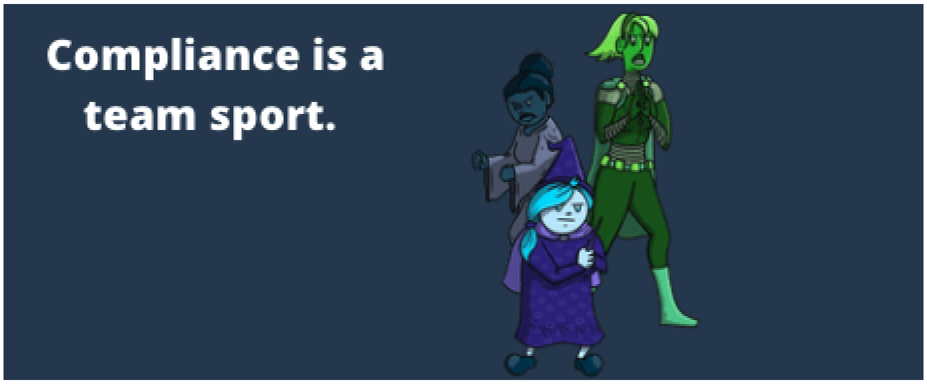

In May 2017, the Saudi Arabian Monetary Authority (SAMA) issued Version 1.0 of its Cyber Security Framework (SAMA CSF). In the introduction, SAMA noted that applying new online services and new developments, such a Fintech and blockchain, require additional regulatory standards to protect against continuously evolving threats.

SAMA explained its Framework's objectives as:

1. To create a common approach for addressing cyber security within the Member Organizations.
2. To achieve an appropriate maturity level of cyber security controls within the Member Organizations.
3. To ensure cyber security risks are properly managed throughout the Member Organizations.

Moreover, SAMA noted that it relied on frameworks previously established by the National Institute of Standards and Technology (NIST), Information Security Forum (ISF), International Standards Organization (ISO), BASEL, and Payment Card Industry Data Security Standard (PCI DSS).

The SAMA CSF defines cyber security as:

> the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.

Within that definition, it incorporates specific definitions governing confidentiality, integrity, and availability:

- Confidentiality – Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure or (un)intended leakage of sensitive data).
- Integrity – Information assets are accurate, complete and processed correctly (i.e., protected from unauthorized modification, which may include authenticity and non-repudiation).

- Availability – Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption).

The SAMA CSF defines its scope as:

- Electronic information.
- Physical information (hardcopy).
- Applications, software, electronic services and databases.
- Computers and electronic machines (e.g., ATM).
- Information storage devices (e.g., hard disk, USB stick).
- Premises, equipment and communication networks (technical infrastructure).

Additionally, it focuses more broadly than other financial cybersecurity frameworks by incorporating applicability to the following industries:

- All Banks operating in Saudi Arabia;
- All Insurance and/or Reinsurance Companies operating in Saudi Arabia;
- All Financing Companies operating in Saudi Arabia;
- All Credit Bureaus operating In Saudi Arabia;
- The Financial Market Infrastructure

As a risk-based framework based on organization maturity, SAMA CSF requires formalized policies, controls, and continuous monitoring to achieve a fully functioning compliance program.

3.1.1 Cyber Security Governance

Principle

A cyber security governance structure should be defined and implemented, and should be endorsed by the board.

Objective

To direct and control the overall approach to cyber security within the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.1.1 - 3.a., 3.b., 3.c	The following positions should be represented in the cyber security committee: a. senior managers from all relevant departments (e.g.,	

	COO, CIO, compliance officer, heads of relevant business departments); b. Chief information security officer (CISO); c. Internal audit may attend as an “observer.	
3.1.1 - 7	The cyber security function should report directly to the CEO/managing director of the Member Organization or general manager of a control function.	

3.1.2 Cyber Security Strategy

Principle

A cyber security strategy should be defined and aligned with the Member Organization’s strategic objectives, as well as with the Banking Sector’s cyber security strategy.

