Level	Description	Priority	Validation References	Classification	Type	Metric
1	**IDENTIFY RISKS IN CLOUD**				Group	*Met1*
1.1	**Asset Management (1.1):** The resources, personnel, infrastructure, equipment, and services that support the Fintech's business processes are identified and managed in alignment with their significance to business goals and the organization's risk strategy.				Metric	*M et1.1*
1.1.1	ID.AM-1: Are all physical IT equipment (computers, laptops, BYOD) within the Fintech inventoried?	HIGH	COBIT 5 BAI09.01, BAI09.02 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8	Fintech Administratiors need to comply.	Sub-Metric	*M et1.1.1*
1.1.2	ID.AM-2: Is there a complete inventory of all system and application software within the Fintech?	HIGH	COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8	Fintech Administratiors need to comply.	Sub-Metric	*M et1.1.2*
1.1.3	ID.AM-3: Do cloud providers enable the Fintech to specify where their content is stored, ensure its security during transit and at rest, and manage it effectively?	LOW	COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	Cloud providers need to provide the information.	Sub-Metric	*M et1.1.3*
1.1.4	ID.AM-4: Does the Fintech ensure that external information system service providers comply with the Fintech's information security requirements, including applicable laws, policies, regulations, standards, and guidelines?	HIGH	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9	Fintech Administratiors need to comply.	Sub-Metric	*M et1.1.4*
1.1.5	ID.AM-5: Does the cloud provider define the resilience measures in place to support the delivery of critical services across all operating states (e.g., during normal operations, under duress or attack, and during recovery)?	Medium	ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 COBIT 5 APO03.03,APO03.04, BAI09.02	Cloud providers need to provide the information.	Sub-Metric	*M et1.1.5*

Level	Description	Priority	Validation References	Classification	Type	Metric
1	**IDENTIFY RISKS IN CLOUD**				Group	*Met1*
1.2	**Governance (1.2):** The frameworks, policies, and processes for managing and overseeing the Fintech's regulatory, legal, risk, environmental, and operational obligations are clearly defined and provide the organization's leadership with insights into cybersecurity risks.				Metric	*M et1.2*
1.2.1	ID.GV-1: Has the cloud provider developed and communicated a comprehensive security policy regarding the protection of data stored on the cloud?	Medium	COBIT 5 APO01.03, EDM01.01, EDM01.02· ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls	Cloud providers need to provide the information.	Sub-Metric	*M et1.2.1*
1.2.2	ID.GV-2: Are employees, including those from third-party providers, regularly trained on their roles and responsibilities related to information security?	Medium	COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PM-1, PS-7	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et1.2.2*
1.2.3	ID.GV-3: Are the legal and regulatory requirements related to cloud security understood and managed by the Fintech, with clear explanations provided by the cloud provider?	HIGH	COBIT 5 MEA03.01, MEA03.04 ISO/IEC 27001:2013 A.18.1 ISA 62443-2-1:2009 4.4.3.7	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et1.2.3*
1.2.4	ID.GV-4: Does the cloud provider keep the Fintech informed of any changes related to risk management processes?	LOW	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 NIST SP 800-53 Rev. 4 PM-9, PM-11	Cloud providers need to provide the information.	Sub-Metric	*M et1.2.4*

Level	Description	Priority	Validation References	Classification	Type	Metric
1	**IDENTIFY RISKS IN CLOUD**				Group	*Met1*
1.3	**Risk Assessment (1.3):** The Fintech understands the cybersecurity risks to its operations, including the impact on its assets, reputation, image, and staff.				Metric	*M et1.3*
1.3.1	ID.RA-1: Does the Fintech regularly update and patch its operating systems and conduct vulnerability scans on its systems?	Medium	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA- 5, SA-11, SI-2, SI-4, SI-5	Fintech Administratiors need to comply.	Sub-Metric	*M et1.3.1*

1.3.2	ID.RA-2: Does the Fintech implement a continuous risk assessment process to identify, evaluate, and mitigate risks across the organization?	LOW	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	Fintech Administratiors need to comply.	Sub-Metric	*M et1.3.2*
1.3.3	ID.RA-3: Does the Fintech assess and identify potential business impacts and the likelihood of risks associated with the cloud?	LOW	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et1.3.3*
1.3.4	ID.RA-4: Does the Fintech have a thorough understanding of the threats, vulnerabilities, likelihoods, and impacts associated with cloud computing?	LOW	COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et1.3.4*
1.3.5	ID.RA-5: Has the Fintech identified and prioritized its responses to cloud-related risks?	LOW	COBIT 5 APO12.05, APO13.02 NIST SP 800-53 Rev. 4 PM-4, PM-9	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et1.3.5*

