Recommended Control Requirements Pertaining for Sample Risk Scenarios - FinCSIRT

		Required Control Categories				
	Risk Scenario	**People**	**Technology**	**Data**	**Location (Physical)**	**Log Files required**
1	User receives phishing email via internal party	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize phishing attacks to avoid clicking on malicious links) • Policy implementation and awareness on email usage • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Restrict internal emails to be received only using the email server itself. (No unauthenticated email submissions from outside allowed) • Scan emails (Virus scan) • SPAM filter • Disable Hyper links using group policy			• email delivery logs • email Anti-Malware system logs • Anti Phishing/Spam system logs
2	User receives phishing email via external party	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize phishing attacks to avoid clicking on malicious links) • Policy implementation and awareness on email usage • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• SPF record check • Scan emails (Virus Scan) • SPAM filter • Digitally sign email from domain(DKIM) • Tag all external emails with an [EXTERNAL] subject tag			• email delivery logs • email Anti-Malware system logs • Anti Phishing/Spam system logs
3	User Clicks on malicious links and downloading malicious software	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize types of attacks and to avoid clicking on malicious links) • Policy implementation and awareness on acceptable infrastructure use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Disable Hyper links using group policy (Via MS OUTLOOK) • Up-to-date Endpoint protection systems on workstations • Web filtering at the perimeter level • Integration of Threat Intelligence feeds to the web filtering			• Proxy/internet gateway logs • Anti-malware protection system logs • DHCP Logs to identify the clients (In a DHCP environment)
4	User Clicks on malicious links and directed to malicious phishing site	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize types of attacks and to avoid clicking on malicious links) • Policy implementation and awareness on acceptable infrastructure use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Up-to-date Endpoint Anti-Malware protection systems on workstations • Web filtering at the perimeter level			• Proxy/internet gateway logs • Anti-malware protection system logs • DHCP Logs to identify the clients (In a DHCP environment)
5	User enter sensitive information to malicious website	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize malicious websites/entities) • Policy implementation and awareness on data governance and acceptable user policies • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Up-to-date Endpoint protection (URL filtering) systems on workstations • Web filtering at the perimeter level	• Allow only required access to sensitive information according to the data classification		• Anti-Malware protection Logs • Proxy/Internet gateway logs
6	Malicious software propagate via network to Other PC	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize malicious software /applications and behavior) • Appoint an incident response team • Policy implementation and awareness on incident response • Compliance monitoring on organizational policies	• Install End-point protections and centrally manage them to enforced policy on scans and updates • Operating System update management • Disable drive Auto Run • Firewall to implement ACLs • Personal firewalls on endpoints • Vulnerability assessments on the network. • Regular network monitoring • Network segmentation	• Take regular backups • Test and Verify the backups		• Proxy/internet gateway logs • email delivery logs • Anti-Malware protection system logs • Firewall logs • Network monitoring logs /Information • DHCP Logs to identify the clients (In a DHCP environment)
7	Malicious software propagate via network to File Share	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize malicious software /applications and behavior) • Appoint an incident response team • Train the technical staff on secure configurations and system hardening • Policy implementation and awareness on incident response and backup • Compliance monitoring on organizational policies	• Use password protection to limit file share access • Disable anonymous access • Install End point protections and centrally manage them to policy on scans and updates • Operating System/Application update management • Disable Auto Run • Use a firewall to implement proper ACLs and IPS to control the traffic • Vulnerability assessments on the network. • Regular network monitoring • Network segmentation	• Take regular backups • Test and Verify the backups • Keep the backups offline		• Audit logs • Anti-Malware protection Logs • Firewall Logs • Network monitoring logs/Information • Backup Logs
8	Malicious software propagate to Servers via the network	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize malicious software /applications and behavior) • Appoint an Incident response team • Train the technical staff on secure configurations and system hardening • Policy implementation and awareness on incident response and backup • Compliance monitoring on organizational policies	• Install Anti-malware protection on the servers • Harden the server and disable unwanted services • Operating System/Application update management • Use ACLs or Firewalls to restrict unauthorized access • Conduct vulnerability assessments • Network segmentations according to business requirements • Regular network monitoring • ACL implementations	• Take regular backups • Test and Verify the backups • Keep the backups offline		• Audit logs • Anti-Malware protection Logs • Firewall / ACL logs • Backup Logs • Network monitoring logs/Information