Objective

To ensure that cyber security initiatives and projects within the Member Organization contribute to the Member Organization’s strategic objectives and are aligned with the Banking Sector’s cyber security strategy.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.1.2 - 2.a., 2.b., 2.c	The cyber security strategy should be aligned with: a. the Member Organization’s overall objectives; b. the legal and regulatory compliance requirements of the Member Organization; c. the Banking Sector’s cyber security strategy	

3.1.2-3.a., 3.b., 3.c.	The cyber security strategy should address: a. the importance and benefits of cyber security for the Member Organization; b. the anticipated future state of cyber security for the Member Organization to become and remain resilient to (emerging) cyber security threats; c. which and when cyber security initiatives and projects should be executed to achieve the anticipated future state.	

3.1.3 Cyber Security Policy

Principle

A cyber security policy should be defined, approved and communicated.

Objective

To document the Member Organization’s commitment and objectives of cyber security, and to communicate this to the relevant stakeholders.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.1.3-4c	The cyber security policy should include: c. a statement of the board’s intent, supporting the cyber security objectives;	
3.1.3-4.f.2, 4.f.4, 4.f.7	4. The cyber security policy should include: f. cyber security requirements	

	that ensure: 2. information is protected in terms of cyber security requirements, in line with the risk appetite; 4. cyber security risk assessments are conducted for information assets; 7. cyber security breaches and suspected cyber security weaknesses are reported;	

3.1.4 Cyber Security Roles and Responsibilities

Principle

Responsibilities to implement, maintain, support and promote cyber security should be defined throughout the Member Organization. Additionally, all parties involved in cyber security should understand and take their role and responsibilities.

Objective

To ensure that relevant stakeholders are aware of the responsibilities with regard to cyber security and apply cyber security controls throughout the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.1.4-1a.,1.b,1.c.	1. The Board of Directors has the ultimate responsibility for cyber security, including: a. ensuring that sufficient budget for cyber security is allocated; b. approving the cyber security committee charter; c. endorsing (after being approved by the cyber security committee): 1. the cyber security governance; 2. the cyber security strategy;	

	3. the cyber security policy.	
3.1.4-2.a., 2.b., 2.c.1-6	2. The cyber security committee should be responsible for: a. monitoring, reviewing and communicating the Member Organization’s cyber security risk appetite periodically or upon a material change in the risk appetite; b. reviewing the cyber security strategy to ensure that it supports the Member Organization objectives; c. approving, communicating, supporting and monitoring: 1. the cyber security governance; 2. the cyber security strategy; 3. the cyber security policy; 4. cyber security programs (e.g., awareness program, data classification program, data privacy, data leakage prevention, key cyber security improvements); 5. cyber security risk management process; 6. the key risk indicators (KRIs) and key performance indicators (KPIs) for cyber security.	
3.1.4 - 4.a, 4.b, 4.c, 4.f, g.1., g.2, g.3,	4. The CISO should be responsible for: a. developing and maintaining: 1. cyber security strategy; 2. cyber security policy; 3. cyber security architecture; 4. cyber security risk management process; b. ensuring that detailed	

	security standards and procedures are established, approved and implemented; c. delivering risk-based cyber security solutions that address people, process and technology; f. conducting cyber security risk assessments on the Members Organization's information assets; g. proactively supporting other functions on cyber security, including: 1. performing information and system classifications; 2. determining cyber security requirements for important projects; 3. performing cyber security reviews.	
3.1.4.- e.1, e.2, e.3, e.4, e.5	4. The CISO should be responsible for: e. the cyber security activities across the Member Organization, including: 1. monitoring of the cyber security activities (SOC monitoring); 2. monitoring of compliance with cyber security regulations, policies, standards and procedures; 3. overseeing the investigation of cyber security incidents; 4. gathering and analyzing threat intelligence from internal and external sources; 5. performing cyber security reviews;	
3.1.4. -4.i.1., 4.i.2., 4.i.2, 4.i.4	4. The CISO should be responsible for: i. measuring and reporting the KRIs and KPIs on:	

	1. cyber security strategy; 2. cyber security policy compliance; 3. cyber security standards and procedures; 4. cyber security programs (e.g., awareness program, data classification program, key cyber security improvements).	
3.1.4-5.a	5. The internal audit function should be responsible for: a. performing cyber security audits.	