Level	Description	Priority	Validation References	Classification	Type	Metric
2	**PROTECT DATA IN THE CLOUD**				Group	*Met2*
2.1	**Access Control (2.1):** Access to IT infrastructure, equipment, facilities, and systems is restricted to authorized personnel and devices, and is limited to performing only authorized actions and transactions.				Metric	*M et2.1*
2.1.1	PR.AC-1: Does the Fintech issue, manage, verify, revoke, and audit user credentials for the cloud, ensuring they are only granted to authorized devices, users, and processes?	HIGH	COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 NIST SP 800-53 Rev. 4 AC-2, IA Family	Fintech to impliment strong authentication technologies.	Sub-Metric	*M et2.1.1*
2.1.2	PR.AC-2: Are physical assets protected, and is access to these assets within the Fintech's premises properly managed?	Medium	COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2,A. 11.1.4, A.11.1.6, A.11.2.3	Fintechs to impliment srong physical controls.	Sub-Metric	*M et2.1.2*
2.1.3	PR.AC-3: Is the Fintech establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidelines for each type of remote access allowed to its systems, in line with its access control policy?	HIGH	COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISO/IEC 27001:2013 A.6.2.2, A.13.1.1,A. 13.2.1	Administrators to give final access for logging in al activities.	Sub-Metric	*M et2.1.3*
2.1.4	ID.AC-4: Does the Fintech ensure that external information system service providers comply with the Fintech's information security requirements, including applicable laws, policies, regulations, standards, and guidelines?	HIGH	CCS CSC 12, 15 ISA 62443-2-1:2009 4.3.3.7.3 1SA I62443-3-3:2013 SR 2.1 NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16	Admins to avoid giving access to unauhorised users.	Sub-Metric	*M et2.1.4*
2.1.5	PR.AC-5: Is the Fintech's LAN and WAN adequately protected, including network segregation where applicable?	Medium	ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3,A. 13.2.1	Fintechs to ensure network is secure.	Sub-Metric	*M et2.1.5*
2.1.6	PR.AC-6: Does the cloud provider implement appropriate authentication technologies, such as single-factor or multi-factor authentication, to ensure that Fintech users, devices, and other assets are properly authenticated?	Medium	COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2,4.3.3.7.2, 4.3.3.7.4	Cloud providers need to provide the information.	Sub-Metric	*M et2.1.6*

Level	Description	Priority	Validation References	Classification	Type	Metric
2	**PROTECT DATA IN THE CLOUD**				Group	*Met2*
2.2	**Awareness and Training (2.2):** The Fintech's users and staff receive regular security awareness training and are adequately equipped to perform their tasks while prioritizing security, in line with established policies, procedures, and agreements.				Metric	*M et2.2*
2.2.1	PR.AT-1: Are all users informed and trained on the security aspects related to their cloud usage?	HIGH	ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-2, PM-13 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et2.2.1*
2.2.2	PR.AT-2: Do the Fintech's privileged users, such as admins and super users, fully understand their privileges and responsibilities related to the cloud?	HIGH	CCS CSC 9 COBIT 5 APO07.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et2.2.2*

