complus

FCA Regulated Firms

IT & Cyber Governance Checklist

A practical checklist for FCA regulated financial services firms

MANAGE. PROTECT. ASSURE.

www.complus-it.com

info@complus-it.com

Purpose of This Checklist

IT and Cyber Readiness for Financial Services Firms

Financial environments combine sensitive data with high expectations of control and accountability. Even small weaknesses can create disproportionate risk.

Why this checklist matters

- Remote and hybrid working is now common
- Client data is accessed across multiple systems
- Cloud platforms and third-party tools are widely used
- Oversight, traceability, and consistency are essential

Where Risk Commonly Appears

Most incidents arise from operational gaps rather than complex technical failures.

- Weak identity and access controls
- Phishing and credential compromise
- Inconsistent device security
- Backups assumed to work but not tested
- Limited visibility across systems and suppliers

MANAGE

IT That Supports Controlled Financial Operations

Use this checklist to review whether your IT environment is structured, documented, and capable of supporting controlled financial operations.

IT Systems & Access

- Core systems handling client and financial data are identified and supported
- Secure access is in place for office and remote working
- User access reflects role and responsibility

Environment & Oversight

- Cloud platforms and third-party tools are documented
- Devices accessing systems meet defined security standards
- System changes and updates are applied consistently

Support & Accountability

- IT ownership and accountability are clearly defined
- Support response times are established

! Why this matters

Weak operational visibility makes it difficult to demonstrate control and respond effectively to incidents.

PROTECT

Data, Identity, and Threat Exposure

Use this checklist to assess whether client data and user identities are adequately protected from misuse and compromise.

Identity & Access

- Multi-factor authentication is enforced on key systems
- Administrative access is restricted and monitored
- Password practices reduce credential risk

Data & System Security

- Sensitive data is access-controlled and segregated
- Endpoint protection covers all devices
- Email threats such as phishing are actively filtered

Monitoring & Response

- Security alerts are monitored and reviewed
- Suspicious activity triggers investigation

❗ Why this matters

Weak identity and email controls remain a primary cause of financial data incidents.

ASSURE

Continuity, Recovery, and Operational Resilience

Use this checklist to review whether your organisation can maintain operations and recover effectively during disruption.

Backup & Recovery

- Critical systems and data are backed up securely
- Backup restoration is tested periodically
- Recovery processes are documented

Resilience & Preparedness

- Key systems have defined recovery priorities
- Incident response responsibilities are clearly assigned
- Logs and records support investigation and review

! Why this matters

Untested recovery and unclear response processes increase the impact and duration of disruption.

Your Resilience Snapshot

What This Checklist Reveals

This checklist provides a practical view of how well your IT and cyber environment supports secure, controlled financial operations.

It helps you identify whether:

- IT systems support day-to-day financial operations without disruption
- Client and financial data is adequately protected
- User access and identities present avoidable risk
- Devices and systems are consistently managed
- Backup and recovery processes are dependable
- Your organisation can respond effectively to IT or cyber incidents

A deeper review may be appropriate if:

- Working patterns have changed
- Systems, platforms, or suppliers have evolved
- Access to client data is widely distributed
- Backup and recovery have not been tested recently

Next Step

If you would like a second opinion

This checklist is intended as a starting point. If you would like an independent view of your IT and cyber resilience, Complus IT can provide structured guidance aligned with financial services operations.

How to get in touch

Email
info@complus-it.com

Address
32 Threadneedle St. London, EC2R8AY

IASME CYBER ASSURANCE LEVEL ONE

CYBER ESSENTIALS CERTIFIED PLUS

UK CYBER SECURITY COUNCIL

bsi

THE EASTERN CYBER RESILIENCE CENTRE

Chartered Institute of Information Security MEMBER 2025