3.1.5 Cyber Security in Project Management

Principle

Cyber security should be addressed in project management and project governance.

Objective

To ensure that the all the Member Organization’s projects meet cyber security requirements.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.1.5-1	1. Cyber security should be integrated into the Member Organization's project management methodology to ensure that cyber security risks are identified and addressed as part of a project.	
3.1.5-2.a., 2.b, 2.c, 2.d., 2.e., 2.f.	2. The Member Organization’s project	

	management methodology should ensure that: a. cyber security objectives are included in project objectives; b. the cyber security function is part of all phases of the project; c. a risk assessment is performed at the start of the project to determine the cyber security risks and to ensure that cyber security requirements are addressed either by the existing cyber security controls (based on cyber security standards) or to be developed; d. cyber security risks are registered in the project-risk register and tracked; e. responsibilities for cyber security are defined and allocated; f. a cyber security review is performed by an independent internal or external party.	

3.1.6 Cyber Security Awareness

Principle

A cyber security awareness program should be defined and conducted for staff, third parties and customers of the Member Organization.

Objective

To create a cyber security risk-aware culture where the Member Organization’s staff, third parties and customers make effective risk-based decisions which protect the Member Organization’s information.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.1.6-6.A., 6.B.	6. The cyber security awareness program should be evaluated to: a. measure the effectiveness of the awareness activities; b. formulate recommendations to improve the cyber security awareness program.	

3.2.1 Cyber Security Risk Management

Principle

A cyber security risk management process should be defined, approved and implemented, and should be aligned with the Member Organization’s enterprise risk management process.

Objective

To ensure cyber security risks are properly managed to protect the confidentiality, integrity and availability of the Member Organization’s information assets, and to ensure the cyber security risk management process is aligned with the Member Organization’s enterprise risk management process.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.1-1	1. The cyber security risk management process should be defined, approved and implemented.	
3.2.1-2	2. The cyber security risk management process should focus on safeguarding the confidentiality, integrity and availability of information assets.	

3.2.1-3	3. The cyber security risk management process should be aligned with the existing enterprise risk management process.	

3.2.1-4.a., 4.b., 4.c., 4.d.	4. The cyber security risk management process should be documented and address:
	a. risk identification;
	b. risk analysis;
	c. risk response;
	d. risk monitoring and review.	

3.2.1.-5.a., 5.b., 5.c.	5. The cyber security risk management process should address the Member Organization's information assets, including (but not limited to):
	a. business processes;
	b. business applications;
	c. infrastructure components.	

3.2.1-6.a.,6.b.,6.c.,.6.d.	6. The cyber security risk management process should be initiated: a. at an early stage of the project; b. prior to critical change; c. when outsourcing is being considered; d. when launching new products and technologies.	
3.2.1-7	7. Existing information assets should be periodically subject to cyber security risk assessment based on their classification or risk profile.	

3.2.1-8.a.,8.b.,8.c.,8.d.	8. The cyber security risk management activities should involve:
	a. business owners;
	b. IT specialists;
	c. cyber security specialists;	

	d. key user representatives.	
3.2.1-9	9. The result of the risk assessment should be reported to the relevant business owner (i.e., risk owner) within the Member Organization;	
3.2.1-10	10. The relevant business owner (i.e., risk owner) within the Member Organization should accept and endorse the risk assessment results.	
3.2.1-11	11. The Member Organization's cyber security risk appetite and risk tolerance should be clearly defined and formally approved.	

3.2.1.1 Cyber Security Risk Identification

Principle

Cyber security risk identification should be performed and should include the Member Organization's relevant assets, threats, existing controls and vulnerabilities.

Objective

To find, recognize and describe the Member Organization's cyber security risks.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.1.1-1	1. Cyber security risk identification should be performed.	

3.2.1.1-2	2. Identified cyber security risks should be documented (in a central register).	
3.2.1.1-3	3. Cyber security risk identification should address relevant information assets, threats, vulnerabilities and the key existing cyber security controls.	

3.2.1.2 Cyber Security Risk Analysis

Principle

A cyber security risk analysis should be conducted based on the likelihood that the identified cyber security risks will occur and their resulting impact.

