Regulatory Audit Readiness Checklist for Life Science Firms

A Comprehensive Guide for Life Science Executives

This checklist is designed to provide Life Science Executives, such as CEOs, CFOs, COOs, and CSOs, with a clear and actionable framework for preparing their organizations for critical regulatory audits. It focuses on the IT security aspects, data integrity, and system validation essential across the entire research-to-commercialization journey, ensuring clarity on compliance exposure and fostering proactive security readiness.

Key Terms and Acronyms

To ensure clarity, here are definitions for key terms and acronyms used throughout this checklist:

- **21 CFR Part 11:** Code of Federal Regulations Title 21, Part 11. This FDA regulation sets forth the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records and handwritten signatures.
- **AI (Artificial Intelligence):** The simulation of human intelligence processes by machines, especially computer systems. In this context, it refers to the secure adoption and management of AI technologies.
- **ALCOA+C:** An acronym representing the principles of data integrity: **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, **A**ccurate, plus **C**omplete, **C**onsistent, **E**nduring, and **A**vailable.
- **APIs (Application Programming Interfaces):** Sets of definitions and protocols for building and integrating application software.
- **CDMOs (Contract Development and Manufacturing Organizations):** Organizations that provide comprehensive services from drug development through manufacturing.
- **CFO (Chief Financial Officer):** A senior executive responsible for managing the financial actions of a company.
- **CIO (Chief Information Officer):** A senior executive responsible for the information technology and computer systems that support enterprise goals.
- **CISO (Chief Information Security Officer):** A senior executive responsible for developing and implementing an information security program.
- **CIS (Center for Internet Security):** A non-profit organization that develops best practices for cybersecurity.
- **CMOs (Contract Manufacturing Organizations):** Organizations that provide manufacturing services for the pharmaceutical industry.
- **COO (Chief Operating Officer):** A senior executive responsible for the day-to-day operation of a company.

- **CROs (Contract Research Organizations):** Organizations that provide support to the pharmaceutical, biotechnology, and medical device industries in the form of research services.
- **CSO (Chief Scientific Officer):** A senior executive responsible for the scientific and research activities of a company.
- **DRP (Disaster Recovery Plan):** A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
- **EDR (Endpoint Detection and Response):** A cybersecurity solution that continuously monitors and collects data from endpoint devices to detect and respond to threats.
- **EHR (Electronic Health Record):** A digital version of a patient’s paper chart.
- **FDA (Food and Drug Administration):** A federal agency responsible for protecting public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices.
- **GDPR (General Data Protection Regulation):** A comprehensive data protection law in the European Union that governs how personal data of EU citizens is collected, processed, and stored.
- **GxP (Good Practice Regulations):** A collection of quality guidelines and regulations for various regulated industries, including Good Clinical Practice (GCP), Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP), and Good Pharmacovigilance Practice (GVP). The overall intent is to ensure food and medical products are safe and data integrity is maintained.
- **HIPAA (Health Insurance Portability and Accountability Act):** A U.S. law that sets standards for protecting sensitive patient health information.
- **HITRUST (Health Information Trust Alliance):** A common security framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management.
- **IDS/IPS (Intrusion Detection System/Intrusion Prevention System):** Network security technologies that monitor network traffic for suspicious activity and take action to prevent or alert on threats.
- **IP (Intellectual Property):** Creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. In life sciences, this often refers to proprietary research, drug formulas, or biotechnological innovations.
- **IRP (Incident Response Plan):** A documented set of procedures for identifying, containing, and recovering from cybersecurity incidents.
- **IT (Information Technology):** The use of computers, storage, networking, and other physical devices, infrastructure, and processes to create, process, store, secure, and exchange all forms of electronic data.
- **MFA (Multi-Factor Authentication):** A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.
- **NIST (National Institute of Standards and Technology):** A U.S. agency that develops technology, measurements, and standards, including cybersecurity frameworks.
- **PHI (Protected Health Information):** Any health information that can be linked to an individual.

- **R&D (Research & Development):** Activities undertaken by companies in the pursuit of innovation, often involving scientific or technological advancements.
- **ROI (Return on Investment):** A performance measure used to evaluate the efficiency or profitability of an investment.
- **RPO (Recovery Point Objective):** The maximum tolerable period in which data might be lost from an IT service due to a major incident.
- **RTO (Recovery Time Objective):** The maximum tolerable duration of time that a computer, system, application, or network can be down after a disaster.
- **SaaS (Software as a Service):** A software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.
- **SMBs (Small and Midsize Businesses):** Businesses that maintain revenues, assets, or a number of employees below a certain threshold.
- **SOC 2 (Service Organization Control 2):** An auditing procedure that ensures your service providers securely manage your data to protect the interests of your organization and the privacy of its clients. It focuses on five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.
- **SOPs (Standard Operating Procedures):** Step-by-step instructions compiled by an organization to help workers carry out complex routine operations.
- **TSC (Trust Services Criteria):** A set of principles and controls developed by the American Institute of Certified Public Accountants (AICPA) that form the basis of SOC 2.

