Co-managed IT responsibility matrix for life-science companies

Who does what between in-house IT and a co-managed IT provider, including GxP and 21 CFR Part 11 duties. The spreadsheet version has a drop-down in every role cell, a one-A check per row and a notes column.

What this is. A responsibility matrix (RACI) for a life-science company that uses co-managed IT: an outside IT provider working alongside in-house IT staff. It covers help desk, endpoints, Microsoft 365, backups, GxP system validation support, Part 11 access reviews, change control, incident response and vendor management, with the record each activity should leave behind.

How to read R, A, C and I. R = responsible: does the work. A = accountable: answers for the outcome and signs off; each row has exactly one A. C = consulted before the work is done. I = informed after. '-' = not involved. 'R/A' means the same party does the work and signs off. The 'One A?' column checks each row.

The letters are a starting point. The four role columns are pre-filled with a common starting point for a company with one or a few internal IT staff. They are not a rule and not a recommendation for your company. Every role cell has a drop-down and can be changed; clear the columns if you prefer to start blank. Add rows above row 300 to keep the drop-downs and the check column. CISA's guidance for managed service provider customers says the balance of responsibilities 'should be jointly agreed to by customers and vendors', and that outsourcing 'does not absolve an organization from risk management responsibilities associated with the IT enterprise'.

Why GxP rows need a named owner. EU GMP Annex 11 expects close cooperation between the process owner, system owner, qualified persons and IT, and says all personnel should have defined responsibilities (section 2). It also requires formal agreements with third parties that maintain computerised systems, with clear statements of their responsibilities, and says IT departments should be considered analogous (section 3.1). In other words, your own IT team needs written responsibilities too.

Who owns validation. The regulated company does. ISPE's GAMP 5 summary puts it plainly: 'Ensuring compliance and fitness for purpose is the responsibility of the regulated company.' Under GMP, the quality unit approves validation plans, risk assessments, test results and release, and the system or process owner runs the work; under GLP or GCP, set the approving roles as your procedures require (for example, a GLP quality assurance unit audits independently). Some companies make the process owner accountable, with quality unit approval as a required signature; set the letters to match your procedures. In-house IT and the co-managed provider supply controlled infrastructure, documented procedures and objective evidence. LAN Service Group does not validate your systems for you and does not decide whether they comply.

Part 11 scope. 21 CFR Part 11 applies to electronic records kept under FDA record requirements (predicate rules such as Parts 211, 820 and 58), to electronic records submitted to FDA, and to electronic signatures (11.1). FDA's 2003 scope and application guidance reads this narrowly and says FDA does 'not intend to take enforcement action to enforce compliance with the validation, audit trail, record retention, and record copying requirements of part 11 as explained in this guidance', and also exercises broader discretion for systems in use before August 20, 1997 that meet criteria set out in the guidance. Predicate-rule requirements, including their own validation and record requirements, and the other Part 11 controls (such as access limits, authority checks, training and signature controls) still apply. Rows citing 11.10(a), (c), (e) or (k)(2) are labelled 'within FDA's 2003 enforcement discretion'; for those, the binding expectation usually comes from the predicate rule. Check with your quality unit which of your systems are in scope.

How often to review access. Part 11 requires access to be limited to authorized individuals (11.10(d)) and, for password-based electronic signatures, identification codes and passwords to be periodically checked (11.300(b)); Annex 11 expects access to be restricted and access changes to be recorded (12.1, 12.3). Neither text sets a frequency for periodic access reviews, or uses that term. Set the frequency in your procedures, based on risk.

Change approvals. The matrix splits GxP changes in two: the provider prepares the technical impact assessment, and the system owner assesses the GxP impact with quality unit approval. If your procedures let the system owner approve low-risk changes, change the letters and note it.

What the References column means. Each reference is the clause or guidance topic the row supports, quoted in full on the References sheet. Every quote was checked word for word against the source text when the file was built. A reference is a pointer, not a compliance mapping: meeting a row does not by itself meet the clause. Rows without a reference are common IT practice and are not drawn from a regulation.