Objective

To analyze and determine the nature and the level of the identified cyber security risks.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.1.2--2	2. The cyber security risk analysis should address the level of potential business impact and likelihood of cyber security threat events materializing.	

3.2.1.3 Cyber Security Risk Response

Principle

The cyber security risks of a Member Organization should be treated.

Objective

To ensure cyber security risks are treated (i.e., accepted, avoided, transferred or mitigated).

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.1.3-1	1. The relevant determined cyber security risks should be treated according to the Member Organization's risk appetite and cyber security requirements.	
3.2.1.3-2	2. Cyber security risk response should ensure that the list of risk treatment options are documented (i.e., accepting, avoiding, transferring or mitigating risks by applying cyber security controls).	
3.2.1.3-3.a, 3.b.1, 3.b.2	3. Accepting cyber security risks should include: a. the consideration of predefined limits for levels of cyber security risk; b. the approval and sign-off by the business owner, ensuring that: 1. the accepted cyber security risk is within the risk appetite and is reported to the cyber security committee; 2. the accepted cyber security risk does not contradict SAMA regulations.	

3.2.1.3-4	4. Avoiding cyber security risks should involve a decision by a business owner to cancel or postpone a particular activity or project that introduces an unacceptable cyber security risk.	
3.2.1.3-5.a., 5.b., 5.c.	5. Transferring or sharing the cyber security risks should: a. involve sharing the cyber security risks with relevant (internal or external) providers; b. be accepted by the receiving (internal or external) provider(s); c. eventually lead to the actual transferring or sharing of the cyber security risk.	
3.2.1.3-6.a.,6.b.1., 6.b.2., 6.b.3., 6.c, 6.d.	6. Applying cyber security controls to mitigate cyber security risks should include: a. identifying appropriate cyber security controls; b. evaluating the strengths and weaknesses of the cyber security controls; 1. assessing the cost of implementing the cyber security controls; 2. assessing the feasibility of implementing the cyber security controls; 3. reviewing relevant compliance requirements for the cyber security controls; c. selecting cyber security controls; d. identifying, documenting and obtaining sign-off for any residual risk by the business owner.	
3.2.1.3-7	7. Cyber security risk	

	treatment actions should be documented in a risk treatment plan.	

3.2.1.4 Cyber Risk Monitoring and Review

Principle

The progress cyber security risk treatment should be monitored and the effectiveness of revised or newly implemented cyber security controls should be reviewed.

Objective

To ensure that the cyber security risk treatment is performed according to the treatment plans.
To ensure that the revised or newly implemented cyber security controls are effective.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.1.4-1.a., 1.b.	1. The cyber security treatment should be monitored, including: a. tracking progress in accordance to treatment plan; b. the selected and agreed cyber security controls are being implemented.	
3.2.1.4-2	2. The design and effectiveness of the revised or newly implemented cyber security controls should be reviewed.	

3.2.2 Regulatory Compliance

Principle

A process should be established by the Member Organization to identify, communicate and comply with the cyber security implications of relevant regulations.

Objective

To comply with regulations affecting cyber security of the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.2-1.a., 1.b., 1.c.	1. A process should be established for ensuring compliance with relevant regulatory requirements affecting cyber security across the Member Organization. The process of ensuring compliance should: a. be performed periodically or when new regulatory requirements become effective; b. involve representatives from key areas of the Member Organization; c. result in the update of cyber security policy, standards and procedures to accommodate any necessary changes (if applicable).	

3.2.3 Compliance with (inter)national industry standards

Principle

The Member Organization should comply with mandatory (inter)national industry standards.

Objective

To comply with mandatory (inter)national industry standards.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables

3.2.3-1.a.,1.b.,1.c.	1. The Member Organization should comply with:
	a. Payment Card Industry Data Security Standard (PCI-DSS);
	b. EMV (Europay, MasterCard and Visa) technical standard;
	c. SWIFT Customer Security Controls Framework – March 2017.	

3.2.4 Cyber Security Review

Principle

The cyber security status of the Member Organization’s information assets should be subject to periodic cyber security review.

