Certificate in Cyber Risk for Financial Services

Module 1: Foundations of Cybersecurity and Cyber Risk

- Meaning and scope of cybersecurity, information security and cyber risk.
- Confidentiality, integrity and availability.
- Threats, vulnerabilities, exposures and controls.
- Distinguishing cyber incidents, data breaches, fraud and operational failures.
- Inherent risk, residual risk and control effectiveness.
- Cyber risk within enterprise and operational risk management.
- Financial, operational, legal and reputational consequences.
- Cyber-risk terminology for non-technical professionals.
- Roles of business teams, technology teams and security specialists.
- Limits of individual competence and specialist escalation.

Module 2: The Financial-Services Cyber Threat Landscape

- Why financial institutions and their customers are targeted.
- Threat actors, motivations and attack methods.
- Phishing, social engineering and credential theft.
- Malware, ransomware and data extortion.
- Account takeover and unauthorised access.
- Denial-of-service attacks and service disruption.
- Insider threats and misuse of authorised access.
- Third-party compromise and supply-chain attacks.
- Cyber threats to banks, lenders, insurers and payment businesses.
- Threats to investment firms, wealth managers and family offices.
- Business consequences of compromised transactions and records.
- Learning from anonymised financial-sector incidents.

Module 3: Cyber-Risk Governance and Accountability

- Board and senior-management oversight.
- Cybersecurity strategy and alignment with business objectives.
- Roles of the CIO, CISO, risk, compliance and internal audit.
- Business ownership of cyber risks.
- Cyber-risk policies and standards.
- Risk appetite, tolerance and exception management.
- Delegation, decision rights and escalation.
- Security committees and management reporting.
- Resource allocation and prioritisation.
- Independent challenge and assurance.
- Accountability in outsourced and smaller operating models.
- Building a security-conscious organisational culture.

Module 4: Technology Foundations for Finance Professionals

- Core components of financial-services technology environments.
- Applications, databases, networks and endpoints.
- On-premises, cloud and hybrid environments.
- Core banking, payment and investment platforms.
- Application programming interfaces and system integrations.
- Digital identities and authentication.
- Encryption, key management and digital certificates: introductory concepts.
- Logs, audit trails and monitoring tools.
- Development, testing and production environments.
- Legacy systems and unsupported software.
- Technology dependencies and single points of failure.
- Interpreting technical findings in business terms.

Module 5: Cyber-Risk Identification and Assessment

- Defining assessment scope and business context.
- Asset inventories and ownership.
- Critical information, systems and business services.
- Data-flow and dependency mapping.
- Threat and vulnerability identification.
- Scenario-based cyber-risk assessment.
- Assessing likelihood and impact.

- Evaluating control design and operating effectiveness.
- Risk registers and risk-control matrices.
- Treatment options: mitigation, avoidance, transfer and acceptance.
- Documenting assumptions, limitations and residual risks.
- Risk acceptance, review and escalation.

Module 6: Identity and Access Management

- Identity lifecycle and access governance.
- Joiner, mover and leaver processes.
- Least privilege and need-to-know access.
- Role-based access and segregation of duties.
- Passwords, multifactor authentication and authentication limitations.
- Privileged accounts and administrative access.
- Service accounts and non-human identities.
- Remote access and third-party access.
- Periodic access reviews.
- Dormant accounts and excessive permissions.
- Emergency access and approval records.
- Detecting and escalating access-control exceptions.

Module 7: Data Protection and Information Handling

- Classification of customer, employee and business information.
- Data ownership and accountability.
- Collection, use, sharing, retention and disposal.
- Confidentiality and appropriate access.
- Encryption in transit and at rest.
- Secure file transfer and collaboration.
- Data-loss prevention: purpose and limitations.
- Handling sensitive information in email and messaging applications.
- Data masking and use of test data.
- Backup confidentiality and access controls.
- Data leakage through vendors and personal devices.
- Secure handling of investment, transaction and family information.

Module 8: Secure Technology Operations

- Secure configuration and system hardening: business-level understanding.
- Patch and vulnerability management.
- Prioritising vulnerabilities by business exposure and impact.
- Endpoint, server and network protection.
- Network segmentation and restricted connectivity.
- Change management and approval controls.
- Emergency changes and retrospective review.
- Logging, monitoring and alert escalation.
- Malware protection and endpoint detection.
- Secure remote working.
- Physical and environmental security.
- Operational exceptions and compensating controls.