2.2.3	PR.AT-3: Do the Fintech's owners and senior personnel fully understand their privileges and responsibilities related to the cloud?	HIGH	COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et2.2.3*
2.2.4	PR.AT-4: Do the Fintech's information security personnel fully understand their privileges and responsibilities related to the cloud?	Medium	CCS CSC 9 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13	The Fintech owner, administrators, and users need to undergo training.	Sub-Metric	*M et2.2.4*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
2	**PROTECT DATA IN THE CLOUD**				Group	*Met2*
2.3	**Data Security (2.3):** Information and records (data) are managed in alignment with the Fintech's risk strategy to ensure the confidentiality, integrity, and availability of information.				Metric	*M et2.3*
2.3.1	PR.DS-1: Is data protected while at rest in the cloud?	HIGH	CCS CSC 17 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 SC-28	Cloud Providers to use Encryption.	Sub-Metric	*M et2.3.1*
2.3.2	PR.DS-2: Is data protected while in transit, such as during uploads or downloads from the cloud?	HIGH	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 CCS CSC 17 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A. 13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	Cloud providers to use TLS.	Sub-Metric	*M et2.3.2*
2.3.3	PR.DS-3: Does the Fintech have sufficient bandwidth capacity to ensure the availability of data if the cloud is maintained?	HIGH	COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISO/IEC 27001:2013 A.6.2.2, A.13.1.1,A. 13.2.1	Use of secondary links.	Sub-Metric	*M et2.3.3*
2.3.4	PR.DS-4: Does the cloud provider implement approved firewall rule sets and access control lists between network fabrics to restrict the flow of information to specific information system services, while addressing multi-tenancy concerns?	Medium	ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A. 7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A. 9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A. 13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS- 6, SC-7, SC-8, SC-13, SC-31, SI-4	Cloud providers need to provide the information.	Sub-Metric	*M et2.3.4*
2.3.5	PR.DS-5: Does the Fintech or cloud provider use integrity verification tools to monitor and detect unauthorized changes to the organization’s software and information?	LOW	ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SI-7	Cloud providers t have Monitoring tools.	Sub-Metric	*M et2.3.5*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
2	**PROTECT DATA IN THE CLOUD**				Group	*Met2*
2.4	**Information Protection Processes and Procedures (2.4):** Security policies that define roles, responsibilities, scope, processes, and procedures are maintained and utilized to manage the protection of information systems and assets.				Metric	*M et2.4*
2.4.1	PR.IP-1: Does the Fintech create and maintain configurations for IT control systems, both for the cloud and internal systems?	HIGH	COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 CCS CSC 3, 10	Cloud providers need to provide the information.	Sub-Metric	*M et2.4.1*
2.4.2	PR.IP-2: Does the Fintech have a System Development Life Cycle (SDLC) in place to manage both cloud and internal systems?	Medium	COBIT 5 APO13.01 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1,A. 14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	Fintechs to impliment a SDLC.	Sub-Metric	*M et2.4.2*

2.4.3	PR.IP-3: Does the Fintech have change control processes in place to track changes in the cloud provider's functionality?	Medium	COBIT 5 BAI06.01, BAI01.06 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4	Cloud providers need to provide the information.	Sub-Metric	*M et2.4.3*
2.4.4	PR.IP-4: Does the cloud provider regularly create, test, and validate backups of data stored in the cloud?	HIGH	COBIT 5 APO13.01 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	Cloud providers to have offshore backups.	Sub-Metric	*M et2.4.4*
2.4.5	PR.IP-5: Is data in the cloud destroyed in accordance with policy, with no copies retained without the Fintech's knowledge?	HIGH	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.4.4.4 NIST SP 800-53 Rev. 4 MP-6	Cloud providers need to provide the information.	Sub-Metric	*M et2.4.5*
2.4.6	PR.IP-6: Does the cloud provider share information on the effectiveness of protection technologies with the Fintech?	LOW	ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	Cloud providers need to provide the information.	Sub-Metric	*M et2.4.6*
2.4.7	PR.IP-7: Are Incident Response, Business Continuity, and disaster/incident recovery plans in place and effectively managed by the cloud provider?	Medium	COBIT 5 DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A. 17.1.2 NIST SP 800-53 Rev. 4 CP-2, IR-8	Cloud providers need to provide the information.	Sub-Metric	*M et2.4.7*
2.4.8	PR.IP-8: Are the above-mentioned Business Continuity (BC) and Disaster Recovery (DR) plans tested and validated on a regular basis?	LOW	ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	Cloud providers need to provide the information.	Sub-Metric	*M et2.4.8*
2.4.9	PR.IP-9: Does the Fintech have a vulnerability management plan in place?	Medium	ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	Should impliment one.	Sub-Metric	*M et2.4.9*
2.4.10	PR.IP-10: Does the Fintech maintain and repair its IT assets in a timely manner, with all repair and maintenance activities approved and logged?	LOW	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A. 11.2.5 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5	Have IT/IOT support time in place.	Sub-Metric	*M et2.4.10*
2.4.11	PR.IP-11: Is remote maintenance of the Fintech's IT assets approved, logged, and performed in a way that prevents unauthorized access?	HIGH	COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 NIST SP 800-53 Rev. 4 MA-4	Fintechs to ensure network is secure.	Sub-Metric	*M et2.4.11*

