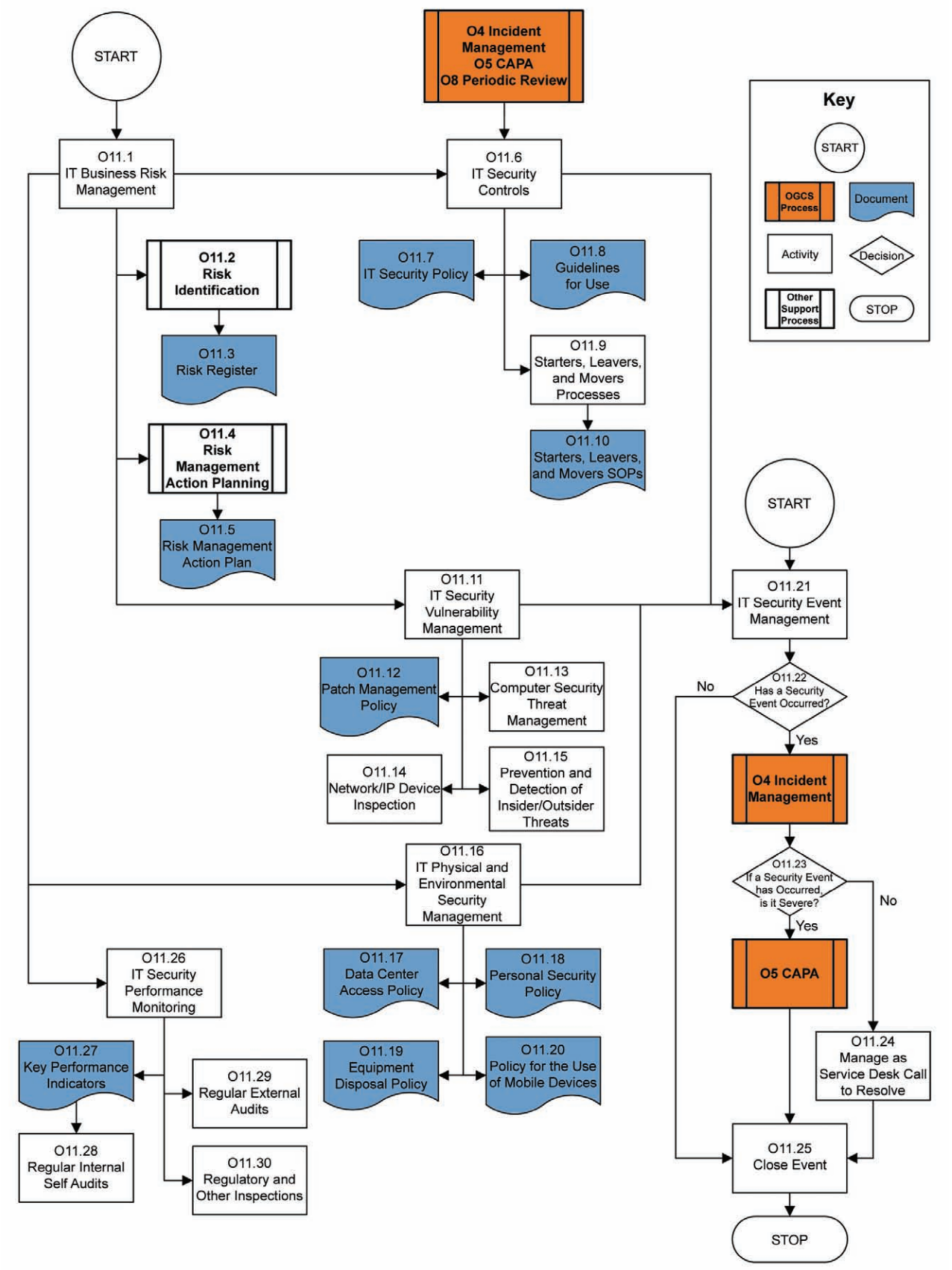
15.3 Roles and Responsibilities

Table 15.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 15.1: Roles and Responsibilities for Security Management

Role	RACI Role	Responsibilities
Process Owner	R	• responsible for maintaining the security of the system
System Owner	A	• accountable for the security management of the system • may coordinate with dedicated IT Security Management, covering areas such as: - evaluating system architecture - user account structure - encryption needs - firewall issues - hardware redundancy aspects - data transmission procedures - patch management procedures - system monitoring
End User	R	• responsible for following usage policies and security procedures to maintain the security of the system
Quality Unit	C	• needs to be consulted during policy developments and changes to the system
Platform Support (SME)	R	• responsible for maintaining the security of system platforms
Application Support (SME)	R	• responsible for maintaining the security of system applications
System Administrator (SME)	R	• responsible for maintaining the security of system administration
Supplier	I	• will need to be informed if there are security issues related to the product or system itself • should comply with any relevant IT security management and procedures
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

15.4 Security Management Process Flow Diagram



15.5 Process Narrative

Process Step/Decision/Record	Description
O11 Security Management	**An operational process which defines the controls required for securing a computerized system in an operational environment. The process ensures that all activities, controls, and documentation required for security of the system have been defined and ownership has been identified.**
O4 Incident Management **O5 CAPA** **O8 Periodic Review**	Other operational processes which may trigger Security Management activities
O11.1 IT Business Risk Management	Information security failures can significantly affect business activities and reputation; therefore, organizations should integrate information security with their risk management processes.
O11.2 Risk Identification	A process for risk identification should be defined. The IT department should work close with Business Risk Team to integrate information risk management into their overall risk management activities.
O11.3 Risk Register	A file that holds all information on identifying and managing a risk
O11.4 Risk Management Action Planning	Implementing a risk driven Information Security Policy
O11.5 Risk Management Action Plan	The output of the Risk Management Action Planning activity
O11.6 IT Security Controls	The organization should determine the optimum way of implementing information security. A modeling process may be followed to derive the optimal set of attributes which accompany information security controls.
O11.7 IT Security Policy	The content of the Information Security Policy will be driven by several factors, a key one of which is risk and subsequently how much risk the organization is willing and able to take. Any effective information security policy should aim to: • Reduce the risk of security incidents • Minimize the effect (or cost) of security incidents • Establish the fundamental rules under which an organization should operate its information systems The Information Security Policy should apply to personnel and contractors. Some parts of the policy will be observed only by persons with a specific job function, e.g., the System Administrator; other parts will require compliance by all personnel. The policy should address controls for granting temporary access to the organization's systems (i.e., for support calls and visits etc). A requirement to comply with the organization's Information Security Policy should be incorporated into both Terms and Conditions of Employment and Job Descriptions. The Information Security Policy will act as the final reference point for any compliance audits.

15.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O11.8 Guidelines for Use	While the Information Security Policy is mandatory, a **Guideline for Use** is a suggested action or recommendation to address a specific area of the policy. Guidelines are considered Best Practice and should be implemented when possible. A guideline typically uses words like 'should' or 'may' in the definition. Guidelines are usually written for a particular environment and are used to help guide users' actions. Guidelines for use will usually supplement the Procedures Manuals with adoption encouraged and promoted rather than enforced.
O11.9 Starters, Leavers, and Movers Processes	These are critical security management processes if the control of user access and permissioning is to be effective and timely. For further information, see Section 15.6.1 of this Guide.
O11.10 Starters, Leavers, and Movers SOPs	The controlling procedures for the security management processes associated with new starters, leavers, and internal transfers within the organization
O11.11 IT Security Vulnerability Management	Vulnerability management is a process that can be implemented to make IT environments more secure and to improve an organization's regulatory compliance. Intellectual property, such as research information or 'trade secrets,' such as manufacturing recipes, provide clear business justification for adequate controls to be established. **Policy** definition is the first step and includes defining the desired state for device configurations, user identity, and resource access. **Baseline** the environment to identify vulnerabilities and policy compliance. **Prioritize** mitigation activities based on external threat information, internal security posture and asset classification. **Shield** the environment, prior to eliminating the vulnerability, by using desktop and network security tools. **Mitigate** the vulnerability and eliminate the root causes. **Maintain** and continually monitor the environment for deviations from policy and to identify new vulnerabilities.
O11.12 Patch Management Policy	The IT department should establish a patch management policy. The goal of Patch Management is to maintain the components installed on the network (hardware, software, and services) up to date with the latest patches and updates, while avoiding any additional risks to system and data security. The network components covered in Patch Management may include: • computers • servers • software • peripherals • routers, switches, and wireless devices • services such as messaging, database, MIS and file storage For more information on this topic, see GAMP® 5 Appendix S4: Patch and Update Management

15.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O11.13 Computer Security Threat Management	The preventive/proactive work connected to identifying and avoiding possible threats before they occur. Establishing processes for managing computer originated threat by applying policies, such as administrative lock down, disk encryption, log on passwords, etc.
O11.14 Network /IP Device Inspection	Security configuration management and policy compliance tools provide a top-down baseline of the IT environment in relation to an organization's defined security configuration policies. An organization can define its 'gold-standard' environment, i.e., the desired state of system configurations and access rights, or it can use a predefined set of best-practice system security configuration templates. Network tools are available that can be used to inspect and audit devices on the network for compliance.
O11.15 Prevention and Detection of Insider/Outsider Threats	To prevent and detect the occurrence of internal and external threats, the following steps may be implemented: • Institute periodic employee security awareness training for all personnel. • Enforce separation of duties and least privilege. • Implement strict password and account management policies and practices. • Log, monitor, and audit employee online actions. • Use extra caution with system administrators and privileged users. • Actively defend against malicious code. • Use layered defense against remote attacks. • Monitor and respond to suspicious or disruptive behavior. • Deactivate computer access following termination. • Collect and save data for use in investigations. • Implement secure backup and recovery processes. • Clearly document insider threat controls.
O11.16 IT Physical and Environmental Security Management	Effective physical security measures help protect against unauthorized access, willful, or accidental damage, or loss of data in areas where critical or sensitive information is prepared or located (including operational areas), or where information processing services supporting key business processes are hosted. The requirements and placement of each physical security barrier should depend upon the value of the information with respect to confidentiality, integrity, and availability. Each level of physical protection should have a defined security perimeter, around which a consistent level of physical security protection is maintained. Managers responsible for sensitive information or for information processing resources should periodically perform a self-assessment to determine the existing level of security vulnerability and compliance with the physical security requirements.

15.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O11.17 Data Center Access Policy	A policy should be established relating to Data Center Access. It is the responsibility of the appropriate individuals to enforce appropriate entry controls and authentication procedures that ensure that only authorized personnel are allowed entry into areas that house critical or sensitive information or information processing resources that host the processing of critical or sensitive information (i.e., Data Center). Facilities where access by unauthorized personnel is to be prevented must, at a minimum, require that ID badges are worn and visible at all times. Personnel should be encouraged to challenge strangers and report their presence to local security personnel. Visitors should be escorted. Physical access to secured areas should be controlled. The award and distribution of keys or passes (including ID badges, card/pass keys) used to physically access secure areas should be strictly controlled and subject to frequent review to ensure that only currently authorized individuals are in possession of access devices. Regular, e.g., quarterly reviews should be performed to ensure that only individuals with a job related need have access to the computing facilities. Whenever individuals change jobs or leave, their access cards should be removed from the card key access system.
O11.18 Personal Security Policy	Achieving a secure environment is facilitated if employees practice good personal security according to a defined policy, e.g., keeping passwords safe and secure and appropriate use of electronic signatures. Organizations also should encourage employees to practice a clear desk policy for papers and diskettes or other media that are sensitive in nature, in order to reduce the risks of unauthorized access, loss of and damage to information outside of normal working hours.
O11.19 Equipment Disposal Policy	A policy should be established for the secure disposal of equipment. All equipment containing storage media, e.g., fixed hard drives, hand-held and mobile devices, Blackberries, memory sticks, etc., should be checked to ensure that any classified and personal information and licensed software are removed or over written prior to disposal in order to prevent identity theft or other unwanted intrusion. Minimum guidelines should be established for removing (‘wiping’) the hard drive of computing equipment. If this is contracted to a supplier, the operation should be reviewed and verified.