GAMP 5 terms. Role names (quality unit, process owner, system owner, subject matter expert) and appendix names and numbers (for example O2 Establishing and Managing Support Services, O4 Incident Management, O5 Corrective and Preventive Action, O6 Operational Change and Configuration Management, O8 Periodic Review, O9 Backup and

Restore, O10 Business Continuity Management, O11 Security Management, M2 Supplier Assessment, S4 Patch Management, S5 Managing Quality within an Outsourced IS/IT Environment) follow ISPE's published GAMP 4 to GAMP 5 summary (2008). The GAMP 5 Guide itself is a paid ISPE publication and is not quoted here. ISPE's 2nd Edition page says suppliers include 'IT service providers, and IT support services, both internal and external to the regulated company'; we have not checked the 2nd Edition's appendix list, which ISPE says was expanded, so check numbering in your copy.

Which rules apply to you. Annex 11 and FDA's data integrity Q&A are written for medicine manufacturing (GMP). Device manufacturers work under 21 CFR Part 820; GLP laboratories under 21 CFR Part 58 and the OECD GLP Principles; clinical work under GCP. Part 11 applies where FDA predicate rules (for example 21 CFR Parts 211, 820, 58 or 312) require the records or signatures and you keep them electronically, and to electronic records submitted to FDA; it does not govern OECD GLP or EU GCP work as such. If the GMP references do not apply to you, use them as good practice, not as your rule set.

Not legal or regulatory advice. This is a planning template. Your quality unit and your procedures decide what applies. Confirm requirements against the current sources; EU Annex 11 has been under revision, so check the European Commission site for the version in force.

About LAN Service Group. Prepared by LAN Service Group, Inc., headquartered in San Ramon, California, in the San Francisco Bay Area, serving clients across the United States and in major international cities. LAN Service Group provides co-managed IT alongside in-house IT teams as well as fully outsourced IT.
https://www.lansg.com/co-managed-it-life-sciences/

Licence. You may copy, edit and use this template inside your organization.

Version. Version 1.0, October 2026. References checked against the source documents on October 20, 2026.

Help desk

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
HD-01	First contact for user requests (phone, email, portal) during business hours	**R/A**	**C**	**-**	**-**	Ticket record with requester, owner and timestamps	GAMP 5 (2008) Appendix O2: Establishing and Managing Support Services
HD-02	After-hours and overflow tickets	**A**	**R**	**-**	**-**	Ticket record; hand-back note to in-house IT	GAMP 5 (2008) Appendix O2: Establishing and Managing Support Services
HD-03	Routing rules, escalation paths, hours covered and response targets by priority, written into the agreement	**A**	**R**	**I**	**-**	Agreed routing and escalation document (version-controlled)	GAMP 5 (2008) Appendix O2: Establishing and Managing Support Services
HD-04	Escalation of scientific and quality application issues (for example ELN, LIMS, QMS) to the software vendor	**R**	**C**	**A**	**I**	Ticket linked to the vendor case	Common IT practice
HD-05	Tickets that change a GxP system or grant access to one reference the change control or access record and close only when that record is complete	**A**	**R**	**C**	**I**	Ticket cross-referenced to the change or access record	EU GMP Annex 11, section 10 (Change and configuration management); EU GMP Annex 11, section 12.3
HD-06	Monthly or quarterly service review: ticket volumes, missed targets, open changes, access reviews, backup test results	**A**	**R**	**C**	**C**	Service review report and minutes	GAMP 5 (2008) Appendix O2: Establishing and Managing Support Services

Endpoints and patching

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
EP-01	Device build, enrolment and asset inventory for office laptops and desktops	**A**	**R**	**-**	**-**	Asset inventory export	Common IT practice
EP-02	Operating system and application patching for office devices, with compliance reporting	**A**	**R**	**-**	**-**	Patch compliance report	Common IT practice
EP-03	Lab and instrument PCs: updates only after instrument vendor and quality review; written list of devices excluded from automatic updates and why	**R**	**C**	**A**	**C**	Exclusion list with rationale; change record for each approved update	EU GMP Annex 11, section 10 (Change and configuration management); GAMP 5 (2008) Appendix S4: Patch Management
EP-04	Endpoint protection (antivirus/EDR) deployment and alert triage	**A**	**R**	**-**	**-**	Endpoint protection console report; alert tickets	Common IT practice
EP-05	Disk encryption, and wiping or destroying devices at retirement	**A**	**R**	**-**	**-**	Encryption report; disposal record or wipe log	Common IT practice
EP-06	Changes to office IT that do not touch GxP systems: standard change process and shared change calendar	**A**	**R**	**-**	**-**	Change tickets; change calendar	Common IT practice