Objective

To ascertain whether the cyber security controls are securely designed and implemented, and the effectiveness of these controls is being monitored.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.4-1	1. Cyber security reviews should be periodically performed for critical information assets.	
3.2.4-2	2. Customer and internet facing services should be subject to annual review and penetration tests.	
3.2.4-3	3. Details of cyber security review performed should be recorded, including the results of review, issues identified and recommended actions.	
3.2.4-4	4. The results of cyber security review should be reported to business owner.	
3.2.4-5	5. Cyber security review should be subject to follow-up reviews to check that: a. all identified issues have been addressed; b. critical risks have been treated effectively; c. all agreed actions are being managed on an ongoing basis.	

3.2.5 Cyber Security Audits

Principle

The cyber security status of the Member Organization’s information assets should be subject to thorough, independent and regular cyber security audits performed in accordance with generally accepted auditing standards and SAMA cyber security framework.

Objective

To ascertain with reasonable assurance whether the cyber security controls are securely designed and implemented, and whether the effectiveness of these controls is being monitored.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.2.5-1	1. Cyber security audits should be performed independently and according to generally accepted auditing standards and SAMA cyber security framework.	
3.2.5-2	2. Cyber security audits should be performed according to the Member Organization's audit manual and audit plan.	

3.3.1 Human Resources

Principle

The Member Organization should incorporate cyber security requirements into human resources processes.

Objective

To ensure that Member Organization staff's cyber security responsibilities are embedded in staff agreements and staff are being screened before and during their employment lifecycle.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables

3.3.1-3.a.,3.c.1,3.c.2.	3. The human resource process should include: a. cyber security responsibilities and non-disclosure clauses within staff agreements (during and after the employment); c. when disciplinary actions will be applicable; e. post-employment cyber security activities, such as: 1. revoking access rights; 2. returning information assets assigned (e.g., access badge, tokens, mobile devices, all electronic and physical information).	

3.3.3 Asset Management -

3.3.4 Cyber Security Architecture

Principle

The Member Organization should define, follow and review the cyber security architecture, which outlines the cyber security requirements in the enterprise architecture and addresses the design principles for developing cyber security capabilities.

Objective

To support the Member Organization in achieving a strategic, consistent, cost effective and end-to-end cyber security architecture.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.4-1	1. The cyber security architecture should be	

	defined, approved and implemented.	
3.3.4-2	2. The compliance with the cyber security architecture should be monitored.	
3.3.4-3.a.,3.b.,3.c.,3.d.,3.e.	3. The cyber security architecture should include: a. a strategic outline of cyber security capabilities and controls based on the business requirements; b. approval of the defined cyber security architecture; c. the requirement of having qualified cyber security architects; d. design principles for developing cyber security controls and applying cyber security requirements (i.e., the security-by-design principle); e. periodic review of the cyber security architecture.	

3.3.5 Identity and Access Management

Principle

The Member Organization should restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles.

Objective

To ensure that the Member Organization only provides authorized and sufficient access privileges to approved users.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.5-3	3. The effectiveness of the cyber security controls within the identity and access management policy should be measured and periodically evaluated.	

3.3.6 Application Security

Principle

The Member Organization should define, approve and implement cyber security standards for application systems. The compliance with these standards should be monitored and the effectiveness of these controls should be measured and periodically evaluated.

Objective

To ensure that sufficient cyber security controls are formally documented and implemented for all applications, and that the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.6-1	1. The application cyber security standards should be defined, approved and implemented.	
3.3.6-2	2. The compliance with the application security standards should be monitored.	
3.3.6-3	3. The effectiveness of the application cyber security controls should be measured and periodically evaluated.	

3.3.6-4	4. Application development should follow the approved secure system development life cycle methodology (SDLC).	
3.3.6-5.b.,5.d.,5.e.,5.g.	5. The application security standard should include: b. the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], identity and access management); d. the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage); e. vulnerability and patch management; g. periodic cyber security compliance review.	

3.3.7 Change Management

Principle

The Member Organization should define, approve and implement a change management process that controls all changes to information assets. The compliance with the process should be monitored and the effectiveness should be measured and periodically evaluated.