15.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O11.20 Policy for the Use of Mobile Devices	Security Policies for Information Processing Equipment in Public Places or Off-Premises should be established. Virus controls should be enabled to protect organization resources. Information processing equipment and media containing highly restricted and confidential data should not be left unattended in public places. Portable computers containing sensitive data should be carried as hand luggage when traveling. Off premises computers with organization classified information should be protected with an appropriate form of access protection, e.g., passwords, smart cards, or encryption, to prevent unauthorized access. Manufacturers' instructions regarding physical protection of equipment should be observed at all times. Security risks (e.g., of damage, theft, eavesdropping) vary considerably between locations and should be considered in determining the most appropriate security measures.
O11.21 IT Security Event Management	The management of any event which appears to be a breach of an organization's information security safeguards, according to the relevant policy and guidelines It is important to respond calmly and to follow a logical process, first to prevent the breach from continuing, if possible, and second, to inform the appropriate person(s) within the organization; this usually includes the appointed IT security representative or service desk.
O11.22 Has a Security Event Occurred?	Identify whether the event constitutes a security violation. If not, it can be recorded and closed out.
O4 Incident Management	If a security event has occurred, **O4 Incident Management** is invoked to investigate and identify the necessary actions for resolution.
O11.23 If a Security Event has Occurred, is it Severe?	If the incident is determined to be a genuine security event, a risk assessment should identify any threats to business assets and the potential effect of such threats. Such analysis should quantify the value of the business assets being protected to decide on the appropriate level of safeguards.
O5 CAPA	Although not directly triggered by the incident, **O5 CAPA** is invoked to identify corrective actions to mitigate the security threat and preventive actions to ensure no reoccurrence. Other operational and support processes also may be triggered.
O11.24 Manage as Service Desk Call to Resolve	If the event has been classified as not being severe,manage it as a Service Desk call through to resolution and closure.
O11.25 Close Event	Close out the event.
O11.26 IT Security Performance Monitoring	The objective of information security policy is to provide the appropriate level of protection to the organization's information resources. High level processes should be established to monitor, review, and report on the efficiency and effectiveness of the overall IT Business Risk Management approach.

15.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O11.27 Key Performance Indicators	Key Performance Indicators (KPIs) for Information Security should be established for critical processes.
O11.28 Regular Internal Self Audits	The IT department or appropriate 'compliance' function should regularly check if information security policy, processes, and infrastructure are effective. The output from these audits may inform the results of **O8 Periodic Review**.
O11.29 Regular External Audits	Independent audits by suitably qualified personnel/organization should be performed to confirm that the Information Security Policy, Processes, and Infrastructure have been established and are being consistently adhered to and applied.
O11.30 Regulatory and Other Inspections	Regulatory inspectors will expect an effective Information Security Management System to be implemented within an organization and that adequate controls are established for access and use of critical systems. Records and logs arising from the application of the security policy and associated procedures should be available for inspection and review. Regulatory inspectors also may be looking for evidence of 'challenge testing' of security controls.

15.6 Procedural Guidelines and Considerations

15.6.1 Starters, Leavers, and Movers Procedures

The controlling procedures for the security management processes associated with new starters, leavers, and internal transfers within an organization could follow the processes described in this section of the Guide. Where the IT and Personnel departments are not responsible for these processes, there should be a mechanism for cross-departmental notification to ensure that any non IT managed access privileges are added, transferred, and revoked as required.

New Starters Process

- The process should be initiated by the Personnel Department upon receipt of a signed contract of employment from new personnel. The IT department should be formally notified of their name and start date, and the name of their Manager.
- The IT department should document the action, preferably in a Service Desk database system. A call is logged within a Service Desk database system for the purpose of recording and monitoring all details. Details, such as the reference number of the Service Desk call, should be supplied to the Personnel Department and the Managers of new personnel.
- The IT department should send the Managers of new personnel a Starters IT Questionnaire. The Starters IT Questionnaire should be completed within agreed time frames.
- New personnel should attend an IT induction training – where appropriate the starter receives training and a documented assessment regarding the appropriate use of electronic signatures.

Leavers Process

- The process should be initiated by the Personnel Department upon receipt of the leaver's letter of resignation. The IT Department should then be formally notified – with details such as name, leave date, manager's name.

- The IT department should document their actions, preferably in a Service Desk database system. A call is logged within a Service Desk database system for the purpose of recording and monitoring all details. The reference number of the Service Desk call should be supplied to the Personnel Department and the Leaver's Managers.

- The IT department complete their tasks on the leaver's "leave date" – such as disabling accounts including all access privileges.

Movers (Internal Transfers) Process

- The process should be initiated by the Personnel Department upon receipt of the signed contract of employment from an existing Company member denoting a transfer of department. The IT Department should be formally notified – with details, such as name of the Company member, Transfer date, Previous Manager and Previous Department name, New Manager and New Department name.

- The IT department should document the action preferably in a Service Desk database system. A call is logged within a Service Desk database system for the purpose of recording and monitoring all details. Details such as a reference number of the Service Desk call should be supplied to the Personnel Department, the Mover's Previous Managers, and New Manager.

- The IT department complete tasks for the transferring Company Member on "Move date" – such as changing and disabling accounts including removal and modification of access privileges as appropriate.

15.7 Records and Record Content

Organizations should develop, maintain, and document an internal security plan to include data integrity, authentication, recovery, and continuity of operations that support administrative data.

Procedures should be established that ensure that access to data and applications is secured, as required.

Operational controls that ensure data protection should be adequately documented.

Records related to the security management operational process include:

- Information System Security Standards
- System Security Controls and Policies
- New Starters List
- Leavers List
- Internal Transfers List:
  - including contractors where relevant
- List of Active Users (network and system)
- User Permissions Matrix (system)
- Evidence that access has been modified when employees terminate or transfer (system log or audit trail)
- Patch Management Policy

- Data Center Access Policy
- Personal Security Policy:
  - Communicating appropriate use and consequences of misuse to users who access the systems or data
- Equipment Disposal Policy
- Policy for the use of Mobile Devices
- Log of security incidents:
  - may be a subset of the incident log
- Security administration records:
  - security violation reports – with evidence of investigation and follow-up
  - ensuring LAN and workstation integrity through virus protection measures and policies
- Where appropriate, Record Access and Use Procedures
- Audit Reports

15.8 Scalability

This section provides an example approach to scalability. This example is intended to be illustrative only, and not definitive.

System Impact is assigned as high, medium, or low using the methodology described in GAMP® 5 Appendix M3 (Reference 7, Appendix 4).

Security Risk is assigned by consideration of the need for confidentiality, integrity (accuracy and completeness), and availability of data within the system.

Plot System Impact versus Security Risk to determine the necessary level of security.

Table 15.2 Example Approach to Scalability for Security Management

		Security Risk		
		Low Security Risk	**Medium Security Risk**	**High Security Risk**
System Impact	**Low Impact System**	L	L	M
	Medium Impact System	L	M	H
	High Impact System	M	H	H

Where:

L = Low Security Level

M = Medium Security Level

H = High Security Level

Essential elements of the system should be captured during the assessment and categorization of the levels of security; otherwise, the resulting system may not be adequately controlled. This may increase the risk to the security of data.

Where feasible, Security Management should be implemented with technical controls. Manual systems may not be as easily kept up to date or can be easily bypassed, particularly if there is a significant overhead involved.

16 System Administration

16.1 Introduction

The System Administration process defines the controls required for the performance of low risk activities and is intended to ensure that:

- Standard, routine, and repetitive tasks are performed in the most effective way and with the appropriate level of review and approval.
- Required tasks are completed and necessary records maintained.
- Review procedures are established.

This section is related to Appendix O12 of GAMP® 5 (Reference 7, Appendix 4).

16.2 Scope

A distinction is made between System Administration and other Operational processes. The System Administration process is intended for standard 'routine and repetitive' and 'on demand' tasks, such as user administration, system maintenance, and monitoring activities relating to the use and maintenance of laboratory, process, and IT systems.

The System Administration process has been introduced to allow a risk-based approach to be adopted by regulated organizations. Low risk tasks can be completed according to standard procedures and where appropriate, evaluated against established SLAs without recourse to review and approval of each task by the Quality Unit. For such tasks, quality is assured by audit and periodic review processes. Where there is a potential GxP impact, these standard procedures should be subject to Quality Unit review and approval; this review also should consider the suitability of a support process for that system to be covered by a standard procedure.

Tasks are only performed using the System Administration process where controlling procedures are established and the risk to do so has been evaluated and is deemed as acceptable. Therefore, it is the responsibility of the regulated organization to determine which tasks are to be performed through the System Administration process by the application of Quality Risk Management or equivalent processes.

Operational Change Control and Configuration Management are not considered to be System Administration tasks – although a System Administrator may be significantly involved in these processes.

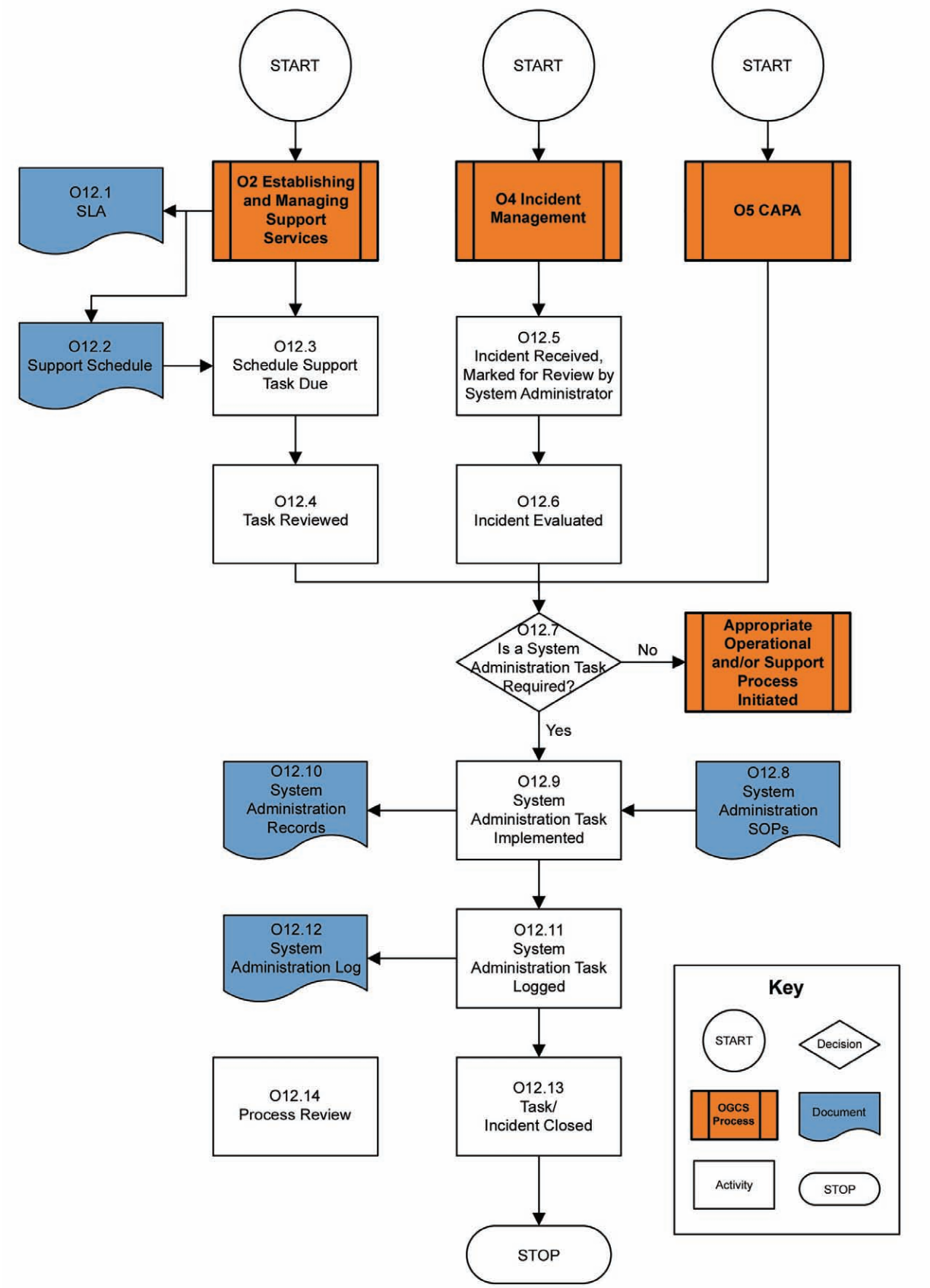
16.3 Roles and Responsibilities

Table 16.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 16.1: Roles and Responsibilities for System Administration

Role	RACI Role	Responsibilities
Process Owner	C	• may be consulted during execution of some System Administration tasks
System Owner	A	• owns the System Administration process • accountable for maintaining the System Administration process according to agreed SLAs
End User	I	• raises requests for support tasks to be performed • is informed about the outcomes of requests
Quality Unit	C	• is consulted during establishment of System Administration process on regulatory and compliance aspects
Platform Support (SME)	C	• is consulted by System Administrator during execution of some System Administration tasks
Application Support (SME)	C	• is consulted by System Administrator during execution of some System Administration tasks
System Administrator (SME)	R	• responsible for the execution of System Administration tasks
Supplier (SME)	R	• responsible for the execution of System Administration tasks if contracted to do so
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

16.4 System Administration Process Flow Diagram



16.5 Process Narrative

Process Step/Decision/Record	Description
O12 System Administration	**An operational process relating to provision of administrative support for a system, including performance of standard administration tasks.**
O2 Establishing and Managing Support Services	An operational process that results in the provision of System Administration resource and definition of scope of System Administration responsibilities
O12.1 SLA	Records the scope of work for System Administration tasks and will contain agreed support performance targets.
O12.2 Support Schedule	An output from the SLA may be a schedule of regular administration tasks – these may be daily, weekly, monthly, or any standard tasks required at defined intervals.
O12.3 Scheduled Support Task Due	A regular standard task is due for execution.
O12.4 Task Reviewed	The System Administrator reviews the scheduled task.
O4 Incident Management	An operational process for the logging and escalation of incidents.
O12.5 Incident Received, Marked for Review by System Administrator	The System Administrator receives the incident from the Incident Management process – this may be via the Service Desk or direct from the user and may be received via an electronic support management system, via a notification e-mail, by telephone, or by other means. All calls should be logged.
O12.6 Incident Evaluated	The System Administrator evaluates the incident.
O5 CAPA	A request for a System Administration task comes directly from **O5 CAPA**.
O12.7 Is a System Administration Task Required?	The System Administrator reviews the scheduled task/evaluates the incident to determine if the resolution is covered by a standard System Administration task. • If 'yes,' the resulting actions are controlled by a standard System Administration procedure. • If 'no,' the resolution to the incident will require the initiation of another operational process, e.g., **O6 Operational Change and Configuration Management**. • In exceptional cases, the task may not be performed or a different task may be required. Deviation from the expected action should be documented with a suitable justification.
Appropriate Operational and/ or Support Process Initiated	If the required actions are not in the scope of defined System Administration tasks, the System Administrator initiates the appropriate operational and or support process.
O12.8 System Administration SOPs	The System Administrator references the controlling procedures required to execute the task as appropriate.
O12.9 System Administration Task Implemented	The System Administrator initiates the appropriate System Administration process.
O12.10 System Administration Records	Records generated by the execution of System Administration tasks – as defined in the System Administration SOPs.
O12.11 System Administration Task Logged	On completion, the Administration Task is logged as complete - where appropriate the requestor should be informed.