Microsoft 365 and identity

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
MS-01	Tenant security baseline: MFA, Conditional Access, admin roles, external sharing defaults	**A**	**R**	**-**	**-**	Baseline document and configuration export	GAMP 5 (2008) Appendix O11: Security Management
MS-02	Business decisions on groups, Teams, sharing and licences	**R/A**	**C**	**C**	**-**	Approved request or decision record	Common IT practice
MS-03	Joiner, mover and leaver account changes, from an approved HR or manager request	**A**	**R**	**I**	**-**	Request and completion record with dates	EU GMP Annex 11, section 12.3
MS-04	Named administrator accounts for each person on both sides, separate from everyday accounts; no shared admin logins	**A**	**R**	**-**	**I**	Admin account list with owner per account	Common IT practice
MS-05	Sign-in and audit log monitoring, and log retention settings	**A**	**R**	**-**	**-**	Retention settings export; alert tickets	Common IT practice
MS-06	Retention and deletion policies for Microsoft 365 content that holds regulated records	**R**	**C**	**A**	**C**	Approved retention schedule and policy export	21 CFR 11.10(c) (within FDA's 2003 enforcement discretion)

Backups and restores

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
BK-01	Decide what must be backed up and how long it is kept, from the record retention requirements	**R**	**C**	**A**	**C**	Backup scope and retention schedule	21 CFR 11.10(c) (within FDA's 2003 enforcement discretion); GAMP 5 (2008) Appendix O9: Backup and Restore
BK-02	Run backups and monitor job success; fix failed jobs	**A**	**R**	**-**	**-**	Backup job reports; tickets for failures	GAMP 5 (2008) Appendix O9: Backup and Restore
BK-03	Periodic restore tests, including systems that hold GxP data, with documented results	**A**	**R**	**C**	**I**	Restore test record (what, when, who, result), including the owner's check that restored GxP data is complete and readable	EU GMP Annex 11, section 7.2; GAMP 5 (2008) Appendix O9: Backup and Restore
BK-04	Backup copies protected from alteration and loss (separate location, restricted access)	**A**	**R**	**-**	**-**	Backup architecture description; access list for backup systems	21 CFR 11.10(c) (within FDA's 2003 enforcement discretion)
BK-05	Business continuity and recovery arrangements for systems that support critical processes	**R**	**C**	**A**	**C**	Continuity plan and test record	EU GMP Annex 11, section 16 (Business continuity); GAMP 5 (2008) Appendix O10: Business Continuity Management

GxP system validation support (GxP)

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
VS-01	Validation plans, risk assessments, test results and release of GxP computerised systems	C	C	R	A	Approved validation plan, risk assessment, test evidence and report	21 CFR 11.10(a) (within FDA's 2003 enforcement discretion); ISPE GAMP 4 to GAMP 5 Summary (2008); ISPE GAMP 4 to GAMP 5 Summary (2008): roles
VS-02	Infrastructure build and configuration records for servers, virtual hosts, network and operating systems under GxP applications, in the form your qualification procedure requires	R	R	C	A	Build and configuration records referenced by the qualification approved under your procedure	EU GMP Annex 11, Principle
VS-03	Objective evidence on request: installation records, configuration exports, logs and test output	A	R	C	I	Evidence package referenced by the validation record	EU GMP Annex 11, Principle; 21 CFR 11.10(a) (within FDA's 2003 enforcement discretion)
VS-04	Up-to-date inventory of computerised systems and their GxP functionality	R	C	A	C	System inventory	EU GMP Annex 11, section 4.3
VS-05	Periodic review of each GxP system to confirm it remains in a valid state and compliant with applicable GxP requirements (Annex 11 section 11 says 'compliant with GMP')	C	C	R	A	Periodic review report	EU GMP Annex 11, section 11 (Periodic evaluation); GAMP 5 (2008) Appendix O8: Periodic Review
VS-06	Time synchronisation of servers and clients so audit-trail time stamps are reliable	A	R	I	-	Time source configuration record	21 CFR 11.10(e) (within FDA's 2003 enforcement discretion)
VS-07	Each party keeps training records for its own staff who maintain GxP systems; the company determines they are adequate	R	R	A	C	Training records per person	21 CFR 11.10(i); EU GMP Annex 11, section 2 (Personnel)
VS-08	Handover of a new or changed system into support (documentation, support procedures, access)	R	R	A	C	Handover record	EU GMP Annex 11, section 2 (Personnel); GAMP 5 (2008) Appendix O1: Handover