Objective

To ensure that all change in the information assets within the Member Organization follow a strict change control process.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.7-3	3. The effectiveness of the cyber security controls within the change management process should be measured and periodically evaluated.	
3.3.7-4.a.,4.c.,4.d.,4.f.,	4. The change management process should include: a. cyber security requirements for controlling changes to information assets, such as assessing the impact of requested changes, classification of changes and the review of changes; b. security testing, which should (if applicable) include: c. approval of changes by the business owner; d. approval from the cyber security function before submitting to Change Advisory Board (CAB); e. approval by CAB; f. post-implementation review of the related cyber security controls;	

3.3.8 Infrastructure Security

Principle

The Member Organization should define, approve and implement cyber security standards for their infrastructure components. The compliance with these standards should be monitored and the effectiveness should be measured and periodically evaluated.

Objective

To support that all cyber security controls within the infrastructure are formally documented and the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.8-1	1. The infrastructure security standards should be defined, approved and implemented.	
3.3.8-2	2. The compliance with the infrastructure security standards should be monitored.	
3.3.8-3	3. The effectiveness of the infrastructure cyber security controls should be measured and periodically evaluated.	
3.3.8-4	4. The infrastructure security standards should cover all instances of infrastructure available in the main datacenter(s), the disaster recovery data site(s) and office spaces.	
3.3.8-5	5. The infrastructure security standards should cover all instances of infrastructure (e.g., operating systems, servers, virtual machines, firewalls, network devices, IDS, IPS, wireless network, gateway servers, proxy servers, email gateways, external connections, databases, file-shares, workstations, laptops, tablets, mobile	

	devices, PBX).	
3.3.8-6.a,6.b.,6.c.,6.d.,6.e.,6.f.,6.g.,6.h1-5.,6.i.,6.j.	6. The infrastructure security standard should include: a. the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention [DLP], identity and access management, remote maintenance); b. the segregation of duties within the infrastructure component (supported with a documented authorization matrix); c. the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage); d. the use of approved software and secure protocols; e. segmentation of networks; f. malicious code/software and virus protection (and applying application whitelisting and APT protection); g. vulnerability and patch management; h. DDOS protection (where applicable); this should include: 1. the use of scrubbing services; 2. specification of the bandwidth agreed; 3. 24x7 monitoring by Security Operating Center (SOC), Service Provider (SP) and scrubbing	

	provider; 4. testing of DDOS scrubbing (minimum twice a year); 5. DDOS services should be implemented for the main datacenter(s) as well as the disaster recovery site(s); i. back-up and recovery procedures; j. periodic cyber security compliance review.	

3.3.9 Cryptography

Principle

The use of cryptographic solutions within the Member Organizations should be defined, approved and implemented.

Objective

To ensure that access to and integrity of sensitive information is protected and the originator of communication or transactions can be confirmed.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.9-1	1. A cryptographic security standard should be defined, approved and implemented.	
3.3.9-2	2. The compliance with the cryptographic security standard should be monitored.	
3.3.9-3	3. The effectiveness of the cryptographic security controls should be measured and periodically evaluated.	
3.3.9-4.a, 4.b.,4.c.	4. The cryptographic security	

	standard should include: a.an overview of the approved cryptographic solutions and relevant restrictions (e.g., technically, legally); B. the circumstances when the approved cryptographic solutions should be applied; C. the management of encryption keys, including lifecycle management, archiving and recovery.	

3.3.13 Electronic Banking Services

Principle

The Member Organization should define, approve, implement and monitor a cyber security standard for electronic banking services. The effectiveness of this standard should be measured and periodically evaluated.

Objective

To ensure the Member Organization safeguards the confidentiality and integrity of the customer information and transactions.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.13-1	1. The cyber security standards for electronic banking services should be defined, approved and implemented.	
3.3.13-2	2. The compliance with cyber security standards for electronic banking services should be monitored.	