9	Malicious software infect a Computer/Server	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (To recognize malicious software /applications and behavior) • Appoint an Incident response team • Policy implementation and awareness on incident response • Compliance monitoring on organizational policies	• Install End point protections and centrally manage them to enforced policy on scans and updates • Operating System update management • Disable Auto Run • Use of personal firewalls (More specifically for the personal computers)	• Take regular backups • Test and Verify the backups		• Anti-Malware protection Logs • Firewall / ACL logs • Backup Logs
10	Unintended data disclosure by an internal party	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On data classifications and sensitive data handling) • Data disposal process done by an authorized person. • Dual authorization/supervision • Policy implementation and awareness on data governance and acceptable user policies • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Methods of disposing media both electronic and printed • Access Control implementation • Data Loss/Leak Prevention implementation	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Proxy/internet gateway logs • email delivery logs • Anti-Malware protection system logs • Firewall logs • Network monitoring logs /Information • DHCP Logs to identify the clients (In a DHCP environment) • Physical access logs • DLP alerts
11	Unintended data disclosure by an external party	• Information Security Training/Awareness sessions for the external parties on organizational information handling and data classification policies and legal actions safeguarding them. • Contractual agreements with Third-party • Data disposal process done by an authorized person. • NDA Agreements are signed with external parties who has access to sensitive information	• Methods of disposing media both electronic and printed • Access Control implementation • Data Loss/Leak Prevention implementation	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Access control logs for Network/Systems • Physical access logs
12	Intended data disclosure by an internal party	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On data classifications and sensitive data handling /organizational policy) • Employee disciplinary Actions • Employee termination procedure • Contracts and agreements • Policy implementation and awareness on data governance and acceptable user policies • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Methods of disposing media both electronic and printed • Access Control implementation • Data Loss/Leak Prevention implementation	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Proxy/internet gateway logs • email delivery logs • Anti-Malware protection system logs • Firewall logs • Network monitoring logs /Information • DHCP Logs to identify the clients (In a DHCP environment) • Physical access logs • DLP alerts
13	Intended data disclosure by an external party	• Information Security Training/Awareness sessions for the external parties on organizational information handling and data classification policies and legal actions safeguarding them. • Contractual agreements with Third-party • disposal process done by an authorized person. • Non-Disclosure Agreements • Policy implementation and awareness on data governance and data backups • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Methods of disposing media both electronic and printed • Access Control implementation • Data Loss/Leak Prevention implementation	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Access control logs for Network • Physical access logs

14	Data unavailability due to data corruption/encryption/deletion	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On proper data handling and management) • Appoint Incident response team • Policy implementation and awareness on data governance Incident Response and data backups • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances		• Maintaining Regular Backups • Keeping Backup integrity data (hashing) • Continues Backup verification • Keeping the encryption keys safe		• Backup Logs • System Logs
15	Data unavailability due to network unavailability/slowness raised by the malicious software	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On identifying malicious behavior) • Appoint Incident response team	• Install End point protections and centrally manage them to enforced policy on scans and updates • Operating System update management • Use a firewall to implement proper ACLs and IPS based actions • Personal firewalls on endpoints • Vulnerability assessments on the network. • Regular network monitoring • Network segmentation			• System Logs • Anti-Malware protection system logs • Firewall Logs • Network monitoring information/Logs
16	Data Stolen via malicious software	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On malicious software and malicious actors) • Appoint incident response team • Policy implementation and awareness on data governance and acceptable use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Install End point protections and centrally manage them to enforced policy on scans and updates • Operating System update management • Use a firewall to implement proper ACLs and IPS based actions • Personal firewalls on endpoints • Vulnerability assessments on the network. • Regular network monitoring • Network segmentation			• System Logs • Anti-Malware protection system logs • Firewall Logs • Network monitoring information/Logs