Part 11 access reviews (GxP)

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
AR-01	Grant, change and remove GxP application access only from an approved request	R	R	A	I	Access request with approval and completion	21 CFR 11.10(d); EU GMP Annex 11, section 12.3
AR-02	Periodic review of who has access to each GxP application and with which role (frequency set by your procedures)	R	C	A	C	Signed access review with corrections made	21 CFR 11.10(d); 21 CFR 11.10(g); FDA, Data Integrity and Compliance With Drug CGMP Q&A (2018), question 4

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
AR-03	Periodic review of privileged and administrator access to GxP servers, databases and backup systems (the provider supplies the account export; no party confirms its own administrator accounts, for example the system owner confirms in-house IT's and the provider's accounts)	**R/A**	**C**	**C**	**I**	Privileged access review record	21 CFR 11.10(d); EU GMP Annex 11, section 12.1; FDA, Data Integrity and Compliance With Drug CGMP Q&A (2018), question 4 (administrator independence)
AR-04	Unique named accounts for every user; no shared logins for review, approval or data changes	**R**	**R**	**A**	**C**	Account list; exceptions documented	FDA, Data Integrity and Compliance With Drug CGMP Q&A (2018), question 5; 21 CFR 11.100(a) (electronic signatures)
AR-05	For systems using ID-code/password electronic signatures: password and identification-code controls, periodic checks or changes, and prompt disabling of lost or compromised tokens and devices	**A**	**R**	**I**	**-**	Password policy export; token or device loss tickets	21 CFR 11.300(b) (ID-code/password electronic signatures); 21 CFR 11.300(c) (ID-code/password electronic signatures)
AR-06	Remove leavers' access to GxP systems promptly and record when it was done	**R**	**R**	**A**	**I**	Leaver checklist with removal dates	EU GMP Annex 11, section 12.3

Change control (GxP)

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
CC-01	Change requests for GxP systems and their infrastructure (patches, configuration, backup schedule): technical impact assessment (what changes, risk to availability, rollback)	**C**	**R**	**A**	**I**	Change request with technical impact assessment	EU GMP Annex 11, section 10 (Change and configuration management); GAMP 5 (2008) Appendix O6: Operational Change and Configuration Management; GAMP 5 (2008) Appendix S4: Patch Management
CC-02	GxP impact assessment of the change (effect on validated state, records and regulated processes), testing needed, and approval before the change	**C**	**C**	**R**	**A**	Change record with GxP impact assessment and approvals (your procedures may let the system owner approve low-risk changes)	EU GMP Annex 11, section 10 (Change and configuration management); 21 CFR 11.10(k)(2) (change control of systems documentation; within FDA's 2003 enforcement discretion); GAMP 5 (2008) Appendix O6: Operational Change and Configuration Management
CC-03	Execute the approved change and record what was done and when	**C**	**R**	**A**	**I**	Completed change record with evidence	EU GMP Annex 11, section 10 (Change and configuration management); GAMP 5 (2008) Appendix O6: Operational Change and Configuration Management

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
CC-04	Emergency changes: documented and reviewed afterwards	**C**	**R**	**A**	**C**	Emergency change record and retrospective review	EU GMP Annex 11, section 10 (Change and configuration management)
CC-05	Configuration baselines for GxP infrastructure kept current	**A**	**R**	**C**	**-**	Configuration baseline record	EU GMP Annex 11, section 10 (Change and configuration management); GAMP 5 (2008) Appendix O6: Operational Change and Configuration Management

Incident response

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
IR-01	Security monitoring, alert triage and technical response	**A**	**R**	**-**	**-**	Alert and incident tickets	GAMP 5 (2008) Appendix O4: Incident Management
IR-02	Incident lead and business decisions during an incident	**R/A**	**R**	**C**	**I**	Incident log with decisions and times	GAMP 5 (2008) Appendix O4: Incident Management
IR-03	Incidents affecting GxP systems or data: reported, assessed for data integrity impact and fed into deviation and CAPA handling	**C**	**C**	**R**	**A**	Deviation or CAPA record linked to the incident	EU GMP Annex 11, section 13 (Incident management); GAMP 5 (2008) Appendix O5: Corrective and Preventive Action
IR-04	Incident response plan kept current and exercised	**A**	**R**	**C**	**C**	Plan version and exercise record	Common IT practice
IR-05	Notifications to customers, partners, insurers or law enforcement	**C**	**I**	**R/A**	**C**	Notification decision record (management and legal as your procedures require)	Common IT practice
IR-06	Decision whether a GxP incident needs a regulatory report, and the report itself	**C**	**I**	**C**	**R/A**	Reportability assessment and any report filed (quality and regulatory affairs per your procedures)	Common IT practice