16.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O12.12 System Administration Log	A record of completion of System Administration tasks.
O12.13 Task/Incident Closed	The Administration task is complete, the Incident can be closed.
O12.14 Process Review	The process is reviewed by the System Owner in order to establish that it is under control and that performance is consistent with SLA targets.

16.6 Procedural Guidelines and Considerations

16.6.1 The System Administrator Role

Typically for an automated system, there will be differentiation of responsibilities between the users of the system and the support function. The person that is charged with the provision of the 'everyday' support for the system is the **System Administrator** and this system support role is termed **System Administration**.

Once operational processes are established and appropriate resource is in place the users of the system will require support to be provided. The interface between the users and the support function is primarily via the **O4 Incident Management** process.

An important part of the support function is also the 'functional support' of the system, as incidents and problems may relate to erroneous use of the system, and the handling of these cases should be supported by experts in the functionality of the system and not technical experts. Many incidents will be related to the 'everyday' use of the system and will be easily resolved by the provision of appropriate advice or by the execution of standard administrative tasks. These standard tasks can be distinguished as either 'routine and repetitive' or 'on-demand.'

Additionally, there may be support activities defined in the **SLA**, which requires routine administrative tasks to be performed and logged.

For a large system, there may be several layers of support and a **System Administrator** function may be provided at each level, e.g., application, server, database, network, etc. For global systems, there may be system administration or equivalent roles at local, regional, and global levels as appropriate to the system. See the GAMP® Good Practice Guide: Global Information Systems Control and Compliance (Reference 8, Appendix 4) for more information on Administration of a global system.

16.6.2 System Administration Tasks

All standard system administration tasks should be identified, documented, and be supported by controlling procedures. System Administrators should be trained to perform these tasks and evidence of their competency retained.

Any activities relating to the system which are not covered by standard procedures should be subject to the operational change management/change control process for the organization. For further information, see Section 10 of this Guide.

Typical System Administration tasks include:

Task	Comment
Infrastructure	
Infrastructure Administration Tasks	• allocation/re-allocation of disk space (resizing or adding partitions and shares) • optimizing database performance • replacement of cables and switches
Application	
User Account Management	• password resetting • user identification and verification • create, update, unlock, disable, re-enable application specific accounts: - this may involve more than one instance of the application, i.e., development, test, qualification, training, production - consideration should be given to relevant controls arising from **O11 Security Management**
Permissioning	• grant, maintain, remove access to specified roles within the application, e.g., trainee, user, super user, engineer, departmental administrator, system administrator, etc. • grant, maintain, remove access to specified data areas within the application (training, validation, production), etc., as defined within the application: - this may involve more than one instance of the application, i.e., development, test, qualification, training, production - user permissions should be granted only after it has been demonstrated that the user is trained on the activities and procedures linked to the desired functions - consideration should be given to relevant controls arising from **O11 Security Management**
Monitoring	• ensures there are regular reviews of error messages and error logs for the application and in associated interfaces • regular reviews of access and permissions
System Maintenance	• running jobs, clearing error messages, starting and stopping services, increasing database table size • checking system interfaces and printer queues • recurring known system errors • 'workarounds'
Data Maintenance	• correction of transactional errors (transactional data modification)
Calibration	• ensure calibration is performed according to the calibration schedule
Maintenance/Like-for-Like Changes	• client reinstallation • midware installation • hardware changes
Patch Application	• low Risk patches to operating system, midware, database
Application Shut-Down and Start-Up	• planned maintenance • for scheduled backups
Routine Backup and Retrieval	• data files • audit trails • system logs For further information, see Section 13 of this Guide.

16.6.3 Periodic Review Considerations

For each system:

- Are there current and appropriate System Administration SOPs established and in use?
- Are System Administration Records and Logs (see Section 16.7.2 of this Guide) being collected and completed appropriately?

16.7 Records and Record Content

16.7.1 System Administration Procedures

System Administration tasks should be carried out according to documented SOPs.

The details of individual SOPs and their content can be found in the other operational process sections contained within this Guide. Typical System Administration SOPs may include:

- User Account Management procedure
- Administration of System access permissions procedure
- System Monitoring procedures
- System and Data Maintenance procedures
- Calibration procedures
- Patch Management procedures
- Start-Up and Shut-Down procedures
- Backup and Restore procedures

16.7.2 System Administration Records

During performance of System Administration tasks, records will be generated, updated, and deleted, either as part of the electronic audit trail within the system or as paper records.

The details of individual records and their content can be found in the other operational process sections contained within this Guide. Typical System Administration records may include:

- system access permissions
- access rights authorizations
- user profile records
- incident records
- backup and restore records/logs
- training records

- master data change records
- log of executed tasks

System Administrators also will require access to records generated elsewhere in order to carry out their monitoring role:

- system logs
- system error logs
- interface error logs
- system access permissions
- user profile records
- incident records
- backup and restore records/Logs
- master data change records
- configuration records

16.8 Scalability

The support model which provides System Administration to the organization is determined by the size and complexity of the systems to be supported and the receiving operational and support organizations. System Administrators may be local to the system and its users or as increasingly common may be provided by a central function. The extent to which this can be achieved depends upon the extent of system rationalization and shared infrastructure which has been achieved.

The following items should be considered:

- System Administration tasks follow a standard procedure. It is anticipated that even for High Impact Systems, such tasks are performed independently by the System Administrator without the involvement of the Quality Unit; however, where relevant, such standard procedures should be reviewed and approved by the Quality Unit.
- Each class of System Administration task should be subject to Impact and Risk Assessment to determine the required level of control (documentation, collection, and retention of evidence, level of Quality Unit review, etc.)
- For High Impact Systems some tasks defined as Administration tasks for a Low Impact System may need to be managed under **O6 Operational Change and Configuration Management**.

Table 16.2 indicates examples approaches based on System Impact. These examples are intended to be illustrative only, and not definitive.

Table 16.2: Possible Approaches Based on System Impact

System Administration Task		User Account Management	Permissioning	Monitoring	System Maintenance	Data Maintenance	Calibration	Maintenance/Like-for-Like Changes	Patch Application	Application Shut-Down and Start-Up	Routine Backup and Restore
System Impact	Low Impact System	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Medium Impact System	✓	✓	✓	✓	Use O6	✓	✓	✓	✓	✓
	High Impact System	✓	Use O6	✓	Use O6	Use O6	✓	✓	Use O6	✓	✓

17 Data Migration

17.1 Introduction

Data Migration is the activity of transferring data between storage types, formats, or computer systems. The need for Data Migration may be triggered when a system is significantly modified or upgraded, when replaced with a similar, but different system (in which case Data Migration should be addressed in the Project Phase of the new system) or when a system is permanently retired (e.g., as part of a closure or transfer operation).

The Data Migration process should follow a project life cycle. Data transformation during migration is likely to require the use of software tools, involving the creation of bespoke code. This guidance is intended to ensure that the appropriate controls are in place for planning, testing, executing, and verifying data migration activities to ensure accurate, complete, and usable data, which retains its contextual meaning following migration.

This section is related to Appendix D7 of GAMP® 5 (Reference 7, Appendix 4).

17.2 Scope

This process covers the migration of electronic data.

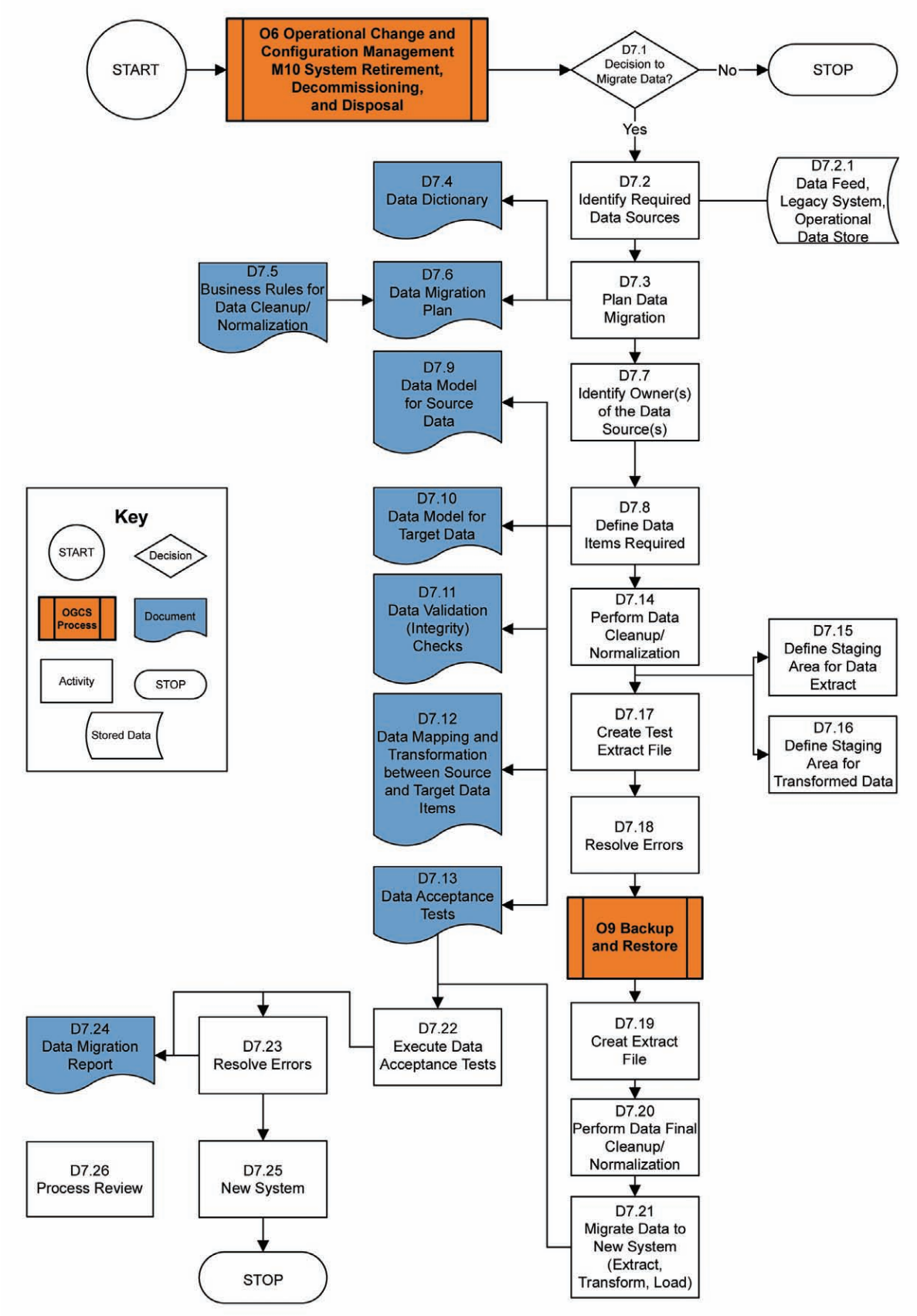
17.3 Roles and Responsibilities

Table 17.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 17.1: Roles and Responsibilities for Date Migration