Level	Description	Priority	Validation References	Classification	Type	Metric
2	**PROTECT DATA IN THE CLOUD**				Group	*Met2*
2.5	**Protective Technology (2.5):** Technical security solutions are managed to ensure the security and resilience of all IT assets, equipment, and systems, while adhering to relevant policies, procedures, and agreements.				Metric	*M et2.5*
2.5.1	PR.PT-1: Are all records related to audits and logs of cloud usage documented and reviewed in compliance with the Fintech's internal policies?	Medium	CCS CSC 14 ACOBIT 5 APO11.04 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family	Admins to administer logging Softwares/Tools.	Sub-Metric	*M et2.5.1*
2.5.2	PR.PT-2: Are removable media used within the Fintech's premises protected and their usage restricted in accordance with the Fintech's policies?	Medium	COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4	Admin to enforce rules.	Sub-Metric	*M et2.5.2*

2.5.3	PR.PT-3: Is access to equipment, systems, and IT assets managed in a way that enforces the principle of least functionality?	Medium	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7	Admin to enforce rules.	Sub-Metric	*M et2.5.3*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
3	**DETECT SECURITY INCIDENTS IN THE CLOUD**				Group	*Met3*
3.1	**Anomalies and Events (3.1):** Unusual or irregular activities are detected promptly, and the potential impacts of such events are thoroughly understood.				Metric	*M et3.1*
3.1.1	DE.AE-1: Does the Fintech manage network operations and data flow for users through the cloud?	LOW	COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	To use SIEM system.	Sub-Metric	*M et3.1.1*
3.1.2	DE.AE-2: Does the Fintech have measures in place to detect events and analyze attacks and their methods?	LOW	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR2.10, SR 2.11, SR2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	Fintechs to Impliment IPS and IDS.	Sub-Metric	*M et3.1.2*
3.1.3	DE.AE-3: Does the cloud provider offer tools or methods to assess the impact of events in the cloud?	Medium	COBIT 5 APO12.06 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4	Cloud providers need to provide the information.	Sub-Metric	*M et3.1.3*
3.1.4	DE.AE-4: Has the cloud provider established incident alert thresholds for their cloud services?	Medium	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.2.3.10 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	Cloud providers need to provide the information.	Sub-Metric	*M et3.1.4*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
3	**DETECT SECURITY INCIDENTS IN THE CLOUD**				Group	*Met3*
3.2	**Security Continuous Monitoring (3.2):** IT systems and assets are monitored at appropriate intervals to detect security events and assess the effectiveness of security controls.				Metric	*M et3.2*
3.2.1	DE.CM-1: Is the LAN and WAN monitored to detect potential cloud security events?	Medium	CCS CSC 14, 16 COBIT 5 DSS05.07 NIST SP 800-53 Rev. 4 AC-2, AU-12	Admins to implimen Monitoring Tools.	Sub-Metric	*M et3.2.1*
3.2.2	DE.CM-2: Is physical IT equipment monitored to detect potential cloud security threats?	LOW	ISA 62443-2-1:2009 4.3.3.3.8 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20	SIEM Implimentation.	Sub-Metric	*M et3.2.2*
3.2.3	DE.CM-3: Is personnel activity monitored to detect any breaches and ensure non-repudiation?	LOW	ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	IDS and IPS to b put in place.	Sub-Metric	*M et3.2.3*
3.2.4	DE.CM-4: Is the cloud environment monitored for unauthorized users or connections?	Medium	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Cloud providers need to provide the information.	Sub-Metric	*M et3.2.4*

