centrexIT™

Your Cyber Readiness Revealed: Life Science Innovation Safeguard Checklist

A centrexIT Checklist for Life Sciences Executives (CEO, CFO, COO, CSO)

Version 1.1

Published July 2025

Introduction

As a Life Sciences Executive, your firm's future hinges on protecting groundbreaking innovation, ensuring stringent regulatory compliance, and maintaining unwavering investor confidence. This checklist provides a strategic overview of key cybersecurity areas to safeguard your intellectual property (IP), streamline regulatory milestones, and secure vital funding.

This comprehensive assessment helps you:

- Protect invaluable innovation and intellectual property (IP)
- Ensure seamless regulatory compliance and audit readiness
- Maintain and enhance investor confidence
- Build resilience across your research and operations

HOW TO USE THIS CHECKLIST

Step 1: For each statement, check **ONE** box that best describes your current situation.

Step 2: Assign points based on your selection:

- **Needs Attention = 0 Points**
- **Partially Implemented = 1 Point**
- **Yes = 2 Points**

Step 3: Add up the points for each section and then calculate your total score at the end.

Step 4: Review your "Cyber Readiness Score" and "Priority Areas" to understand your next steps.

SCORING GUIDE

- **[ ] Yes (2 Points):** This is fully or mostly implemented and consistently maintained.
- **[ ] Partially Implemented (1 Point):** This is in progress, has partial coverage, or needs more work.
- **[ ] Needs Attention (0 Points):** This is not implemented, partially implemented, or requires significant improvement.

SECTION 1: INTELLECTUAL PROPERTY (IP) & RESEARCH DATA PROTECTION

Foundation: Safeguarding Core Innovation Assets

1.1 Data Encryption for IP & Research Data Are your proprietary research data and IP (e.g., drug formulations, genetic sequences, clinical trial results) encrypted both in transit and at rest?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

1.2 Access Controls for R&D Systems & Data Do you have strict, granular, role-based access controls for all R&D systems and sensitive data repositories, with Multi-Factor Authentication (MFA) for privileged access?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

1.3 Data Loss Prevention (DLP) Strategy Is a Data Loss Prevention (DLP) strategy implemented to monitor and prevent unauthorized exfiltration of sensitive IP and research data from your network and cloud environments?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

SECTION 1 TOTAL: _____ / 6 Points

SECTION 2: REGULATORY COMPLIANCE & AUDIT READINESS

Critical: Navigating the Complex Regulatory Landscape

2.1 Compliance with Industry Regulations Are your IT systems and data management practices compliant with relevant life sciences regulations (e.g., GxP, 21 CFR Part 11, HIPAA, GDPR)?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

2.2 Regular Compliance Audits & Validation Do you conduct regular internal audits or engage external auditors to validate compliance and security controls before key regulatory submissions or inspections?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

2.3 Data Integrity & Audit Trail Maintenance Is there a clear process for maintaining comprehensive audit trails and ensuring the integrity and authenticity of all data used for regulatory purposes?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

SECTION 2 TOTAL: _____ / 6 Points

SECTION 3: INVESTOR CONFIDENCE & DUE DILIGENCE

Advanced: Demonstrating Security as a Strategic Asset

3.1 Cybersecurity Posture Communication Can you clearly articulate your firm's cybersecurity posture, risk management strategy, and incident response capabilities to potential investors and board members?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

3.2 Due Diligence Readiness Are you prepared to provide comprehensive security documentation (e.g., assessment reports, policies, certifications) and demonstrate your security program during due diligence for funding rounds or M&A?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

3.3 Cybersecurity as a Strategic Asset Do you actively communicate cybersecurity as a strategic asset that protects valuation, ensures future revenue streams, and enhances competitive advantage?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)

- [ ] Needs Attention (0 Points)

Notes:
_____
_____
_____

SECTION 3 TOTAL: _____ / 6 Points

SECTION 4: OPERATIONAL TECHNOLOGY (OT) & LAB SYSTEMS SECURITY

Governance: Protecting Specialized Research and Manufacturing Environments

4.1 OT Network Segmentation Are your specialized lab equipment and manufacturing control systems (OT/ICS) segmented and isolated from the general corporate IT network?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:
_____
_____
_____