Role	RACI Role	Responsibilities
Process Owner	A	• accountable for the Data Migration Plan • accountable for the execution and verification of the Data Migration • accountable for the data to be migrated and assigning data ownership • responsible for approval of the Data Migration Plan and Report
System Owner	R	• responsible for preparing aspects of the Data Migration Plan • responsible for approval of the Data Migration Plan and Report
Quality Unit	C	• consulted on content of Data Migration Plan for regulatory and compliance aspects • responsible for approval the Data Migration Plan and Report
End User	R	• informed that data will be migrated • responsible for verifying aspects of the Data Migration
Platform Support (SME)	R	• responsible for preparing aspects of the Data Migration Plan • responsible for executing and verifying platform dependent aspects of Data Migration
Application Support (SME)	R	• responsible for preparing aspects of the Data Migration Plan • responsible for approval of the Data Migration Plan • responsible for executing, verifying and reporting Data Migration
Project Manager	R	• responsible for managing Data Migration
Supplier	C	• consulted during Data Migration planning, execution, and verification, as required
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

17.4 Data Migration Process Flow Diagram



17.5 Process Narrative

Process Step/Decision/Record	Description
D7 Data Migration	**An Operational process for transferring data between storage types, formats, or computer systems.**
O6 Operational Change and Configuration Management **M10 System Retirement, Decommissioning, and Disposal**	These Operational processes may trigger a requirement for the **D7 Data Migration** process to be performed.
D7.1 Decision to Migrate Data	A proposal for Data Migration, can be triggered by: • retiring a system, but the data needs to be retained • system replacement or system upgrade • systems consolidation – consolidating many systems into one • ongoing system operations that require transfer of differing data from various sources to a common database • system platform change • archiving data for record retention purposes • outsourcing • remote hosting • change of site where the data is held
D7.2 Identify Required Data Sources	Data to be migrated can come from one or multiple sources, shown in the process flow diagram at D7.2.1 as Stored Data.
D7.3 Plan Data Migration	Planning is the key to any successful project. For data migration, consider the following: • What are the data sources? • Who owns the data? • Will all the data be migrated? • Is this a one-time data migration or will there be several iterations? • reconciliation with constraints both technical and business • development of a Data Migration Plan: - Need to validate the migration tool in advance of migration • post migration verification checks For further information, see Section 17.6.5 of this Guide.
D7.4 Data Dictionary	This is an complete inventory of: • source application data tables • the name, meaning, format, and 'relationships to other data' for each data table field
D7.5 Business Rules for Data Cleanup/Normalization	Data that is incorrect, obsolete, redundant, or incomplete should be identified. Rules for data cleanup/normalization should be established. A process for performing the data corrections should be defined. These rules inform the Data Migration Plan

17.5 Process Narrative (continued)

Process Step/Decision/Record	Description
D7.6 Data Migration Plan	The Data Migration Plan should contain: • definition of project scope and purpose • definition of tasks and deliverables including: - migration strategy/steps - data mapping and modeling - data transformation rules - data verification strategy - acceptance standards • risk management strategy • environment configuration management strategy addressing the following environments: - source - staging - target • budget • roles and responsibilities: - internal and external resources • tools • documentation requirements • timeline The Data Migration Plan should include: **Cutover Plan** This provides guidance for the execution of the various migration/ transformation steps. It should define procedures for promotion of the migrated data to becoming the valid master data and to change the status of the 'old' data to no longer being valid. A procedure for escalating migration issues to the appropriate stakeholder for resolution should be defined. Issues may include: • data cleanup/normalization • program changes • mapping changes • procedural changes • sequencing changes **Backout Plan** The plan should include in detail the steps to be followed to stop the migration process and return both the source and target systems to a qualified operational state.
D7.7 Identify Owner(s) of the Data Source(s)	It is important to identify the owner of the data source early in a project to ensure co-operation and resource availability for the data migration project. The owner of the data from the source system may not be a part of the organization that is implementing the target system. This means gaining buy-in and resources from an organization that may not have anything to gain from this project.

17.5 Process Narrative (continued)

Process Step/Decision/Record	Description
D7.8 Define Data Items Required	This is a listing of the data items to be migrated. It should include metadata as well as the actual data items. Creating this list is done by going through the source system's data structure and determining whether or not a data item should be migrated, i.e., whether the data is required for business, technical, or regulatory purposes. The team working on this aspect of the data migration should understand the data and meta-data content and context, structure, quality, and dependencies. This is a cross-functional effort (involving Technical Support and the Business Process Owners). Technical Support is necessary when defining the metadata.
D7.9 Data Model for Source Data	For the Source data: a Data Model describes all the data represented in an application and the relationships among them.
D7.10 Data Model for Target Data	For the Target data: a Data Model describes all the data represented in an application and the relationships among them. *Data models usually describe data as either structured hierarchies or networks.*
D7.11 Data Validation (Integrity) Checks	After the Business Rules for the data cleanup or normalization have been established, data validity/integrity checks should be defined. These checks will be used to enforce the Business Rules.
D7.12 Data Mapping and Transformation between Source and Target Data Items	This is an analysis phase to identify the links between the source system data fields and the corresponding target system data fields, in addition to the transformation rules by which the source data will be adjusted for the new system. One of the first questions to be addressed here is does data required by the target system even exist in the source system? The analysis requires detailed knowledge of both the source data and the target system. Consideration should be given to: • data elements that will not be migrated, including the rationale for the decision • filtering data for sub-set processing (e.g., take only US data) • doing lookups for translation values (e.g., $ = USD) • date/time formatting/standardization • changing data types • aggregating data for sums and averages • routing data for branching and case logic • joining disparate tables files • field lengths/truncated data • splitting fields • name and address standardization • link between e-signature to the signed record • audit trail migration
D7.13 Data Acceptance Tests	The Acceptance Tests should be developed from the data mapping and transformation rules.

17.5 Process Narrative (continued)

Process Step/Decision/Record	Description
D7.14 Perform Data Cleanup/ Normalization	The corrections defined in D7.9 should be verified using the data validation (integrity) checks defined in D7.10. This is an iterative process until the required level of correctness is achieved. This will depend on the data items and risk.
D7.15 Define Staging Area for Data Extract	A specific area should be established for storing the extract file that will be created from the source data.
D7.16 Define Staging Area for Transformed Data	A specific area should be established for storing the source data after it has been transformed.
D7.17 Create Test Extract File	Programs should be developed that will prepare the data based on the approved transformation rules and then load the data into an extract file based on the approved mapping rules. Data mapping, transformation, and load programs should be reviewed and finalized as required based on the test results. This is an iterative process until the required level of correctness is achieved.
D7.18 Resolve Errors	After each run, the data will have to be reviewed to detect and correct any errors in the mapping, transformation, or load programs. This is an iterative process until the required level of correctness is achieved. For further information on verification testing methods, see Section 17.6.5 of this Guide.
O9 Backup and Restore	A backup of the source data is taken before execution of the data migration commences.
D7.19 Create Extract File	Create Extract File using rules and programs as finalized in steps D7.16 and D7.17.
D7.20 Perform Final Data Cleanup/Normalization	This is the final opportunity before the actual data migration is executed to correct any data problems.
D7.21 Migrate Data to New System (Extract, Transform, Load)	Complete the migration of data to new system (Extract, Transform, and Load).
D7.22 Execute Data Acceptance Tests	Run Acceptance Tests (Data Integrity) defined in D7.12.
D7.23 Resolve Errors	This is the last opportunity before acceptance and release to correct any data problems.
D7.24 Data Migration Report	The Data Migration Report should provide a brief summary of the success of the verification activities, highlighting any deviations from process or expected results, explaining the impact of these deviations on the status of the data migration. Additionally, if for any reason the scope of the data migration has changed, the report should document and justify this decision. Data issues listed in the Data Migration Report as 'to be resolved after acceptance and release' should be addressed on a timely basis.

17.5 Process Narrative (continued)

Process Step/Decision/Record	Description
D7.25 New System	Accurate and complete migrated data is available and usable in the new system. There should be a procedure for withdrawing or annulling the 'old' version of the data so it is unambiguous which data is valid.
D7.26 Process Review	The **D7 Data Migration** process is likely to be an infrequent process for any individual system. SMEs involved should hold a process review as soon as possible after the completion of the data migration to ensure that any opportunities for improvement of the process are identified and documented.

17.6 Procedural Guidelines and Considerations

It is recommended that an organization has a controlling Policy and Procedure for Data Migration activities.

17.6.1 Approach to Migration

Data migration efforts can vary greatly in scope, complexity, and risk, and may occur several times during the life cycle of a computerized system. The Data Migration process should be documented throughout the computerized system life cycle.

17.6.2 Data Relationships

Considerable complexity can be involved when migrating data from one database structure to another. It is critical that data relationships (e.g., between records in different tables) are maintained in order to ensure that data retains its contextual meaning.

17.6.3 Electronic Signatures

Where signed electronic records are being migrated, the links between the record and the electronic signature should be maintained.

17.6.4 Master Data

The master data/valid data set should be determined and documented (in situations where at a given point in time, two sets of data (old and new) may coexist, e.g., before final close down of the old system has been achieved).

17.6.5 Verification Testing Methods

In order to test and verify the migration, the following methods may be used:

- code checking of migration scripts/tools, e.g., by peer review
- use of CHECKSUMs when executing the migration
- comparing records from before migration (in source system) and after migration (in target system) manually

17.6.6 Periodic Review Considerations

The life cycle documentation and records produced as part of the Data Migration project should be reviewed following completion of the data migration effort. Outstanding actions reported in the Data Migration Report should be investigated to ensure appropriate resolution.

17.7 Records and Record Content

Suggested contents for the documents identified in this section:

Record Examples

Data Migration Plan

1. Purpose of Document
2. Project Scope and Purpose:
    - definition of source and target systems
    - budget
3. Justification for the Data Migration:
    - brief explanation of the business rationale
4. Roles and Responsibilities for executing the plan:
    - The organizations involved, e.g., will any suppliers or partners be involved?
    - The departments/roles involved within each organization and their responsibility.
    - Indicate who will be ultimately in control.
5. Planned Timeline
6. Details of any Documentation to be archived:
    - Ensure that full documentation is maintained for Audit purposes.
    - Explanation of how, where, and how long it will be archived.
7. Details of any Data to be archived:
    - List source systems.
    - Explanation of how, where, and for how long the archived data will be retained.
8. Definition of Tasks and Deliverables
    - migration strategy/steps
    - data verification strategy
    - acceptance standards
    - risk management strategy
    - environment configuration management strategy

9. Details of what other things will be affected and how

In addition, consider at least the following:

- Cutover Plan (for suggested contents see below)
- Backout Plan (for suggested contents see below)
- tools or scripts used for migration
- other computer systems
- SOPs
- training
- supplier support agreements
- any required changes to Configuration Items List (e.g., 'old' platform components retired, 'new' platform added; software version updates)
- overviews/network diagrams
- spare part lists ('old' components no longer required, 'new' components should be available)
- Service Level Agreement(s)and Escrow agreement(s)
- backup schedules
- Business Continuity Plan

Cutover Plan

1. Purpose of Document
2. Responsibility for executing the Cutover Plan:
   - The organizations involved, e.g., will any suppliers or partners be involved?
   - The departments/roles involved within each organization and their responsibility.
   - Indicate who will be ultimately in control.
   - Communication Plan – including communication of any data migration issues.
3. Documents:
   - Indicate what needs to be done to execute the various data migration/transformation steps.
   - Includes a procedure for escalating data migration issues to the appropriate stakeholder for resolution.
4. Timelines and Dependencies:
   - What is the timeline to achieve the migration?

- If the timeline is not met, what dependencies should be considered when extending the task or moving a task to another date?

Backout Plan

1. Purpose of Document

   The purpose of the backout plan is to determine what needs to be done to return the source and target systems to their original operational state in a controlled manner.

   The scope of the backout plan should be defined; usually the data included in the target system is backed up and the backout plan is limited to the restoration of the back-up.

2. Responsibility for executing the Backout Plan:

   - The organizations involved, e.g., will any suppliers or partners be involved?
   - The departments/roles involved within each organization and their responsibility.
   - Indicate who will be ultimately in control.

3. Documents:

   - Indicate whether any documents from the original data migration plan can remain archived as they are no longer needed for operational use.

4. Data:

   - Indicate what needs to be done to return the data to its original state.
   - Indicate if other actions are necessary to make a system useable from the restoration date, e.g., running overnight runs with no transactions to bring the system up to the current date or re-enabling user access.

5. Software

   - Indicate what needs to be done to return the source or target system's software to its original state.

6. Hardware

   - Indicate what needs to be done to return the source or target system's hardware to its original state – particularly if the data migration is to move from an obsolete or unsupported platform.

7. Validation Scope

   - Indicate and justify the amount of validation and qualification to be performed prior to the source or target systems being re-released for use.

