# Financial Institution Cyber Threat Assessment Checklist

## 1. Governance & Management

| Checklist Item | Compliant | Notes |
|---|---|---|
| Information Security Policy established and regularly reviewed | □ | |
| Regular risk assessments conducted | □ | |
| Incident response plan in place | □ | |

## 2. Access Control & Authentication

| Checklist Item | Compliant | Notes |
|---|---|---|
| Multi-factor authentication enabled for all systems | □ | |
| Access rights reviewed and updated regularly | □ | |
| Password policy enforced | □ | |

## 3. Network Security

| Checklist Item | Compliant | Notes |
|---|---|---|
| Firewalls configured and monitored | □ | |
| Intrusion detection and prevention systems in place | □ | |
| Network segmentation implemented | □ | |

## 4. Malware & Endpoint Protection

| Checklist Item | Compliant | Notes |
|---|---|---|
| Anti-virus and anti-malware tools deployed and updated | □ | |
| Endpoints regularly patched and updated | □ | |
| Removable media usage controlled | □ | |

## 5. Data Protection & Privacy

| Checklist Item | Compliant | Notes |
|---|---|---|

| | | |
|---|---|---|
| Data encryption (at rest and in transit) enabled | □ | |
| Data retention and destruction procedures in place | □ | |
| Data loss prevention systems implemented | □ | |

## 6. Security Awareness & Training

| Checklist Item | Compliant | Notes |
|---|---|---|
| Staff receive regular cybersecurity training | □ | |
| Regular phishing simulations conducted | □ | |
| Clear reporting process for suspicious activity | □ | |

## 7. Third-Party & Vendor Management

| Checklist Item | Compliant | Notes |
|---|---|---|
| Third-party security assessments conducted | □ | |
| Service-level agreements cover cybersecurity expectations | □ | |
| Vendors monitored for ongoing compliance | □ | |

## 8. Monitoring & Response

| Checklist Item | Compliant | Notes |
|---|---|---|
| Continuous monitoring for suspicious activities | □ | |
| Established incident response process | □ | |
| Regular review and updates of monitoring procedures | □ | |

## 9. Backup & Recovery

| Checklist Item | Compliant | Notes |
|---|---|---|
| Regular backups performed and tested | □ | |
| Backup data is encrypted and securely stored | □ | |
| Disaster recovery plan established | □ | |