17	Data Stolen via internal authorized person	• Employee disciplinary Actions • Employee termination procedure • Contracts and agreements • Background checks conducted on the recruitments • Policy implementation and awareness on data governance and acceptable use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Maintain Access Control lists	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Access control logs • Workstation System Logs • Physical access logs
18	Data Stolen via internal unauthorized person	• Employee disciplinary Actions • Employee termination procedure • Contracts and agreements • Background checks conducted on the recruitments • Policy implementation and awareness on data governance and acceptable use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Maintain Access Control lists	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Access control logs • Workstation System Logs • Physical access logs
19	Data Stolen via personal communication method chat, email, SMS, call	• Employee termination procedure • Contracts and agreements • Background checks conducted on the recruitments • Policy implementation and awareness on BYOD and personal device usage • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Restrictions on personal resource usage in sensitive areas	• Encrypt all sensitive company information • Records of media managing and disposal • Allow only required access to sensitive information according to the data classification	• Limit access to the sensitive information locations • Location based surveillance	• Access control logs • Workstation System Logs • Physical access logs
20	Data stolen via business communication channels (E.g.: hacker downloading application data remotely)	• Appoint incident response team • Employee termination procedure • Contracts and agreements • Background checks conducted on the recruitments • Policy implementation and awareness on data governance and acceptable use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Encrypted communication channels • Server / system Hardening • Conduct periodic Vulnerability Assessment and Penetration testing • Use strong authentication and authorization mechanism • Network segmentation and access control • Network monitoring • Security Incident and Log monitoring • Data Loss/Leak Prevention implementation	• Data encryption at data Rest , Data Process/In Use and Data in Transit		• System access logs • Networking monitoring information/Logs • Authentication and Access Logs • Physical access logs
21	Data Stolen via physical medium	• Employee disciplinary Actions • Employee termination procedure • Contracts and agreements • Background checks conducted on the recruitments • Appoint incident response team • Policy implementation and awareness on data governance and acceptable use • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Authentication and Authorization mechanisms on all sensitive data/systems • Audits on access logs • Data Encryption • Prevent Uploads ,USB/SD card, CV/DVD burning without prior approvals. • Data Loss/Leak Prevention implementation	• Data encryption at data Rest , Data Process/In Use and Data in Transit	• Limit access to the sensitive information locations • Location based surveillance	• System access logs • Networking monitoring information/Logs • Physical access logs
22	Hacker penetrate internal systems	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On incident handling and identifying malicious behavior) • Policy implementation and awareness on incident handling • Compliance monitoring on organizational policies	• Install End point protections and centrally manage them to enforced policy on scans and updates • Operating System update management • Network segmentation • Monitor network for anomalies • Review login history • Use Strong password • Change default passwords on the applications • Disable unused services and ports • Vulnerability assessments on the network • Data Integrity should be monitored • Forensics are performed/incident management procedure		• Limit access to the sensitive information locations • Location based surveillance	• Anti-malware protection system logs • Networking monitoring information/Logs • File Integrity monitoring system logs • Firewall Logs • System access/Login logs • NetFlow/ OpenFlow information (If Available) • Physical access logs
23	Hacker penetrate external systems (E.g.: external hosted DNS, Web, Cloud)	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On incident handling and identifying malicious behavior) • Policy implementation and awareness on incident handling	• Install End point protections and centrally manage them to enforced policy on scans and updates • Operating System update management • Review login history • Use Strong password • Change default passwords on the applications • Disable unused services and ports • Vulnerability assessments on the network • Forensics are performed/incident management procedure • Monitor external system activity • Logins expire after a short period of inactivity • Use TLS for communication whenever possible • Data Integrity should be monitored			• Networking monitoring information/Logs • System access/Login logs • NetFlow/ OpenFlow information (If Available)
24	Hackers penetrate internal systems and has access to SWIFT network	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On criticality and safeguarding SWIFT network) • SWIFT systems should be differentiate from other infrastructure to the bank staff	• Critical Data backup • Operating System update management • SWIFT network should be separated to a different network • Implement swift mandatory SWIFT security controls • Install End point protections and centrally manage them to enforced policy on scans and updates • Firewall to protect the special access requirements according to the SWIFT network • Forensics are performed/incident management procedure		• Limit access to the sensitive information locations • Location based surveillance	• Networking monitoring information/Logs • System access/Login logs • Firewall Logs • NetFlow/ OpenFlow information (If available) • Physical access logs