Data Migration Report

1. Purpose of the Document

2. Deviations from the Data Migration Plan

3. Documents:

    - The impact of any deviations on the accuracy and completeness of the data migration.

    - Any changes in the scope of the data migration.

4. Open Issues:

    - A list of any open issues outstanding from the migration and a time-line for their resolution.

17.8 Scalability

- The basic process will be the same for all systems. When the Data Migration is planned, the amount, complexity, and risk of the data to be migrated will influence the scale of the migration and testing activities.

- For large data volumes or complex migration tasks, it may be necessary to develop automated software tools to migrate the data effectively, the need for the qualification of such tools also should follow a risk-based approach. For high impact systems, the regulated organization should be able to demonstrate high confidence in the integrity of migrated data.

18 System Retirement, Decommissioning, and Disposal

18.1 Introduction

System retirement, decommissioning, and disposal ensure that the appropriate controls are in place when a system is removed from day to day use, e.g., through obsolescence or replacement:

- to ensure other systems and data are unaffected
- to retain and protect data from the removed system until that data is deemed to be no longer required

This section is related to Appendix M10 of GAMP® 5 (Reference 7, Appendix 4).

18.2 Scope

This guidance covers retirement, decommissioning, and disposal of a system. This approach also could be extended to parts of a system or of data out from systems.

Definitions

Retirement – System is removed from active operations, i.e., 'normal operational' users are deactivated and interfaces disabled. No data is added to the system from this point forward. 'Special access' is retained for data reporting, results analysis, and support.

Decommissioning – The controlled shutdown of a Retired System. A system may be stored if required to be reactivated at a later date, e.g., for retrieval of regulatory data or results.

Disposal – Data, documentation, software, or hardware can be permanently destroyed. Each may reach this stage at a different time. Data and documentation may not be disposed of until they have reached the end of the record retention period as specified in the Record Retention policy.

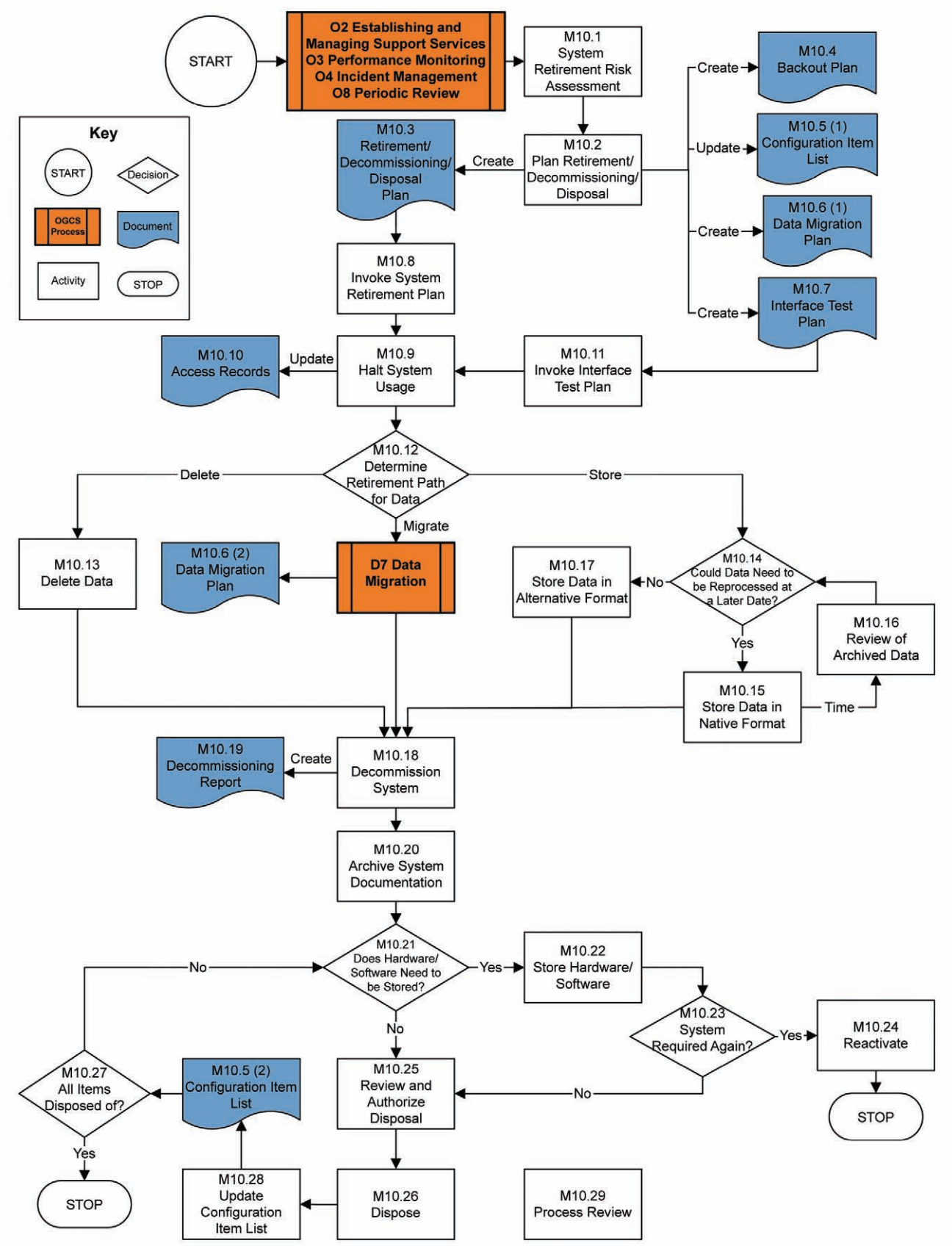
18.3 Roles and Responsibilities

Table 18.1 provides an indicative example. Individual organizations should allocate roles and responsibilities based on organizational structure and the specific system involved.

Table 18.1: Roles and Responsibilities System Retirement, Decommissioning, and Disposal

Role	RACI Role	Responsibilities
Process Owner	A	• accountable for the Retirement Plan • accountable for the execution and verification of the Retirement Plan • accountable for the data and documentation related to the system being retired and ensuring compliance with relevant retention policies • responsible for approval of the Retirement Plan and Report
System Owner	R	• responsible for preparing aspects of the Retirement Plan • responsible for approval of the Retirement Plan and Report
Quality Unit	C	• consulted on content of Retirement Plan for regulatory and compliance aspects • responsible for approval the Retirement Plan and Report
End User	I	• informed of the plan to retire the system • responsible for verifying aspects of the Retirement Plan, e.g., ongoing data accessibility, impact on interfaced systems
Platform Support (SME)	R	• responsible for preparing aspects of the Retirement Plan • responsible for executing platform dependent aspects of the Retirement Plan
Application Support (SME)	R	• responsible for preparing aspects of the Retirement Plan • responsible for approval of the Retirement Plan • responsible for executing the Retirement Plan • responsible for reporting on Retirement Report
System Administrator (SME)	R	• responsible for preparing aspects of the Retirement Plan
Archivist (SME)	R	• consulted on content of Retirement Plan for organization records retention policies • responsible for executing the archive aspects of the Retirement Plan
Project Manager	R	• responsible for managing retirement, decommissioning, and disposal
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

18.4 System Retirement, Decommissioning, and Disposal Process Flow Diagram



18.5 Process Narrative

Process Step/Decision/Record	Description
M10 System Retirement, Decommissioning, and Disposal	**An Operational process for the Retirement, Decommissioning, and Disposal of Systems**
O2 Establishing and Managing Support Services **O3 Performance Monitoring** **O4 Incident Management** **O8 Periodic Review**	A proposal for System Retirement, can be triggered by: • or a major business process change
M10.1 System Retirement Risk Assessment	An assessment is made of the risks (business, technical, and regulatory) associated with retiring a system. It may be appropriate to conduct a Periodic Review as an input to the risk assessment and a rationale of whether or not to retire the system is developed. If the risks of continuing to operate a system are considered greater than the risks associated with retiring a system, a plan is developed to take it through retirement and decommissioning to disposal.
M10.2 Plan Retirement/ Decommissioning/Disposal	Inputs to the planning process will be from several sources: e.g., • System Retirement Risk assessment (M10.1) • Backup and Restore – what backups need to be taken • Security – which access rights need to be revoked and which need to be retained • Record Retention Policy – the time period for which system data should be retained: - An analysis of records held within a system is required to determine the appropriate retention periods in line with relevant regulatory requirements and business policies - Several different retention periods may be identified; system data may be retained for the longest period. • Data migration – whether/how data from a system can be migrated to another system • Business continuity plan – to understand the impact on the rest of the business if this system is removed. Outputs from the planning process include: • Retirement/Decommissioning/Disposal Plan • Backout plan (to provide the ability to revert to the operational system) • Interface Test plan (to ensure interfaced systems continue to operate correctly when this system is retired) • Migration Test Plan • A baselined Configuration Items List • Formal confirmation to the business of the intention to retire the system
M10.3 Retirement/ Decommissioning/Disposal Plan (Create)	The Plan explains why the system is to be retired and what needs to occur to achieve system retirement.
M10.4 Backout Plan (Create)	The Backout Plan contains detailed steps to be followed should it be decided to reverse the process, prior to disposal, and make a system operational again.

18.5 Process Narrative (continued)

Process Step/Decision/Record	Description
M10.5 (1) Configuration Item List (Update)	A list of hardware, software, data, and documentation which comprise the system. It is reviewed and updated immediately prior to retirement to ensure that it is up to date.
M10.6 (1) Data Migration Plan (Create)	The Migration Plan details which data will be moved from a Retiring System to a new System and the tests to demonstrate that records are transferred successfully and data is fully accessible in the new system.
M10.7 Interface Test Plan (Create)	The Interface Test Plan details the tests to be performed to ensure that systems which interface with the retired system operate normally when the interface is removed.
M10.8 Invoke System Retirement Plan	The relevant parts of the Retirement/Decommissioning/Disposal Plan are invoked in order to shut down the System.
M10.9 Halt System Usage	The System is removed from operational use. This includes: • Deactivation of 'normal operational' user access (triggered by Access Rights Authorization Requests) • Where appropriate, e.g., for laboratory systems, a 'final' calibration of a system may be required • Deactivation of interfaces with a system • Update to operational documents, e.g., SLAs, SOPs, Network diagrams and Backup schedules • If appropriate, a final calibration of equipment should be performed to ensure that the equipment has performed as intended since the last calibration until removal from use. **Note:** if a System is required to be brought back into routine use, be prepared to reactivate according to M10.4 Backout Plan.
M10.10 Access Records	The Access Rights Authorization requests, System Access Permissions, and User Profile Records are updated.
M10.11 Invoke Interface Test Plan	Use the Interface Test plan to test that those Systems which interface with the System to be removed will continue to operate normally.
M10.12 Determine Retirement Path for Data	Determine how the data should be retired. This assessment is risk-based and should consider: • The time period for which data should be retained (per a Records Retention Policy) • In what format data may be accessed Data may be: • Deleted • Migrated to another electronic System • Stored
'Delete' Path M10.13 Delete Data	The outcome of the Risk Assessment at step M10.12 indicates that data is not required to be retained and it is permanently deleted.
'Migrate' Path M10.6 (2) Data Migration Plan	The outcome of the Risk Assessment at step M10.12 indicates that data is to be retained and migrated to a new system. The Data Migration Plan is implemented.

18.5 Process Narrative (continued)

Process Step/Decision/Record	Description
D7 Data Migration	The data is moved to another electronic system of similar functionality, e.g., from one supplier's LIMS system to another. This does not include an upgrade of the existing system. The integrity of the data, meta-data, and the number of records should be maintained via a qualified conversion process so that data is fully accessible with the entire functionality of a new system. The data integrity should be verified post migration The migrated data is available to the entire functionality in a new system, e.g., it can be viewed, queried, and sorted.
'Store' Path M10.14 Could Data Need to be Reprocessed at a Later Date? (Store)	The outcome of the Risk Assessment at step M10.12 indicates that data is to be retained. Determine whether the data may need to be reinstated in the future to decide the format in which it is stored. If data will not need to be reinstated into the original system, it can be stored in an 'alternative' format (M10.17). If it could need to be reinstated to the original system, it is stored in the native format.
M10.15 Store Data in Native Format	The data is retained, but outside the original system. **O9 Backup and Restore** and the **GAMP® Good Practice Guide: Electronic Data Archiving** (Reference 8, Appendix 4) provide further guidance. Store the data in native electronic format which can be restored into the original system, e.g., backup raw data and meta-data and restore to reactivate a system. The data is stored for the time period specified in the Records Retention policy.
M10.16 Review of Archived Data	Following a documented risk assessment, the data may be transferred from the native format to the alternative format over time, e.g., as hardware and software ages, it may not be possible to reinstate the original system and paper records of results may be required.
M10.17 Store Data in Alternative Format	The data is retained, but outside the original system. Store the data and associated meta-data in human readable format, e.g., printed, microfiche, PDF. This format may store either results, e.g., reports containing the results of calculations or the raw data. The data is stored for the time period specified in the Records Retention policy.
M10.18 Decommission System	Shutdown the hardware and software assets. **Note:** if data is stored in alternative format, the hardware and software may be disposed of once the data is verified as being complete and readable.