Vendor management

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
VM-01	Written agreement setting out the provider's responsibilities, with a quality or technical agreement for GxP work	**R**	**C**	**C**	**A**	Signed agreement and approved quality/technical agreement	EU GMP Annex 11, section 3.1 (Suppliers and service providers); GAMP 5 (2008) Appendix S5: Managing Quality within an Outsourced IS/IT Environment

Ref	Activity	In-house IT	LAN Service Group	System or process owner	Quality unit	Record it should leave	References
VM-02	Assessment and qualification of the co-managed provider, and of your own IT team, as GxP suppliers	**C**	**C**	**R**	**A**	Supplier assessment record	EU GMP Annex 11, section 3.2; ISPE, GAMP 5 Guide 2nd Edition (publication page); GAMP 5 (2008) Appendix M2: Supplier Assessment; GAMP 5 (2008) Appendix S5: Managing Quality within an Outsourced IS/IT Environment
VM-03	List of the provider's subcontractors and cloud services that touch company data, kept current	**A**	**R**	**-**	**I**	Subprocessor and tools list	EU GMP Annex 11, section 3.1 (Suppliers and service providers)
VM-04	Collect and review independent reports (for example SOC reports or ISO certificates) for the provider's key tools and cloud services, where they exist	**R/A**	**C**	**-**	**C**	Report files and review notes	GAMP 5 (2008) Appendix M2: Supplier Assessment
VM-05	Support contracts and contacts for scientific software and instrument vendors	**C**	**I**	**R/A**	**-**	Vendor contact and contract register	Common IT practice
VM-06	Exit and handover if the contract ends: documentation, credentials and records returned	**A**	**R**	**C**	**C**	Signed handover checklist	EU GMP Annex 11, section 3.1 (Suppliers and service providers)

RACI key

R = responsible (does the work). A = accountable (answers for the outcome and signs off; exactly one per row). C = consulted before. I = informed after. - = not involved. The letters are a common starting point; change them to fit your company.

References (each quote checked word for word against the source)

Key	Citation	Wording in the source
A11-10	EU GMP Annex 11, section 10 (Change and configuration management)	Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.
A11-11	EU GMP Annex 11, section 11 (Periodic evaluation)	Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.
A11-12.1	EU GMP Annex 11, section 12.1	Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons.
A11-12.3	EU GMP Annex 11, section 12.3	Creation, change, and cancellation of access authorisations should be recorded.
A11-13	EU GMP Annex 11, section 13 (Incident management)	All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.
A11-16	EU GMP Annex 11, section 16 (Business continuity)	provisions should be made to ensure continuity of support for those processes in the event of a system breakdown
A11-2	EU GMP Annex 11, section 2 (Personnel)	All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.
A11-3.1	EU GMP Annex 11, section 3.1 (Suppliers and service providers)	formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.
A11-3.2	EU GMP Annex 11, section 3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.
A11-4.3	EU GMP Annex 11, section 4.3	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.
A11-7.2	EU GMP Annex 11, section 7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.
A11-GLOSS	EU GMP Annex 11, Glossary	Process owner: The person responsible for the business process. System owner: The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.
A11-P	EU GMP Annex 11, Principle	The application should be validated; IT infrastructure should be qualified.
CISA-ABSOLVE	CISA Insights, Risk Considerations for Managed Service Provider Customers	does not absolve an organization from risk management responsibilities associated with the IT enterprise
CISA-SPLIT	CISA Insights, Risk Considerations for Managed Service Provider Customers	The specific balance of responsibilities between a customer and a vendor will depend on several factors and should be jointly agreed to by customers and vendors
FDA-DI-4	FDA, Data Integrity and Compliance With Drug CGMP Q&A (2018), question 4	establish and implement a method for documenting authorized personnel's access privileges for each CGMP computer system in use
FDA-DI-4b	FDA, Data Integrity and Compliance With Drug CGMP Q&A (2018), question 4 (administrator independence)	The system administrator role, including any rights to alter files and settings, should be assigned to personnel independent from those responsible for the record content.
FDA-DI-5	FDA, Data Integrity and Compliance With Drug CGMP Q&A (2018), question 5	When login credentials are shared, a unique individual cannot be identified through the login and the system would not conform to the CGMP requirements in parts 211 and 212.
FDA-P11-ED	FDA, Part 11 Scope and Application guidance (2003)	we do not intend to take enforcement action to enforce compliance with the validation, audit trail, record retention, and record copying requirements of part 11 as explained in this guidance