Module 9: Application, API and Digital-Channel Risk

- Security across the application lifecycle.
- Business requirements and security-by-design.
- Secure development and testing: introductory concepts.
- Authentication, authorisation and transaction integrity.
- API access and third-party integrations.
- Mobile applications and customer-facing platforms.
- Vulnerability assessment and penetration-testing reports.
- Remediation ownership and retesting.
- Release approvals and production changes.
- Software components and supply-chain dependencies.
- Customer-session and account-security controls.
- Recognising when technical specialist review is required.

Module 10: Cloud, Outsourcing and Third-Party Risk

- Cloud service models and shared responsibilities.
- Outsourcing versus transfer of accountability.
- Vendor selection and cyber due diligence.
- Criticality assessment and dependency concentration.
- Access to customer data and production systems.
- Subcontractors and fourth-party dependencies.
- Contractual security obligations.

- Incident notification and cooperation provisions.
- Audit rights and assurance reports.
- Data location, portability and exit considerations.
- Service continuity and recovery dependencies.
- Ongoing monitoring and remediation tracking.

Module 11: Payments, Banking and Lending Cyber Risk

- Cyber risks across payment initiation, authorisation and settlement.
- Beneficiary changes and payment-instruction integrity.
- Digital banking and mobile-channel exposures.
- Customer authentication and account protection.
- Payment gateways and processing dependencies.
- Reconciliation and exception monitoring.
- Cyber risks in digital lending and servicing.
- Compromised credentials, devices and interfaces.
- Treasury and high-value transaction controls.
- Coordination between cyber, fraud and operations teams.
- Customer communication during service disruption.
- Escalation of suspected unauthorised transactions.

Module 12: Cyber Risk in Investments, Wealth and Family Offices

- Risks across trading, investment administration and reporting.
- Client portals and digital onboarding.
- Custodian, broker, administrator and registrar dependencies.
- Confidential investment and transaction information.
- Unauthorised dealing instructions and account changes.
- Business-email compromise and executive impersonation.
- Private-market deal rooms and document sharing.
- Family-member, trustee and authorised-signatory access.
- Personal devices and informal communication channels.
- Concentrated access in small teams.
- Continuity of investment operations and client servicing.
- Protecting privacy without weakening accountability.

Module 13: Cyber-Enabled Fraud and Human Risk

- Relationship between cybersecurity and fraud prevention.
- Phishing, smishing, vishing and malicious links.
- Executive, employee, vendor and customer impersonation.
- Invoice diversion and payment-redirection schemes.
- Remote-access scams and credential harvesting.
- Deepfake voice and video.
- Manipulation of urgency, authority and confidentiality.
- Independent verification and callback controls.
- Staff awareness and simulated exercises.
- Reporting mistakes and suspected compromise promptly.
- Avoiding blame-driven underreporting.
- Coordinating fraud response with technical containment.

Module 14: Security Monitoring and Threat Intelligence

- Purpose of security monitoring.
- Security operations centres and managed services.
- Event, alert and incident distinctions.
- Log coverage, retention and access.
- Alert prioritisation and escalation.
- Detection coverage for critical business services.
- Threat intelligence and its business relevance.
- Indicators of compromise: introductory understanding.
- False positives and missed detections.
- Threat hunting: purpose and specialist boundaries.
- Monitoring effectiveness and service-provider performance.
- Translating technical alerts into business decisions.

Module 15: Cyber Incident Response and Crisis Management

- Incident-response policies, plans and responsibilities.
- Severity assessment and escalation triggers.
- Mobilising technical, business, legal and communications teams.
- Containment, eradication and recovery: conceptual understanding.
- Preserving evidence and maintaining decision records.
- Avoiding unauthorised changes that compromise investigation.
- Customer, employee and stakeholder communications.

- Coordination with vendors, insurers and external specialists.
- Applicable regulatory and contractual notifications.
- Ransomware and extortion decision-making.
- Tabletop exercises and crisis simulations.
- Post-incident review and corrective actions.