18.5 Process Narrative (continued)

Process Step/Decision/Record	Description
M10.19 Decommissioning Report (Create)	The Decommissioning report is produced to record what actually occurred when the system was retired. Where appropriate, the decommissioning report also should document that the validated state of the system was maintained until the system was closed down, e.g., by a final baseline review.
M10.20 Archive System Documentation	Archive the System documentation in accordance with the Document Management Policy and Records Retention Policy. GAMP® 5 Sections **M9 Document Management** and **O13 Archiving and Retrieval** plus the **GAMP® Good Practice Guide: Electronic Data Archiving** (Reference 8, Appendix 4) provide further guidance on document and e-record archiving respectively. • This includes any Validation documentation, supplier manuals, user documentation, SOPs, SLAs, and escrow.
M10.21 Does Hardware/Software Need to be Stored?	Determine whether the hardware or software need to be retained in case there is a need to reinstate the original System for reprocessing of data.
M10.22 Store Hardware/Software	Store the hardware and software assets in accordance with Manufacturers recommendations for the time period required by any native data (M10.15) which may be required to be reactivated.
M10.23 System Required Again?	Determine whether a system needs to be reinstated to operational use.
M10.24 Reactivate	A System is brought back into operational use, using the Backout Plan produced at step M10.4 as a reference.
M10.25 Review and Authorize Disposal	Determine whether any items on the Configuration Item List can be disposed of. For data and documentation, the record retention period (as specified in the Records Retention Policy) should have been reached. If so, and there is no other reason to retain the system, authorize the disposal of those System components. This step may occur several times until all System components have been disposed of.
M10.26 Dispose	The items authorized for disposal in M10.25 are permanently destroyed. This may include: hardware, software (application and platform code), data, and documentation. Responsibility (dependent on item(s) to be disposed of): Platform Support, Application Support, Archivist.
M10.28 Update Configuration Item List	Update the Configuration Item list to indicate which items have been disposed of and which remain.
M10.5 (2) Configuration Item List	The list is updated.
M10.27 All Items Disposed of?	Review the Configuration Item List and determine whether all items on it have been disposed of. If not, periodically re-review (M10.21) whether any of the remaining items can be disposed of. When all items on the Configuration Item List have been disposed of, the process is complete.

18.5 Process Narrative (continued)

Process Step/Decision/Record	Description
M10.29 Process Review	Following retirement and decommissioning of a system, there should be a formal review of the process to ensure that all steps have been completed and that any 'lessons learned' are captured for future retirement activities.

18.6 Procedural Guidelines and Considerations

18.6.1 Risk Assessment

For the determination of the risk associated with retirement and decommissioning of a system, the following should be considered, as a minimum:

- type of computerized system (e.g., using GAMP® Categories 3, 4, or 5)
- type of records within the system and their business and regulatory criticality:

See Appendix 6 of the GAMP® Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures (Reference 8, Appendix 4) for examples of records and signatures required by current GxP regulations

- complexity of the system
- risk to other systems of retiring this system
- GxP risks, e.g., impact on product quality and patient safety
- compliance status of system
- system stability
- business risk, e.g., impact on brand recognition, patient safety, corporate reputation
- risks in keeping the system running, e.g., supplier support withdrawn
- risks to the data if it remains on this System, e.g., viruses, hacking, accidental deletion
- potential future need for the system or results produced from the system
- whether the system is a 'hybrid' system producing paper records
- the need to retain obsolete skills to reactivate the system hardware and software (e.g., use of DOS rather than Windows, recovery of data from tape not CD, etc.)

18.7 Record and Record Content

It is recommended that an organization has a controlling Policy and Procedure for System Retirement, Decommissioning, and Disposal.

Suggested contents for the documents identified in this section:

18.7.1 Retirement, Decommissioning, and Disposal Plan

1. Purpose of Document
2. Brief Description of the System
3. Justification for Retirement, Decommissioning, or Disposal
   - brief explanation of the business rationale
4. Responsibility for executing the Plan:
   - The organizations involved, e.g., will any suppliers or partners be involved?
   - The departments/roles involved within each organization and their responsibility.
   - Indicate who will be in control ultimately.
5. Planned Timescales:
   - start date and expected duration
   - dependencies
6. Details of Documentation to be archived:
   - list extracted from Configuration Items (CI) list
   - explanation of how, where, and for how long it will be archived
7. Details of Data to be Archived:
   - list
   - explanation of how it will be removed and where/how long it will be retained
8. Details of hardware to be shutdown:
   - list extracted from Configuration Item list
   - explanation of how it will be shutdown and whether/where/how long it will be retained
9. Details of software to be removed:
   - list extracted from Configuration Item list
   - explanation of how it will be removed and whether/where/how long it will be retained
10. Details of what other things will be affected and how

    Items that should be considered include:

    - other computer systems

- interfaces
- SOPs
- training
- supplier support agreements
- Configuration Items List
- overviews/network diagrams
- spare part lists
- SLAs and escrow agreements
- backup schedules
- Business Continuity Plan

18.7.2 Backout Plan

1. Purpose of Document
2. Responsibility for executing the Backout Plan:
   - The organizations involved, e.g., will any suppliers or partners be involved?
   - The departments/roles involved within each organization and their responsibility.
   - Indicate who will be ultimately in control.
3. Documents:
   - Indicate what needs to be done to return the documentation to its original state.
   - Indicate whether any documents from the original plan can remain archived as they are no longer needed for operational use.
4. Data:
   - Indicate what needs to be done to return the data to its original state.
   - Indicate if other actions are necessary to make a system useable from the restoration date, e.g., running overnight runs with no transactions to bring the system up to the current date or re-enabling user access.
5. Hardware:
   - Indicate what needs to be done to return the hardware to its original state.
   - Indicate whether upgrades need to be performed to achieve an operational system, e.g., because a supplier no longer supports the hardware which was retired.

6. Software

    - Indicate what needs to be done to return the software to its original state.

    - Indicate whether any upgrades need to be performed to achieve an operational system, e.g., because a supplier no longer supports the software version which was retired.

7. Validation Scope:

    - Indicate and justify the amount of validation and qualification to be performed prior to the system being re-released.

18.7.3 Migration Plan

- Purpose of Document
- Data to be Moved:
    - Indicate the data to be moved, where it will move to and how, e.g., automated or manual set up.
- Test Plan
    - Include tests to show that all records have been transferred and all data is fully accessible.

For further information, see Section 17 of this Guide.

18.7.4 Interface Test Plan

- Purpose of Document
- Systems to be Tested
- Test Details:
    - for each system

18.7.5 Decommissioning Report

1. Purpose of the Document
2. Deviations from the Retirement, Decommissioning, and Disposal Plan
3. Documents:
    - Indicate what has been removed, where it is retained, and for how long (or if it has been disposed of).
4. Data:
    - Indicate what has been removed, where it is retained, and for how long.
5. Hardware:
    - Indicate what has been removed, where it is retained, and for how long (or if it has been disposed of).

6. Software:

    - Indicate what has been removed, where it is retained, and for how long (or if it has been disposed of).

7. Validated State

Where appropriate the decommissioning report also should document that the validated state of the system was maintained until a system was closed down, e.g., by a final baseline review.

18.8 Scalability

The basic process will be the same for all Systems. When the Retirement/Decommissioning/Disposal is planned the size of the Configuration Item List, the amount and complexity of data and documentation, and the Record Retention period will influence the scale of the operation.

19 Appendix 1 – RACI Roles and Operational Processes

This section presents the RACI roles allocated to the operational processes and defines each role (according to GAMP® 5 (Reference 7, Appendix 4) terminology where available).

19.1 RACI Terms

The RACI terms are defined as below:

- **Responsible (R)** – this role identifies the "doers" of the process task. They should complete the task. Several individuals can be jointly responsible.
- **Accountable (A)** – this person is the "owner" of the business process and related tasks. This person should make sure that roles and responsibilities are assigned and ensure that resource is provided. There is only one person accountable for each business process (where a system supports more than one business process the accountability for the system can be shared).
- **Consulted (C)** – these are the people who need to give input before the work can be done, during the execution of the work and at sign-off. These people are active participants in the process.
- **Informed (I)** – these people need to be kept "in the picture." They need updates on progress, but they do not need to be formally consulted, nor do they contribute directly to the process task.

For clarity, an implicit hierarchy has been assumed:

- Accountable
- Responsible
- Consulted
- Informed

Where an individual may take several RACI roles in the execution of a higher level process step, the highest ranking role is assigned and the subsidiary roles may be applicable for some parts of the process, e.g., a Responsible person would always be Consulted and Informed regarding modifications to the process for which they have responsibility.

19.2 Grid Showing Operational Process versus RACI Role

Operational Process / Role	O1 Handover	O2 Establishing and Managing Support Services	O3 Performance Monitoring	O4 Incident Management	O5 Corrective and Preventive Action	O6 Operational Change and Configuration Management	O7 Repair Activity	O8 Periodic Review	O9 Backup and Restore	O10 Business Continuity Management	O11 Security Management	O12 System Administration	D7 Data Migration	M10 System Retirement, Decommissioning, and Disposal
Process Owner	R	C	I	C	R	A	I	A		A	R	C	A	A
System Owner (IT/Eng)	R	A	A	A	R	A	A	R	A	A	A	A	R	R
Project Manager	A	R											R	R
End User	I	I		C	I	I	I	C	I	I	I	I	R	I
Quality Unit	C	C		C	A	R	C	C	C	C	C	C	C	C
Platform Support (SME)	R	R	R	R	R	R	R	C	R	R	R	C	R	R
Application Support (Technical/Repairs) (SME)	R	R	R	R	R	R	R	C	C	R	R	C	R	R
System Administrator	R	R	R	R	R	R		C	I	R	R	R	I	R
Reviewer/Auditor (SME)								R						
Supplier	C	C	C	C		C	C	C		C	I	R	C	
Where R = Responsible, A = Accountable, C = Consult, I = Inform														

Note: Archiving and Retrieval (O13) is not included in this grid as a more detailed discussion of this topic is included in the ISPE GAMP® Good Practice Guide: Electronic Data Archiving (Reference 8, Appendix 4).

19.3 Roles

The roles are defined as detailed below.

19.3.1 Process Owner

The Process Owner is responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable SOPs throughout its useful life. Responsibility for control of system access should be agreed between process and System Owner. In some cases, the Process Owner also may be the System Owner.

Note: ownership of the data held on a system should be defined and typically belongs to the Process Owner (see GAMP® 5 (Reference 7, Appendix 4)).

19.3.2 System Owner

The System Owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable SOPs. Responsibility for control of system access should be agreed between process and System Owner. In some cases, the System Owner also may be the Process Owner (GAMP® 5).

19.3.3 Project Manager

The person responsible for managing activities in accordance with defined and approved plans.

19.3.4 End User

The organization or group responsible for the operation of a system [GMA-NAMUR, 1966].

19.3.5 Quality Unit

An encompassing term that includes many quality-related roles that are important to developing and managing regulated computerized systems.

"The Quality Unit has a key role to play in successfully planning and managing the compliance and fitness for intended use of computerized systems, and provides an independent role in the:

- approval or audit of key documentation, such as policies, procedures, acceptance criteria, plans, reports
- focus on quality critical aspects
- involvement of SMEs
- approval of changes that potentially affect patient safety, product quality , or data integrity
- audit processes and supporting documentary evidence to verify that compliance activities are effective" [GAMP® 5, ISPE, 2008].

19.3.6 Subject Matter Expert (SME)

SMEs are those individuals with specific expertise in a particular area or field. SMEs should take the lead role in the verification of computerized systems. SME responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results [ASTM E2500] (Reference 3, Appendix 4).

Three SME roles are identified in this Good Practice Guide:

- **Platform Support:** the person(s) responsible for providing technical support for all components of the IT infrastructure upon which the computerized system operates.
- **Application Support (Technical/Repairs):** the person(s) responsible for providing technical support for the computerized system application.
- **System Administrator:** the person(s) responsible for providing routine support for the computerized system application – including account management.

19.3.7 Supplier

Suppliers provide a range of products, applications, and services for hardware, software, and related technologies (see GAMP® 5 (Reference 7, Appendix 4)).

20 Appendix 2 – Mapping of Operational Processes to ITIL® and COBIT®

For regulated organizations, making use of other support management models has been incorporated to show how the guidance in this Guide is consistent and aligned with initiatives such as Information Technology Infrastructure Library (ITIL®) (Reference 10, Appendix 4) and Control Objectives for Information and related Technology (COBIT®) (Reference 9, Appendix 4).