4.2 Vulnerability Management for OT Systems Do you have a controlled process for identifying and applying security patches or mitigating vulnerabilities in OT systems and scientific instruments?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:
_____

_____
_____

4.3 Security Measures for Research/Manufacturing Processes Are specific security measures in place to prevent tampering, unauthorized access, or disruption of critical research and manufacturing processes via OT systems?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

SECTION 4 TOTAL: _____ / 6 Points

SECTION 5: SUPPLY CHAIN & THIRD-PARTY RISK MANAGEMENT

Leadership: Extending Resilience Beyond Your Organization

5.1 Third-Party Vendor Cybersecurity Vetting Do you have a rigorous process for vetting the cybersecurity posture of all third-party vendors (CROs, CMOs, cloud providers, software vendors) that interact with your data or systems?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

5.2 Business Associate Agreements (BAAs) / Vendor Contracts Are Business Associate Agreements (BAAs) or equivalent contracts in place with all vendors handling sensitive data, clearly defining security responsibilities and breach notification requirements?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

5.3 Ongoing Third-Party Risk Monitoring Is there ongoing monitoring of critical third-party security postures and data exchange mechanisms to identify and address emerging risks?

- [ ] Yes (2 Points)
- [ ] Partially Implemented (1 Point)
- [ ] Needs Attention (0 Points)

Notes:

_____
_____
_____

SECTION 5 TOTAL: _____ / 6 Points

YOUR INNOVATION SAFEGUARD SCORE

TOTAL SCORE CALCULATION

Section	Your Score	Max Score
IP & Research Data Protection	____	6
Regulatory Compliance & Audit Readiness	____	6
Investor Confidence & Due Diligence	____	6
OT & Lab Systems Security	____	6
Supply Chain & Third-Party Risk Management	____	6

YOUR TOTAL SCORE ____ **30**

LIFE SCIENCES CYBERSECURITY READINESS ASSESSMENT

Check your readiness level based on your total score:

- **24-30 Points - INNOVATION DEFENDER!** - Your firm demonstrates excellent cybersecurity for innovation, compliance, and investor confidence.
  - *Action: Continue to lead with robust security practices and leverage them as a strategic advantage.*
- **15-23 Points - INNOVATION AWARE!** - You have a good foundation, but there are clear opportunities to strengthen cybersecurity across key areas.
  - *Action: Focus on addressing identified gaps to enhance IP protection, regulatory readiness, and investor appeal.*
- **6-14 Points - INNOVATION AT RISK!** - Significant cybersecurity gaps exist that need urgent attention to protect IP, ensure compliance, and secure funding.
  - *Action: Prioritize addressing critical vulnerabilities immediately to safeguard your firm's core assets.*
- **Under 6 Points - INNOVATION EXPOSED!** - Your firm is highly exposed to cyber threats that could jeopardize IP, regulatory approvals, and investment.
  - *Action: Immediate, comprehensive action is required to build foundational cybersecurity for your innovation.*

YOUR PRIORITY AREAS FOR IMPROVEMENT

(Review sections where you scored lower) Focus your immediate attention on sections with more "Needs Attention" marks.

NEXT STEPS: SECURE YOUR LIFE SCIENCES BREAKTHROUGHS

READY FOR A DEEPER DIVE?

Your self-assessment is a great start. To truly understand your unique risks and build an ironclad defense for your business, a professional assessment is key.

SCHEDULE YOUR FOLLOW-UP CYBERSECURITY ASSESSMENT

Meet with our expert team for a personalized follow-up assessment. We'll help you translate your checklist results into a strategic, actionable plan tailored to your business.

Ready to Strengthen Your Security Posture?https://pages.centrexit.com/cybersecurity-risk-assesment-request

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 with our team:

https://pages.centrexit.com/free-30-minute-cyber-security-assessment