Key	Citation	Wording in the source
GAMP-M-SA	GAMP 5 (2008) Appendix M2: Supplier Assessment	Appendix M2 Supplier Assessment
GAMP-O-BCM	GAMP 5 (2008) Appendix O10: Business Continuity Management	Appendix O10 Business Continuity Management
GAMP-O-BR	GAMP 5 (2008) Appendix O9: Backup and Restore	Appendix O9 Backup and Restore
GAMP-O-CAPA	GAMP 5 (2008) Appendix O5: Corrective and Preventive Action	Appendix O5 Corrective and Preventive Action
GAMP-O-CHG	GAMP 5 (2008) Appendix O6: Operational Change and Configuration Management	Appendix O6 Operational Change and Configuration Management
GAMP-O-HO	GAMP 5 (2008) Appendix O1: Handover	Appendix O1 Handover
GAMP-O-INC	GAMP 5 (2008) Appendix O4: Incident Management	Appendix O4 Incident Management
GAMP-O-PR	GAMP 5 (2008) Appendix O8: Periodic Review	Appendix O8 Periodic Review
GAMP-O-SEC	GAMP 5 (2008) Appendix O11: Security Management	Appendix O11 Security Management
GAMP-O-SUPPORT	GAMP 5 (2008) Appendix O2: Establishing and Managing Support Services	Appendix O2 Establishing and Managing Support Services
GAMP-REGCO	ISPE GAMP 4 to GAMP 5 Summary (2008)	Ensuring compliance and fitness for purpose is the responsibility of the regulated company.
GAMP-ROLES	ISPE GAMP 4 to GAMP 5 Summary (2008): roles	Clarifying the role of the Quality Unit, and introducing the roles of Process Owner, System Owner, and Subject Matter Experts
GAMP-S4	GAMP 5 (2008) Appendix S4: Patch Management	Appendix S4 Patch Management
GAMP-S5	GAMP 5 (2008) Appendix S5: Managing Quality within an Outsourced IS/IT Environment	Appendix S5 Managing Quality within an Outsourced IS/IT Environment
GAMP-SUP	ISPE, GAMP 5 Guide 2nd Edition (publication page)	Suppliers include providers of software, hardware, equipment, system integration services, IT service providers, and IT support services, both internal and external to the regulated company.
P11-100a	21 CFR 11.100(a) (electronic signatures)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
P11-10a	21 CFR 11.10(a) (within FDA's 2003 enforcement discretion)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
P11-10c	21 CFR 11.10(c) (within FDA's 2003 enforcement discretion)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.
P11-10d	21 CFR 11.10(d)	Limiting system access to authorized individuals.
P11-10e	21 CFR 11.10(e) (within FDA's 2003 enforcement discretion)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.
P11-10g	21 CFR 11.10(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
P11-10i	21 CFR 11.10(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
P11-10k	21 CFR 11.10(k)(2) (change control of systems documentation; within FDA's 2003 enforcement discretion)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
P11-300b	21 CFR 11.300(b) (ID-code/password electronic signatures)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised
P11-300c	21 CFR 11.300(c) (ID-code/password electronic signatures)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information

Sources

eCFR: 21 CFR Part 11, Electronic Records; Electronic Signatures: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11

European Commission: EudraLex Volume 4, Annex 11, Computerised Systems (2011): https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf

FDA guidance: Data Integrity and Compliance With Drug CGMP, Questions and Answers (2018): https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers

FDA guidance: Part 11, Electronic Records; Electronic Signatures, Scope and Application (2003): https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

ISPE: GAMP 5 Guide, 2nd Edition (publication page): https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition

ISPE: GAMP 4 to GAMP 5 Summary (2008), table of contents, published via Techstreet: https://images.techstreet.com/direct/tocs/ISPE/ISPE_GAMP_4-5_sum.pdf

CISA Insights: Risk Considerations for Managed Service Provider Customers: https://www.cisa.gov/sites/default/files/publications/cisa-insights_risk-considerations-for-msp-customers_508.pdf