3.2.5	DE.CM-5: Are vulnerability scans conducted regularly on the cloud environment?	Medium	COBIT 5 BAI03.10 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5	Cloud providers need to provide the information.	Sub-Metric	*M et3.2.5*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
3	**DETECT SECURITY INCIDENTS IN THE CLOUD**				Group	*Met3*
3.3	**Detection Processes (3.3):** Threat detection methods and procedures are continuously maintained and tested to ensure timely and effective awareness of unusual or irregular events.				Metric	*M et3.3*
3.3.1	DE.DP-1: Do the Fintech and cloud provider define the roles and responsibilities of all users to ensure accountability for their actions?	LOW	CCS CSC 5 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	Cloud Providers/ Fintech should clearly define the roles and resposibilities.	Sub-Metric	*M et3.3.1*
3.3.2	DE.DP-2: Do the threat detection measures comply with all relevant requirements?	Medium	ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4	Measures shoud be relevant and up to standard.	Sub-Metric	*M et3.3.2*
3.3.3	DE.DP-3: Are the above-mentioned threat detection measures regularly tested?	LOW	ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI- 4	Testing should be done.	Sub-Metric	*M et3.3.3*
3.3.4	DE.DP-4: Are the above-mentioned threat detection measures communicated to the Fintech's personnel?	Medium	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	Clear and timely communication.	Sub-Metric	*M et3.3.4*
3.3.5	DE.DP-5: Are the above-mentioned threat detection measures and processes continuously improved?	LOW	COBIT 5 APO11.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM- 14	Regular updates required.	Sub-Metric	*M et3.3.5*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
4	**RESPOND TO SECURITY EVENTS IN THE CLOUD**				Group	*Met4*
4.1	**Response Planning (4.1):**Procedures and measures are implemented and continuously maintained to ensure prompt and effective responses to identified cloud security incidents within the Fintech ecosystem.				Metric	*M et4.1*
4.1.1	RS.RP-1:A valid response plan is executed promptly in the event of a detected incident, ensuring an effective and timely resolution within the Fintech environment.	LOW	COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8	Fintech/ Cloud Providers to clarify how.	Sub-Metric	*M et4.1.1*
4.2	**Communications (4.2):**Response activities are coordinated within the Fintech organization, including collaboration with external entities such as law enforcement agencies when necessary.				Metric	*M et4.2*
4.2.1	RS.CO-1:Do all Fintech staff understand their roles and the established procedures to follow when a response is required?	LOW	ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3,4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	Staff to undergo training.	Sub-Metric	*M et4.2.1*
4.2.2	RS.CO-2: Are all incidents reported in alignment with the predefined criteria within the Fintech organization?	LOW	ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	Clear stracture of the organization to be presented.	Sub-Metric	*M et4.2.2*

4.2.3	RS.CO-3: Is information exchanged between the Fintech organization and the cloud provider in accordance with the established response plans?	LOW	ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	Fintechs/ Cloud providers to clarify.	Sub-Metric	*M et4.2.3*
4.2.4	RS.CO-4: Is coordination between the Fintech organization and the cloud provider carried out in alignment with the established response plans?	LOW	ISA 62443-2-1:2009 4.3.4.5.5 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud providers and Fintech need to have a good plan.	Sub-Metric	*M et4.2.4*

Level	Description	Priority	Validation References	Classification	Type	Metric
4	**RESPOND TO SECURITY EVENTS IN THE CLOUD**				Group	*Met4*
4.3	**Analysis (4.3):** Thorough analysis is conducted to ensure that response and recovery efforts are adequate and effective within the Fintech environment.				Metric	*M et4.3*
4.3.1	RS.AN-1: Are notifications from detection systems thoroughly investigated by both cloud providers and administrators within the Fintech organization?	LOW	COBIT 5 DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	Fintech/ Cloud Providers to clarify how.	Sub-Metric	*M et4.3.1*
4.3.2	RS.AN-2: Is the potential impact of any incident fully understood by the Fintech organization?	Medium	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4	Staff to undergo training.	Sub-Metric	*M et4.3.2*
4.3.3	RS.AN-3: Are forensic investigations conducted for any potential security incidents within the Fintech organization?	LOW	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR2.10, SR 2.11, SR2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4	Organization to have measures in place.	Sub-Metric	*M et4.3.3*
4.3.4	RS.AN-4: Are incidents categorized in accordance with the response plans within the Fintech organization?	LOW	ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8	Proper planning to be in place.	Sub-Metric	*M et4.3.4*