25	Hackers penetrate internal systems and has access to ATM network	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On criticality and safeguarding ATM network)	• Critical Data backup • Operating System/application update management • ATM network should be separated to a different network • Install End point protections and centrally manage them to enforced policy on scans and updates • Firewall to protect the special access requirements according to the ATM network		• Limit access to the sensitive information locations • Location based surveillance	• Networking monitoring information/Logs • ATM System access/Login logs • Firewall Logs • NetFlow/ OpenFlow information (If Available) • Physical access logs

26	Malicious software spread/installed on SWIFT network	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On criticality and safeguarding SWIFT network)	• Critical Data backup • Operating System update management • Install End point protections and centrally manage them to enforced policy on scans and updates • Firewall to protect the special access requirements according to the SWIFTnetwork • Network segmentation • Change the default BIOS password • Monitor system reboots / alarms/alerts/logs • Implement swift mandatory SWIFT security controls			• Anti-malware protection system logs • Networking monitoring information/Logs • SWIFT System access/Login logs • Firewall Logs
27	Malicious software spread/installed on ATM network	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On criticality and safeguarding ATM network)	• Critical Data backup • Operating System update management • Install End point protections and centrally manage them to enforced policy on scans and updates • Firewall to protect the special access requirements according to the ATM network • Network segmentation • Change the default BIOS password • Monitor system reboots / alarms/alerts/logs • Monitor software updates being installed unauthorized • Forensics are performed/incident management procedure			• Anti-malware protection system logs • Networking monitoring information/Logs • ATM System access/Login logs • Firewall Logs
28	Credential Stealing/Leaking	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On safeguarding credentials) • Clear desk/clear screen policy • Policy implementation and awareness credential handling • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Use strong password enforcement • Change the credentials frequently • Store hashes of the password • Multi factor authentication • Monitor/review logins • User Access controls • Password management methods enforced (Password managers etc..) • Anti-Phishing and Anti-Spam methodologies used	• Data encryption at data Rest , Data Process/In Use and Data in Transit	• Limit access to the sensitive information location • Location based surveillance	• Database Access logs • Multi-Factor authentication system Logs • Firewall logs • Access control logs • Physical access logs
29	hacking using network vulnerabilities	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On infrastructure safety) • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Vulnerability assessments / Penetration testing on the network • Network segmentation • Protect Wi-Fi access points • Strong passwords • Access control • Use IDS/IPS to track potential packet floods	• Data encryption at data Rest , Data Process/In Use/In Use and Data in Transit		• Firewall Logs • Switch/Router access Logs • IPS/IDS detection logs • Network monitoring information/Logs
30	hacking using application vulnerabilities	• Appoint incident response team • Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of patch and update management) • In-depth technical training for staff who are responsible for managing the infrastructure • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Vulnerability assessments / Penetration testing • Update and patch management on the applications • Change default passwords on the applications on the applications • Enforcement of server validation on the applications • Properly handle exceptions and default error pages • TLS usage across all communication methods • Restrict administrative services to inside network or filtered endpoints • Disable unused services and ports	• Data encryption at data Rest , Data Process/In Use and Data in Transit		• System/Application version details • Application debug logs • Application error logs • Application access logs • System access logs
31	hacking using OS server vulnerabilities	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of patch and update management) • In-depth technical training for staff who are responsible for managing infrastructure • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Conduct vulnerability assessments and Penetration testing • Install End point protections and centrally manage them to enforce policy on scans and updates • Operating System update management • Disable unused services and ports • Restrict administrative services to inside network or filtered endpoints • Proper update and patch management system for the Operating system	• Data encryption at data Rest , Data Process/In Use and Data in Transit		• System access logs • System audit logs