Section 1: General IT Security & Data Integrity Foundations

Before diving into specific regulations, ensure your foundational IT security and data integrity practices are robust.

- **Data Inventory & Classification:**
  - [ ] Have all sensitive Intellectual Property (IP) and Research & Development (R&D) data been identified and classified (e.g., confidential, restricted)?
  - [ ] Is there a clear understanding of where all critical data resides (on-premise, cloud, third-party vendors)?
  - [ ] Are data retention policies defined and enforced for all data types?
- **Access Control & Authentication:**
  - [ ] Is Multi-Factor Authentication (MFA) enforced for all critical systems and remote access?
  - [ ] Are access privileges regularly reviewed and aligned with the principle of least privilege?
  - [ ] Is there a robust process for onboarding and offboarding users, ensuring timely access revocation?
- **Network Security:**
  - [ ] Are network segmentation strategies implemented to isolate critical systems and data?

  - [ ] Are firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint detection and response (EDR) solutions properly configured and monitored?
  - [ ] Is there a regular vulnerability scanning and penetration testing program in place?
- **Backup & Disaster Recovery:**
  - [ ] Are comprehensive data backup and recovery plans documented, tested, and regularly updated?
  - [ ] Is there a robust disaster recovery plan (DRP) that includes IT systems and data, with defined recovery time objectives (RTOs) and recovery point objectives (RPOs)?
- **Incident Response Plan (IRP):**
  - [ ] Is a formal Incident Response Plan (IRP) in place, documented, and regularly tested through simulations?
  - [ ] Are roles and responsibilities for incident response clearly defined and communicated?
  - [ ] Is there a process for reporting and escalating security incidents, including potential data breaches?
- **Vendor & Third-Party Risk Management:**
  - [ ] Is a formal program in place to assess and manage the cybersecurity risks posed by third-party vendors (e.g., CROs, CMOs, cloud providers)?
  - [ ] Are security clauses included in all vendor contracts, specifying data protection, audit rights, and incident notification requirements?
  - [ ] Are third-party security postures regularly reviewed and monitored?

Section 2: GxP Compliance (Good Practice Regulations)

Focus on IT systems supporting GxP-regulated activities (e.g., GCLP, GCP, GLP, GMP, GVP).

- **System Validation:**
  - [ ] Are all computer systems used in GxP-regulated activities formally validated according to established protocols?
  - [ ] Is there documented evidence of validation, including user requirements, functional specifications, testing, and traceability matrices?
  - [ ] Are revalidation procedures in place for system changes or upgrades?
- **Data Integrity:**
  - [ ] Are systems designed to ensure data integrity principles (ALCOA+C: Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available)?
  - [ ] Are audit trails enabled and regularly reviewed for all GxP-critical systems, capturing all data changes and user actions?
  - [ ] Are data backup and recovery procedures specifically designed to maintain the integrity and availability of GxP data?
- **Electronic Records & Signatures:**

    - [ ] Do electronic records meet regulatory requirements for authenticity, integrity, and confidentiality?
    - [ ] Are electronic signatures legally binding and equivalent to handwritten signatures, with appropriate controls in place?
- **Change Control:**
    - [ ] Is a formal change control process implemented for all GxP-relevant IT systems, including hardware, software, and configurations?
    - [ ] Are all changes documented, reviewed, approved, and tested before implementation?

Section 3: 21 CFR Part 11 Compliance (FDA Regulations for Electronic Records)

Specific requirements for electronic records and electronic signatures for FDA-regulated industries.

- **System Controls:**
    - [ ] Do systems ensure the authenticity, integrity, and confidentiality of electronic records?
    - [ ] Are audit trails secure, computer-generated, time-stamped, and unalterable, capturing all actions related to electronic records?
    - [ ] Are there controls to prevent unauthorized access to systems and records?
- **Electronic Signatures:**
    - [ ] Are electronic signatures unique to individuals and securely linked to the electronic record?
    - [ ] Is there a process for verifying the identity of individuals using electronic signatures?
    - [ ] Are electronic signatures protected from unauthorized use and alteration?
- **Documentation & Procedures:**
    - [ ] Are standard operating procedures (SOPs) in place for all aspects of electronic record management and electronic signatures?
    - [ ] Is there documentation of system validation, security policies, and audit trail reviews?