Table 20.1: Mapping of Operational Processes to ITIL® and COBIT®

GAMP® 5 – O Appendices	ITIL® V3	COBIT® 4.0
O1 Handover The process for transfer of responsibility of a computerized system from a project to operation.	Release Management (Service Support) (Service Transition) The process responsible for planning, scheduling, and controlling the movement of releases to test and live environments.	A12 – Acquire and maintain application software A14 – Enable operation and use A17 – Install and accredit solutions and changes
O2 Establishing and Managing Support Services The process that ensures that support services (whether internal or external) are appropriately specified and managed. This is often managed through the use of SLAs.	Service Design Package Document(s) defining all aspects of an IT Service and its requirements through each stage of its life cycle. Capacity Management (Service Delivery) (Service Design) The process responsible for ensuring that the capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Service Level Management (Service Life cycle Mgt) (Service Delivery) (Service Design) (Continual Service Improvement) The process responsible for negotiating SLAs and ensuring that these are met. Availability Management (Service Delivery) (Service Design) The process responsible for defining, analyzing, planning, measuring, and improving all aspects of the Availability of IT Services.	P01 – Define a strategic IT plan P09 – Assess and manage IT Risks A13 – Acquire and maintain technology infrastructure A14 – Enable operation and use A16 – Manage changes A17 – Install and accredit solutions and changes DS1 – Define and manage service levels DS3 – Manage performance and capacity DS5 – Ensure systems security DS11 – Manage data ME1 – Monitor and evaluate IT performance

Table 20.1: Mapping of Operational Processes to ITIL® and COBIT® (continued)

GAMP® 5 – O Appendices	ITIL® V3	COBIT® 4.0
O3 Performance Monitoring That part of overall preventive maintenance that obtains performance data that is useful in diagnosing system problems. It provides trends that may indicate performance problems, which can be used as part of Corrective and Preventive Actions (CAPA) to reduce application or system down time.	Performance Management (Service Delivery) (Continual Service Improvement) The Process responsible for day-to-day Capacity Management Activities. These include monitoring, threshold detection, Performance analysis, and Tuning, and implementing changes related to Performance and Capacity."	DS3 – Manage performance and capacity ME1 – Monitor and evaluate IT performance
O4 Incident Management Ensure that any unplanned issues that could impact patient safety, product quality, and data integrity are addressed before any harm occurs.	Incident Management (Service Support) (Service Operation) The process responsible for managing the life cycle of all incidents. The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible. Where the ITIL® definition of an incident is: (Service Operation) An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident. For example Failure of one disk from a mirror set.	P09 – Assess and manage IT Risks DS8 – Manage service desk and incidents
O5 Corrective and Preventive Action A process for investigating, understanding, and correcting discrepancies, while attempting to prevent their recurrence and for recognizing potential discrepancies to prevent their occurrence.	Problem Management (Service Support) (Service Operation) The Process responsible for managing the Life cycle of all Problems. The primary Objectives of Problem Management are to prevent Incidents from happening, and to minimize the Impact of Incidents that cannot be prevented.	P09 – Assess and manage IT Risks DS8 – Manage service desk and incidents DS10 – Manage problems

Table 20.1: Mapping of Operational Processes to ITIL® and COBIT® (continued)

GAMP® 5 – O Appendices	ITIL® V3	COBIT® 4.0
O6 Operational Change and Configuration Management Change Management is the process of controlling the life-cycle of changes. Configuration Management comprises those activities necessary to be able to precisely define a computerized system at any point during its life-cycle, from the initial steps of development through to retirement.	Change Management (Service Support) (Service Transition) The Process responsible for controlling the Life cycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made with minimum disruption to IT Services. Configuration Management (Service Support) (Service Transition) The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Life cycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.	A16 – Manage changes A17 – Install and accredit solutions and changes DS9 – Manage the configuration
O7 Repair Activity The process of managing repair or replacement of a failed or defective component, which may be a Configuration Item. It is a form of Change Control in which the relevant specifications do not change.	Repair (Service Operation) The replacement or correction of a failed Configuration Item.	A16 – Manage changes A17 – Install and accredit solutions and changes
O8 Periodic Review Periodic Reviews are used throughout the operational life of a computerized system to verify that it remains compliant with regulatory requirements, fit for intended use, and satisfies organization policies and procedures.	IT Service Continuity Management (ITSCM) (Service Delivery) (Service Design) The Process responsible for managing Risks that could seriously impact IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels, by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services. ITSCM should be designed to support Business Continuity Management.	DS3 – Manage performance and capacity DS4 – Ensure continuous service

Table 20.1: Mapping of Operational Processes to ITIL® and COBIT® (continued)

GAMP® 5 – O Appendices	**ITIL® V3**	**COBIT® 4.0**
O9 Backup and Restore Backup is the process of copying records, data, and software to protect against loss of integrity or availability of the original. Restore is the subsequent restoration of records, data, or software when required.	Backup and Restore Backup (Service Design) (Service Operation) Copying data to protect against loss of integrity or availability of the original. Restore (Service Operation) Taking action to return an IT Service to the users after repair and recovery from an Incident.	DS4 – Ensure continuous service
O10 Business Continuity Management Business Continuity Management (BCM) encompasses the steps required to restore business processes following a disruption, while continuing to provide product or services to the customer.	Business Continuity Management (BCM) (Service Design) The Business Process responsible for managing Risks that could seriously impact the Business. BCM safeguards the interests of key stakeholders, reputation, brand. and value creating activities. The BCM Process involves reducing Risks to an acceptable level and planning for the recovery of Business Processes should a disruption to the Business occur. BCM sets the Objectives, Scope, and Requirements for IT Service Continuity Management.	DS3 – Manage performance and capacity DS4 – Ensure continuous service
O11 Security Management The process that ensures the confidentiality, integrity, and availability of an organization's regulated systems, records, and processes	Information Security Management (ISM) (Service Delivery) (Service Design) The Process that ensures the Confidentiality, Integrity, and Availability of an Organization's Assets, information, data, and IT Services. Information Security Management usually forms part of an Organizational approach to Security Management, which has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls etc., for the entire Organization.	DS5 – Ensure systems security

Table 20.1: Mapping of Operational Processes to ITIL® and COBIT® (continued)

GAMP® 5 – O Appendices	ITIL® V3	COBIT® 4.0
O12 System Administration Routine management and support of systems to ensure that they are running efficiently and effectively.	System Management The part of IT Service Management (ITSM) that focuses on the management of IT infrastructure rather than process. The implementation and management of Quality IT Services that meet the needs of the business.	A14 – Enable operation and use DS13 – Manage operations ME2 – Monitor and evaluate internal control ME4 – Provide IT governance
O13 Archiving and Retrieval The process of taking records and data off-line by moving them to a different location or system, often protecting them against further changes.	Archiving and Retrieval Not a specific ITIL® function/activity It would be covered in the Service Design Package.	DS4 – Ensure continuous service

21 Appendix 3 – List of Control Records

This list of control records is intended to assist with the preparation of a Periodic Review checklist. Depending on the depth of Periodic Review these records may be subject to review at different levels of rigor.

Organizations may assign different names to these records and they may be incorporated into other records, e.g., the Handover Report for a system may be included in a larger project Handover Report.

O1 Handover:

- Handover Plan
- Handover Report
- (Baseline) Configuration Item List

O2 Establishing and Managing Support Services:

- Audit Report
- SLAs
- Support SOPs
- Support Records
- Performance Reports

O3 Performance Monitoring:

- Performance Monitoring Plan
- Performance Measurements
- Alarm Notifications

O4 Incident Management:

- Incident Log
- Incident Record
- Incident Report

O5 CAPA:

- CAPA Log Entry
- CAPA Record (includes Root Cause Analysis)

O6 Operational Change and Configuration Management:

Operational Change:

- Change Log
- Change Plan
- Impact Assessment
- Functional Risk Assessment
- Modification Specifications
- Backout Plan
- Installation Evidence
- Test Protocols
- Updated URS, FS, Configuration Item List etc
- Change Review Report

Configuration Management:

- Configuration Item List – current
- Archived Configuration Item Records (preserved)

O7 Repair Activity:

- SLA
- Work Request/ Permit
- Test Documentation
- Service/Maintenance Log and Reports

O8 Periodic Review:

- Previous Periodic Review Report
- Related CAPA records

O9 Backup and Restore:

- Backup and Media Rotation Schedule
- Media Inventory Record
- Media Restore Requests log
- Restore Test Evidence
- Backup Log
- Archived records

- Archive restoration log

O10 Business Continuity Management (including Disaster Recovery Planning):

- BCP Plan
- Fail-Over/Disaster Recovery Plans/Instructions
- Fail-Over/DR Test Protocols
- DR Test Exercise Protocol
- Updated DR Test Exercise Protocol
- BCP/DR Report

O11 Security Management:

- Starters, Leavers, and Movers Procedure
- IT Security Policy
- Guidelines for Use
- Patch Management Procedure
- Prevention and Detection Procedure
- Data Centre Access Policy
- Risk Register
- Security settings actually implemented in the system

O12 System Administration:

- SLA
- Support Schedule
- System Administration SOPs
- System Administration Records
- System Administration Log
- System user list
- User level matrix (matrix where the functions allowed to each user level are mapped)

D7 Data Migration (where applicable):

- Data Migration Plan
- Data Migration Report

The following topics do not have a dedicated appendix, but are covered in the appropriate sections of GAMP® 5 or associated Good Practice Guide (Reference 8, Appendix 4).

Training:

Training Records – should contain:

- Name of Trainee
- Name of Trainer/evidence of Trainer Qualification
- Title/Description of Training Course
- Date(s) of Training
- Evidence of completion
- Evidence of competence (where applicable)

Calibration:

- Calibration Policy
- Calibration Plan/Schedule
- Equipment Records
- Calibration Log
- Calibration Records including management of non-conformances

Application Specific Operational SOPs:

Other Life Cycle Documentation including Specification and Verification:

Other topics that may be checked/verified in the periodic review include:

- Regulation changes (have any changes being made to the applicable regulations and has an impact analysis been carried out on the system?)
- Business process changes
- Risk Management: the Periodic Review provides an opportunity to reconsider risk throughout the Operation Phase of the system. Areas to consider are:
  - Are previously agreed controls still effective?
  - Are any previously unrecognized hazards present?
  - Are any previously identified hazards no longer applicable?
  - If any estimated risk associated with a hazard is no longer acceptable?
  - If the original assessment is otherwise invalidated (e.g., following changes to applicable regulations or change of system use)

22 Appendix 4 – References

1. US FDA Code of Federal Regulations (CFR), Title 21, Food and Drugs, www.fda.gov.

    - Part 11: Electronic Records, Electronic Signatures
    - Part 820: Quality System Regulation (Medical Device)

2. Volume 4 – EU Good Manufacturing Practice (GMP) Guidelines: Volume 4 of "The rules governing medicinal products in the European Union" containing guidance for the interpretation of the principles and guidelines of good manufacturing practices for medicinal products for human and veterinary use laid down in Commission Directives 91/356/EEC, as amended by Directive 2003/94/EC, and 91/412/EEC respectively, and including Annex 11 – Computerized Systems.

3. ASTM Standard E2500, 2007, "Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment," ASTM International, West Conshohocken, PA, www.astm.org.

4. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management, July 2007, (ISO/IEC 27002), International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), www.iso.org and www.iec.ch.

5. *Quality Risk Management – Q9*, International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH), www.ich.org.

6. *Pharmaceutical Quality System – Q10*, International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH), www.ich.org.

7. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems*, International Society for Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, www.ispe.org.

8. *ISPE GAMP® Good Practice Guides*, International Society for Pharmaceutical Engineering (ISPE), www.ispe.org.

    - Calibration Management, December 2001
    - Global Information Systems Control and Compliance, November 2005
    - Risk-Based Approach to Compliant Electronic Records and Signatures, February 2005
    - Testing of GxP Systems, December 2005
    - IT Infrastructure Control and Compliance, September 2005
    - Electronic Data Archiving, July 2007

9. COBIT 4.1: *Control Objectives for Information and related Technology* (COBIT®), (2007) published by IT Governance Institute® (ITGI), www.itgi.org.

10. Service Management – ITIL® (IT Infrastructure Library) Version 3, 2007, published by Office of Government Commerce (OGC), www.itil-officialsite.com.