32	hacking using server software vulnerabilities	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of patch and update management) • In-depth technical training for staff who are responsible for managing the software • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Conduct vulnerability assessments and Penetration testing • Update and patch management on the applications • Change default passwords on the applications on the applications • Enforcement of server validation on the applications • Exception and Error handling • TLS usage across all communication methods • Restrict administrative services to inside network or filtered endpoints	• Data encryption at data Rest , Data Process/In Use and Data in Transit		• System/Application version details • Server Software debug logs • Server Software error logs • Server Software access logs • System access logs
33	hacking using application components and repositories vulnerabilities	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of patch and update management) • In-depth technical training for staff who are responsible for managing the software • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Conduct vulnerability assessments and Penetration testing • Update and patch management on the applications components • Keep a track of all the third party software used for application • Forensics are performed/incident management procedure • Monitor the repositories using a File Integrity monitoring system	• Data encryption at data Rest , Data Process/In Use and Data in Transit		• Repository and library version details
34	Hacking using misconfiguration/poor configuration	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of system hardening) • In-depth technical training for staff who are responsible for managing infrastructure • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Conduct vulnerability assessments and Penetration testing • follow checklist for hardening guidelne for configurations • Continues audits for system configurations	• Data encryption at data Rest , Data Process/In Use and Data in Transit		
35	Network attack via DDOS	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of system hardening) • In-depth technical training for staff who are responsible for managing infrastructure • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Monitor Network abnormal traffic • Use cloud mitigation provider like Cloudflare to redirect the traffic • Local Load balancers • Configuring your firewall or router to drop incoming unnecessary packets • Contact procedures to the ISP • Multiple Communication links			• Networking monitoring information/Logs • Firewall Logs • System access/Login logs • NetFlow/ vs OpenFlow information (If Available)
36	Application containing backdoor	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On importance of system hardening) • In-depth technical training for staff who are responsible for managing applications • Policy implementation and awareness on hardening and securing the infrastructure • Compliance monitoring on organizational policies	• Conduct vulnerability assessments and Penetration testing • Continues network monitoring • Source code analysis			• System Access logs • Networking monitoring information/Logs • Server software Access, Error logs
37	Application logs containing sensitive information	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On data governance and managing data properly) • In-depth technical training for staff who are responsible for managing the application • Conducting awareness sessions for the development team on the organizational data classification	• Log segmentation for Security , Access and Transaction • Code analysis for identifying logging problems • Access Control to logs	• Data encryption at data Rest , Data Process/In Use and Data in Transit • Data masking		• Application related logs
38	Hacker/unauthorized user changing configuration files/critical files	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On identifying malicious behavior) • In-depth technical training for staff who are responsible for managing the application • Policy implementation and awareness on configuration management • Compliance monitoring on organizational policies	• File Integrity monitoring system for critical configuration files • Change management systems and Audit logs		• Limit access to the sensitive information locations • Location based surveillance	• FIMS logs • System Audit logs • Physical access logs

39	Unauthorized/hacker conduct malicious transactions	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On identifying malicious behavior) • In-depth technical training for staff who are responsible for managing the application • Policy implementation and awareness on configuration management • Compliance monitoring on organizational policies	• Maintain transaction logs for every transaction • Monitor transaction for anomaly • Forensics are performed/incident management procedure			• Transaction logs • Application access logs • System access logs • Database access and transaction logs
40	Unavailability of the systems due to natural disaster/failure of critical services	• Appoint incident response team • Training sessions for BCP/DR procedures • Policy implementation and awareness on BCP/DR • Compliance monitoring on organizational policies	• DR site to cater RTO objective of the organization • DR site to cater RPO objective of the organization • BCP strategy		• Data duplication and backups on multiple physical locations • DR management	• System uptime monitoring log