Level	Description	Priority	Validation References	Classification	Type	Metric
4	**RESPOND TO SECURITY EVENTS IN THE CLOUD**				Group	*Met4*
4.4	**Mitigation (4.4):** Strategic actions are taken to prevent the escalation of a security incident, with measures implemented to mitigate and eliminate the threat within the Fintech environment.				Metric	*M et4.4*
4.4.1	RS.MI-1: Are cloud incidents contained promptly as per the established protocols and previous reports within the Fintech organization?	HIGH	ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 IR-4	Cloud providers need to provide the information.	Sub-Metric	*M et4.4.1*
4.4.2	RS.MI-2: Are cloud incidents mitigated effectively when they occur, following the protocols outlined in previous reports within the Fintech organization?	HIGH	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4	Cloud providers need to provide the information.	Sub-Metric	*M et4.4.2*
4.4.3	RS.MI-3: Are new vulnerabilities either mitigated or documented as accepted risks within the Fintech organization?	HIGH	ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5	Cloud providers need to provide the information.	Sub-Metric	*M et4.4.3*
4.5	**Improvements (4.5):** The Fintech organization's response activities are enhanced by integrating lessons learned from both current and past detection and response efforts.				Metric	*M et4.5*

4.5.1	RS.IM-1: Are response plans updated to incorporate lessons learned from previous incidents within the Fintech organization?	LOW	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud providers need to provide the information.	Sub-Metric	*M et4.5.1*
4.5.2	RS.IM-2: Are response strategies updated as needed based on lessons learned and evolving threats within the Fintech organization?	LOW	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud providers need to provide the information.	Sub-Metric	*M et4.5.2*
Level	**Description**	**Priority**	**Validation References**	**Classification**	**Type**	**Metric**
5	**RECOVER FROM BREACHES IN THE CLOUD**				Group	*Met5*
5.1	**Recovery Planning (5.1):** Recovery procedures and techniques are executed and maintained to ensure the effective restoration of IT systems or assets impacted by security events within the Fintech organization.				Metric	*M et5.1*
5.1.1	RC.RP-1: Is the recovery plan effectively implemented in the event of a security incident within the Fintech organization?	Medium	CCS CSC 8 COBIT 5 DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	Cloud providers need to provide the information.	Sub-Metric	*M et5.1.1*
5.2	**Improvements (5.2):** Recovery planning and techniques are continuously refined by integrating lessons learned.				Metric	*M et5.2*
5.2.1	RC.IM-1: Do all recovery documents incorporate lessons learned from past incidents within the Fintech organization?	LOW	COBIT 5 BAI05.07 ISA 62443-2-1 4.4.3.4	Cloud providers need to provide the information.	Sub-Metric	*M et5.2.1*
5.2.2	RC.IM-2: Are all recovery strategies updated to reflect lessons learned and evolving requirements within the Fintech organization?	LOW	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 COBIT 5 BAI07.08	Cloud providers need to provide the information.	Sub-Metric	*M et4.5.2.2*
5.3	**Communications (5.3):** Restoration activities are coordinated with the Fintech organization.				Metric	*M et5.3*
5.3.1	RC.CO-1: Restoration progress and accomplishments are communicated to relevant Fintech teams.	Medium	NIST SP 800-53 Rev. 4 CP-2, IR-4	Cloud providers need to provide the information.	Sub-Metric	*M et5.3.1*

Level	Description	Metric	Sec Index
1	**IDENTIFY RISKS IN CLOUD**	Met1	
1.1	**Asset Management (1.1):** The resources, personnel, infrastructure, equipment, and services that support the Fintech's business processes are identified and managed in alignment with their significance to business goals and the organization's risk strategy.	M et1.1	
1.1.1	ID.AM-1: Are all physical IT equipment (computers, laptops, BYOD) within the Fintech inventoried?	M et1.1.1	**0**
1.1.2	ID.AM-2: Is there a complete inventory of all system and application software within the Fintech?	M et1.1.2	**0**
1.1.3	ID.AM-3: Do cloud providers enable the Fintech to specify where their content is stored, ensure its security during transit and at rest, and manage it effectively?	M et1.1.3	**1**
1.1.4	ID.AM-4: Does the Fintech ensure that external information system service providers comply with the Fintech's information security requirements, including applicable laws, policies, regulations, standards, and guidelines?	M et1.1.4	**0**
1.1.5	ID.AM-5: Does the cloud provider define the resilience measures in place to support the delivery of critical services across all operating states (e.g., during normal operations, under duress or attack, and during recovery)?	M et1.1.5	**1**
Secure ?			**0**