Module 16: Business Continuity and Operational Resilience

- Cybersecurity, business continuity and disaster recovery.
- Identifying critical business services.
- Business impact analysis.
- Recovery time objectives and recovery point objectives.
- Tolerable disruption and dependency assessment.
- Backup design, segregation and restoration.
- Recovery testing and evidence of successful restoration.
- Manual workarounds and their control risks.
- Alternative communication arrangements.
- Third-party continuity and exit plans.
- Reconciliation and integrity checks before resuming services.
- Lessons from exercises and actual disruptions.

Module 17: Legal, Regulatory and Compliance Considerations

- Indian cybersecurity and financial-sector regulatory architecture.
- Roles of RBI, SEBI, IRDAI, PFRDA, IFSCA and CERT-In.
- Applicable information-technology and data-protection requirements.
- Entity-specific scope, proportionality and exemptions.
- Governance, audit and reporting obligations.
- Incident-reporting requirements and escalation ownership.
- Regulatory deadlines versus contractual notification periods.
- Record retention and evidence preservation.
- Privacy, confidentiality and lawful information sharing.
- Cross-border operations and jurisdictional considerations.
- Regulatory inspections, observations and remediation.
- Monitoring amendments, commencement dates and clarifications.

Module 18: Cybersecurity Frameworks, Assurance and Audit

- Purpose of cybersecurity frameworks and control standards.
- Introductory overview of NIST CSF, ISO/IEC 27001 and CIS Controls.
- Mapping business risks to control objectives.
- Framework alignment versus independent certification.
- Internal assessments, external audits and technical testing.
- Scope, exclusions and limitations of assurance reports.
- Reviewing findings by severity and business impact.
- Management responses and corrective-action plans.
- Evidence of remediation and closure.
- Independent validation and retesting.
- Avoiding checklist-only compliance.
- Communicating assurance limitations to management.

Module 19: Cyber-Risk Measurement and Reporting

- Key risk indicators and key performance indicators.
- Measures of exposure, control coverage and remediation.
- Access-review exceptions and privileged-account trends.
- Vulnerability ageing and overdue remediation.
- Detection, response and recovery measures.
- Phishing-reporting and awareness indicators.
- Third-party risk and concentration dashboards.
- Scenario analysis and loss estimation.
- Uncertainty and limitations in cyber-risk quantification.
- Reporting residual risk and accepted exceptions.
- Board-level reporting and decision-oriented communication.
- Avoiding misleading metrics and false precision.

Module 20: Cyber Insurance and Financial Impact

- Purpose and limitations of cyber insurance.
- First-party and third-party exposures.
- Policy wording, exclusions and coverage conditions.
- Incident-response services and insurer coordination.
- Notification, consent and documentation requirements.
- Business interruption and recovery costs.
- Liability, legal expenses and customer remediation.

- Fraud and cyber coverage interfaces.
- Aggregation and concentration risks.
- Insurance due diligence and specialist advice.
- Risk transfer versus control investment.
- Financial planning for uninsured losses.

Module 21: AI and Emerging Technology Risk

- AI use cases in financial-services operations.
- Data leakage through public AI tools.
- AI-generated phishing, impersonation and document fabrication.
- Risks of inaccurate or unsupported AI outputs.
- Access privileges and actions taken by AI-enabled systems.
- Human oversight and approval boundaries.
- Vendor due diligence for AI services.
- Security of connected systems and automated workflows.
- Digital assets, private-key custody and tokenisation risks.
- Emerging technologies and changing attack surfaces.
- Assessing innovation without assuming security or regulatory permission.
- Maintaining accountability as technology changes.

Module 22: Ethics, Professional Conduct and Security Culture

- Responsible handling of confidential information.
- Authorised access and acceptable use.
- Boundaries of security testing.
- Responsible reporting of vulnerabilities.
- Conflicts of interest in vendor selection and assurance.
- Transparency about incidents and control weaknesses.
- Pressure to conceal findings or bypass controls.
- Employee fairness and privacy.
- Accurate reporting without exaggeration or false reassurance.
- Professional scepticism towards vendor and technology claims.
- Recognising limits of competence.
- Escalating concerns and maintaining defensible records.