41	Unavailability of the systems due to attacks	• Appoint incident response team • Training sessions for BCP/DR procedures • In-depth technical training for staff who are responsible for securing the infrastructure • Policy implementation and awareness on BCP/DR • Compliance monitoring on organizational policies	• DR site to cater RTO objective of the organization • DR site to cater RPO objective of the organization • BCP strategy		• Data duplication and backups on multiple physical locations • DR management	• System uptime monitoring log
42	Unavailability of the systems due to hardware failure	• Training sessions for BCP/DR procedures • In-depth technical training for staff who are responsible for managing the infrastructure • Policy implementation and awareness on critical system management • Compliance monitoring on organizational policies	• DR site to cater RTO objective of the organization • DR site to cater RPO objective of the organization • BCP strategy • High availability systems		• Data duplication and backups on multiple physical locations • DR management	• System uptime monitoring log
43	Unavailability of the systems due to software failure	• Training sessions for BCP/DR procedures • In-depth technical training for staff who are responsible for managing the infrastructure • Policy implementation and awareness on critical system management • Compliance monitoring on organizational policies	• DR site to cater RTO objective of the organization • DR site to cater RPO objective of the organization • BCP strategy • High availability systems			• System uptime monitoring log • Application debug, error and access logs
44	Unavailability of the systems due to external link down	• Training sessions for BCP/DR procedures • In-depth technical training for staff who are responsible for managing the infrastructure • Policy implementation and awareness on critical system management • Compliance monitoring on organizational policies	• DR site to cater RTO objective of the organization • DR site to cater RPO objective of the organization • BCP strategy • High availability systems using multiple communication links		• Critical Services to be addressed with backup link • DR management	• Communication link uptime monitoring log
45	Unavailability of the systems due to internal link down	• Training sessions for BCP/DR procedures • In-depth technical training for staff who are responsible for managing the infrastructure • Policy implementation and awareness on critical system management • Compliance monitoring on organizational policies	• DR site to cater RTO objective of the organization • DR site to cater RPO objective of the organization • BCP strategy • High availability network infrastructure using internal routing paths		• Resilient Network infrastructure design using technologies such as STP etc.. • Critical Services to be addressed with backup link • DR management	• Internal network monitoring information /logs
46	Unavailability of the systems due to capacity overloading	• In-depth technical training for staff who are responsible for managing the infrastructure	• Identify critical IT resources that needs maximum availability • Identify seasonality peaks in business activity • Projections for future capacity requirements • Load Balancing within multiple backends			• System performance monitoring metrics (CPU, Memory etc.…) • System logs
47	Unavailability of the service due to misconfiguration	• In-depth technical training for staff who are responsible for managing the infrastructure	• High availability systems • Change management systems followed		• Configuration backups on multiple physical locations • DR management	• Configuration management system logs
48	Critical person unavailability	• Multiple role training for redundant staff management	• Documentation on procedures for critical process • Process automation			
49	Data alter by authorized parties	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On data governance and criticality) • Employee disciplinary Actions • Employee termination procedure • Contracts and agreements • Background checks conducted on the recruitments • Policy implementation and awareness on information sharing • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Access control systems • Periodic Audit and review logs • Forensics are performed/incident management procedure • File Integrity monitoring system for critical files		• Limit access to the sensitive information locations • Location based surveillance	• Access control logs • FMIS logs • Physical access logs
50	Data alter by unauthorized parties	• Continuous Information Security Training Sessions / Awareness sessions/ Drills for the staff (On data governance and criticality) • Employee disciplinary Actions • Employee termination procedure • Contracts and agreements • Enforcement of policies related to third-party service providers • Policy implementation and awareness on information sharing • Compliance monitoring on organizational policies • Implement and awareness on disciplinary actions for non-compliances	• Access control systems • Periodic Audit and review logs • Forensics are performed/incident management procedure • File Integrity monitoring system for critical files		• Limit access to the sensitive information locations • Location based surveillance	• Access control logs • FMIS logs • Physical access logs

* BCP,DR and Incident response policy and procedure should address the risk scenarios based on the criticality of the affected assets

* Minimum requirement for the relevant policies and procedures, Please refer the minimum policy requirement guide

* Continuous Audit, Drills, Revise and Improvement should be done periodically according to the defined KPI,KCI and KRI

* KPI, KCI, KRI should be validated regularly and fine-tune

* Control implementation should be in accordance with the risk reduction requirements of the company.

* Control should configured in accordance with the relevant risk criticality level