23 Appendix 5 – Glossary

23.1 Abbreviations and Acronyms

AER	Adverse Event Reporting
BCM	Business Continuity Management
BCP	Business Continuity Plan
CAPA	Corrective and Preventative Action
CI	Configuration Items
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DCS	Distributed Control System
DOS	Disk Operating System
DR	Disaster Recovery
DRP	Disaster Recovery Planning
DSS	Data Security Standards
ERP	Enterprise Resource Planning
FD&C	Food, Drug, and Cosmetic Act (US)
FISMA	Federal Information Security Management Act
FS	Functional Specification
FTP	File Transfer Protocol
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GEP	Good Engineering Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
HDS	Hardware Design Specification
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
ICH	International Conference on Harmonisation
ID	Identification

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineering
ISM	Information Security Management
ISO	International Standards Organization
IT	Information Technology
ITIL®	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
KPI	Key Performance Indicator
LAN	Local Area Network
LIMS	Laboratory Information Management System
NIST	National Institute for Standards and Technology
OGCS	A Risk-Based Approach to Operation of GxP Computerized Systems
PCI	Payment Card Industry
PDA	Parenteral Drug Association
PC	Personal Computer
PHS	Public Health Service
PLC	Programmable Logic Controller
QA	Quality Assurance
QM	Quality Management
QMS	Quality Management System
RACI	Responsible Accountable Consulted Informed
ROI	Return On Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDS	Software Design Specification
SLA	Service Level Agreement
SME	Subject Matter Expert
SOP	Standard Operating Procedures
SOX	Sarbanes-Oxley
URS	User Requirements Specification
WAN	Wide Area Network

23.2 Definitions

Audit (ISO)

Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which agreed criteria are fulfilled.

Backup

Differential Backup

A differential backup is a cumulative backup of all changes made after the last full backup. The advantage to this is the quicker recovery time as compared to Incremental Backup, requiring only a full backup and the latest differential backup to restore the system. The disadvantage is that for each day elapsed since the last full backup; more data needs to be backed up, especially if a majority of the data has been changed.

Full Backup

A full backup is the starting point for all other backups and is a complete backup of all system files irrespective of whether they have changed or not. A full backup takes a longer time to perform than incremental and differential backups and requires the largest amount of storage space. For this reason in most organizations, full backups are generally completed on a weekly or monthly schedule.

Incremental Backup

An incremental backup will only back up files that have been changed since the last backup of any type. This provides the quickest means of backup since it only makes copies of files that have not yet been backed up. The downside to this is that in order to perform a full restore, it is necessary to restore the last full backup first, followed by each of the subsequent incremental backups to the present day in the correct order. Should any one of these backup copies be damaged (particularly the full backup), the restore will be incomplete

Business Continuity Planning (ISO)

A managed process for developing and maintaining cross-organizational plans to counteract interruptions to business activities.

Change Control (PDA)

A formal process by which qualified representatives from appropriate disciplines review proposed or actual changes to a computer system. The main objective is to document the changes and ensure that the system is maintained in a state of control.

Computer System (IEEE)

A system containing one or more computers and associated software.

Computerized System

A broad range of systems including, but not limited to, automated manufacturing equipment, automated laboratory equipment, process control and process analytical, manufacturing execution, laboratory information management, manufacturing resource planning, clinical trials data management, vigilance and document management systems.

The computerized system consists of the hardware, software, and network components, together with the controlled functions and associated documentation.

Computerized System Validation

Achieving and maintaining compliance with applicable GxP regulations and fitness for intended use by:

- the adoption of principles, approaches, and life cycle activities within the framework of validation plans and reports
- the application of appropriate operational controls throughout the life of the system

Design Review (IEEE)

A process or meeting during which a system, hardware, or software design is presented to project personnel, managers, users, customers, or other interested parties for comment or approval. Types include critical design review, preliminary design review, and system design review.

Electronic Production Record

A record that is a store of data and information from production-related activities created by and/or manually entered into systems, typically during execution of control recipes. The EPR may be located in one or more systems or databases.

GxP Compliance

Meeting all applicable pharmaceutical and associated life-science regulatory requirements.

GxP Regulated Computerized System

Computerized systems that are subject to GxP regulations. The regulated company must ensure that such systems comply with the appropriate regulations.

GxP Regulation

The underlying international pharmaceutical requirements, such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese regulations, or other applicable national legislation or regulations under which a company operates. These include but are not limited to:

- Good Manufacturing Practice (GMP) (pharmaceutical, including Active Pharmaceutical Ingredient (API), veterinary, and blood)
- Good Clinical Practice (GCP)
- Good Laboratory Practice (GLP)
- Good Distribution Practice (GDP)
- Good Quality Practice (GQP)
- Good Pharmacovigilance Practice
- Medical Device Regulations
- Prescription Drug Marketing Act (PDMA)

Harm (ICH Q9)

Damage to health, including the damage that can occur from loss of product quality or availability.

Hazard (ICH Q9)

The potential source of harm (ISO/IEC Guide 51).

Incident

Operational event which is not part of standard operation.

Network (ISO)

A system [transmission channels and supporting hardware and software] that connects several remotely located computers via telecommunications.

Periodic Review

A documented assessment of the documentation, procedures, records, and performance of a computer system to determine whether it is still in a validated state and what actions, if any, are necessary to restore its validated state. The frequency of review is dependent upon the systems complexity, criticality, and rate of change.

Pharmacovigilance

Detection, assessment, understanding, and prevention of adverse effects, particularly long term and short term side effect, of medicines.

Process (ISO)

A set of interrelated or interacting activities which transform inputs into outputs.

Process Owner

The person ultimately responsible for the business process or processes being managed.

Product Lifecycle (ICH Q9)

All phases in the life of the product from the initial development through marketing until the product's discontinuation.

Quality (ICH Q9)

The degree to which a set of inherent properties of a product, system, or process fulfills requirements (see ICH Q6a definition specifically for "quality" of drug substance and drug (medicinal) products.)

Quality (Product) (ICH Q8)

The suitability of either a drug substance or drug product for its intended use. This term includes such attributes as the identity, strength, and purity (from ICH Q6A Specifications: Test Procedures and Acceptance Criteria for New Drug Substances and New Drug Products: Chemical Substances).

Quality Management System (ISO)

Management system to direct and control an organization with regard to quality.

Quality Plan (ISO)

Document specifying which procedures and associated resources shall be applied by whom and when to a specific project, product, process, or contract.

Quality Risk Management (ICH Q9)

A systematic process for the assessment, control, communication, and review of risks to the quality of the drug (medicinal) product across the product lifecycle.

Quality System (ICH Q9)

The sum of all aspects of a system that implements quality policy and ensures that quality objectives are met.

Requirement (ISO)

Need or expectation that is stated, generally implied, or obligatory.

Risk (ICH Q9)

The combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51).

Risk Analysis (ICH Q9)

The estimation of the risk associated with the identified hazards.

Risk Assessment (ICH Q9)

A systematic process of organizing information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.

Software Life Cycle (NIST)

Period of time beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases denoting activities, such as requirements, design, programming, testing, installation, and operation and maintenance.

Specification (IEEE)

A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component, and often, the procedures for determining whether these provisions have been satisfied.

Subject Matter Expert

Those individuals with specific expertise in a particular area or field. Subject Matter Experts should take the lead role in the verification of computerized systems. Subject Matter Expert responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results.

Supplier

An organization or individual internal or external to the user associated with the supply and/or support of products or services at any phase throughout a systems life cycle.

System Owner

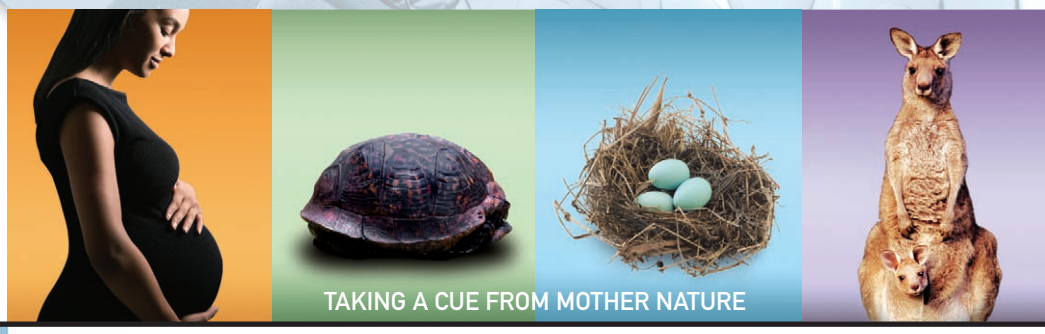
The person ultimately responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system.

User

The pharmaceutical customer or user organization contracting a supplier to provide a product. Therefore, in the context of this document it is not intended to apply only to individuals who use the system, and is synonymous with customer.

Weiler Engineering...IT'S SAFER INSIDE

1395 Gateway Drive
Elgin, Illinois 60124 USA
PHONE: **847-697-4900**
FAX: **847-697-4915**



Corporate Description

Weiler Engineering, a leading provider of aseptic custom packaging equipment for pharmaceutical and healthcare applications, has virtually eliminated contamination concerns.

Committed to the highest standards of excellence and to further expanding products and systems to enhance patient care, Weiler's proprietary ASEP-TECH® Blow/Fill/Seal packaging machines produce shatterproof, durable, aseptically-packaged products in one uninterrupted operation. This hands-free manufacturing process ensures parenterals, ophthalmic solutions, and respiratory drugs reach the marketplace in the most sterile, cost-effective manner possible—every time.

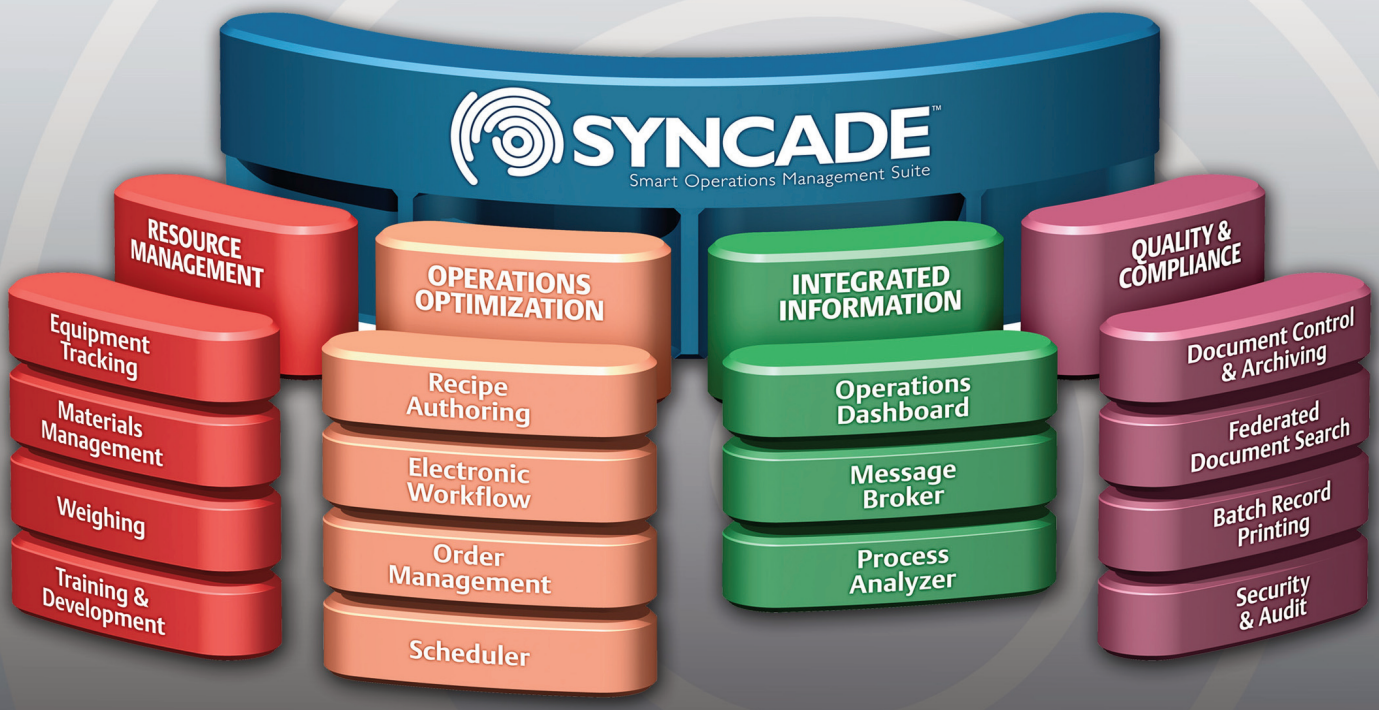
The ASEP-TECH® System is the culmination of 40 years of innovation in machine design and sterile process development, producing the most advanced aseptic liquid packaging process available today.

WEILER®

Safeguarding solutions through innovative packaging

www.asep-tech.com

When quality, efficiency and compliance matter.



Syncade™

Smart Operations Management Suite

Syncade Smart Operations Management Suite helps you work smarter. By replacing paper-driven operations with an electronic manufacturing system, the Syncade suite increases plant-wide operational efficiency by integrating work activities with real-time information, assuring consistent production is performed right the first time. Increase productivity and profitability, visit: **www.EmersonProcess.com/Syncade** or contact: **Syncade@emerson.com**

SYNCADE™
Smart Operations Management Suite

EMERSON™
Process Management

EMERSON. CONSIDER IT SOLVED.™