Section 4: GDPR Compliance (General Data Protection Regulation)

Focus on the protection of personal data of EU citizens and residents.

- **Data Mapping & Inventory:**

  - [ ] Have all personal data (including employee, patient, and research participant data) collected, processed, and stored been identified and mapped?
  - [ ] Is the legal basis for processing each category of personal data clearly documented?
- **Data Protection by Design & Default:**
  - [ ] Are new systems and processes designed with data protection principles in mind from the outset?
  - [ ] Are default settings for privacy the most protective?
- **Data Subject Rights:**
  - [ ] Are processes in place to handle data subject requests (e.g., right to access, rectification, erasure, data portability)?
  - [ ] Is there a clear privacy notice informing individuals about how their data is processed?
- **Data Breach Notification:**
  - [ ] Is there a clear procedure for detecting, reporting, and investigating personal data breaches within 72 hours to supervisory authorities and affected individuals (where required)?
- **International Data Transfers:**
  - [ ] Are mechanisms in place (e.g., Standard Contractual Clauses, Binding Corporate Rules) for lawful transfer of personal data outside the EU/EEA?
- **Data Protection Officer (DPO):**
  - [ ] If required, has a Data Protection Officer been appointed and their contact details published?

Section 5: SOC 2 Compliance (Service Organization Control 2)

Focus on controls related to security, availability, processing integrity, confidentiality, and privacy of data.

- **Trust Services Criteria (TSC) Alignment:**
  - [ ] Have the relevant Trust Services Criteria (Security is mandatory; others as applicable) been identified and mapped to your IT controls?
  - [ ] Is there documented evidence that controls are designed and operating effectively to meet these criteria?
- **Control Environment:**
  - [ ] Are there documented policies and procedures for information security, access control, change management, and risk management?
  - [ ] Is there a clear organizational structure with defined roles and responsibilities for security?
- **Monitoring & Logging:**
  - [ ] Are security events continuously monitored, logged, and reviewed?

    - [ ] Are alerts configured for suspicious activities, and is there a process for timely response?
- **Risk Management:**
    - [ ] Is a formal risk assessment process in place to identify, analyze, and mitigate information security risks?
    - [ ] Are risk mitigation strategies regularly reviewed and updated?
- **Communication & Training:**
    - [ ] Is security awareness training provided to all employees, contractors, and relevant third parties?
    - [ ] Are security policies and procedures regularly communicated and acknowledged?

Section 6: Proactive Security Readiness & Continuous Improvement

Beyond compliance, focus on strategic readiness and continuous enhancement.

- **Cybersecurity Posture Assessment:**
    - [ ] Have you conducted a recent comprehensive cybersecurity risk assessment to identify current vulnerabilities and threats?
    - [ ] Is there a clear understanding of your organization's cyber maturity relative to industry benchmarks?
- **Strategic Planning:**
    - [ ] Is cybersecurity integrated into your overall business strategy, particularly for new product development, clinical trials, and market expansion?
    - [ ] Are resources allocated to address identified security gaps and support future growth initiatives?
- **Investor & Partner Assurance:**
    - [ ] Are you prepared to provide investor-friendly cyber risk summaries that articulate your security posture and risk mitigation strategies?
    - [ ] Can you confidently attest to your security controls for new clients or strategic partners requiring security attestations?
- **Continuous Monitoring & Adaptation:**
    - [ ] Is there a process for continuously monitoring the evolving threat landscape and regulatory changes?
    - [ ] Are your security controls and compliance programs regularly adapted to address new risks and requirements?

This checklist serves as a living document. Regular review and updates are crucial to maintain compliance and a strong security posture in the dynamic life sciences landscape.

Ready to Strengthen Your Security Posture?

Take the centrexIT 2-Minute Cybersecurity Assessment to identify your organization's risk exposure:

https://centrexit.com/cyber-security-readiness-assessment/

Or schedule a free 30-minute consultation: https://pages.centrexit.com/free-30-minute-cyber-security-assessment

References

- centrexIT Segment Personas_1.0.pdf
- https://aws.amazon.com/compliance/gxp-part-11-annex-11/
- https://www.cognidox.com/the-guide-to-gxp-compliance
- https://regardd.org/21-cfr-part-11
- https://learn.microsoft.com/en-us/compliance/regulatory/offering-fda-cfr-title-21-part-11
- 5
- https://gdpr-text.com/
- https://www.paloaltonetworks.com/cyberpedia/soc-2
- https://auditboard.com/blog/soc-2-framework-guide-the-complete-introduction