3.3.13-3	3. The effectiveness of the cyber security standard for electronic banking services should be measured and periodically evaluated.	
3.3.13-4.b.5, 4.b.8	4. Electronic banking services security standard should cover: b. use of brand protection measures to protect online services including social media. online, mobile and phone banking: 5. use of communication techniques to avoid ‘man-in-the-middle’-attacks (applicable for online and mobile banking); 8. high availability of the electronic banking services should be ensured;	

3.3.14 Cyber Security Event Management

Principle

The Member Organization should define, approve and implement a security event management process to analyze operational and security loggings and respond to security events. The effectiveness of this process should be measured and periodically evaluated.

Objective

To ensure timely identification and response to anomalies or suspicious events within regard to information assets.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables

3.3.14-1	1. The security event management process should be defined, approved and implemented.	
3.3.14-2	2. The effectiveness of the cyber security controls within the security event management process should be measured and periodically evaluated.	
3.3.14-3.a	3. To support this process a security event monitoring standard should be defined, approved and implemented. a. the standard should address for all information assets the mandatory events which should be monitored, based on the classification or risk profile of the information asset.	
3.3.14-4.d.,4.e,4.f,4.h.,4.i,4.j., 4.k.,4.l.,	4. The security event management process should include requirements for: d. resources required continuous security event monitoring activities (24x7); e. detection and handling of malicious code and software; f. detection and handling of security or suspicious events and anomalies; h. adequately protected logs; i. periodic compliance monitoring of applications and infrastructure cyber security standards j. automated and centralized analysis of security loggings	

	and correlation of event or patterns (i.e., Security Information and Event Management (SIEM)); k. reporting of cyber security incidents; l. independent periodic testing of the effectiveness of the security operations center (e.g., red-teaming).	

3.3.15 Cyber Security Incident Management

Principle

The Member Organization should define, approve and implement a cyber security incident management that is aligned with the enterprise incident management process, to identify, respond to and recover from cyber security incidents. The effectiveness of this process should be measured and periodically evaluated.

Objective

To ensure timely identification and handling of cyber security incidents in order to reduce the (potential) business impact for the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.15-1	1. The cyber security incident management process should be defined, approved, implemented and aligned with the enterprise incident management process.	
3.3.15-2	2. The effectiveness of the cyber security controls within the cyber security incident management process should be measured and periodically evaluated.	

3.3.15-3	3. The standard should address the mandatory and suspicious security events which should be responded to.	
3.3.15-4.e.,4.f.,4.g,4.h.,4.i.,4.j.	4. The security incident management process should include requirements for: e. the classification of cyber security incidents; f. the timely handling of cyber security incidents, recording and monitoring progress; g. the protection of relevant evidence and loggings; h. post-incident activities, such as forensics, root-cause analysis of the incidents; i. reporting of suggested improvements to the CISO and the Committee; j. establish a cyber security incident repository.	
3.3.15-7.a.,7.b.,7.c.,7.d.,7.e., 7.g.,7.h.,7.i.	7. The Member Organization should submit a formal incident report 'SAMA IT Risk Supervision' after resuming operations, including the following incident details: a. title of incident; b. classification of the incident (medium or high); c. date and time of incident occurred; d. date and time of incident detected; e. information assets involved; g. root-cause analysis; h. corrective activities performed and planned; i. description of impact (e.g., loss of data, disruption of services, unauthorized modification of data,	

	(un)intended data leakage, number of customers impacted);	

3.3.16 Threat Management

Principle

The Member Organization should define, approve and implement a threat intelligence management process to identify, assess and understand threats to the Member Organization information assets, using multiple reliable sources. The effectiveness of this process should be measured and periodically evaluated.

Objective

To obtain an adequate understanding of the Member Organization's emerging threat posture.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.16-1	1. The threat intelligence management process should be defined, approved and implemented.	
3.3.16-2	2. The effectiveness of the threat intelligence management process should be measured and periodically evaluated.	
3.3.16-3a.,3.b.,3.c.,3.d.,3.e.,3.f.	3. The threat intelligence management process should include: a. the use of internal sources, such as access control, application and infrastructure logs, IDS, IPS, security tooling, Security Information and Event Monitoring (SIEM), support functions (e.g., Legal, Audit, IT Helpdesk,	

	Forensics, Fraud Management, Risk Management, Compliance); b. the use of reliable and relevant external sources, such as SAMA, government agencies, security forums, (security) vendors, security organizations and specialist notification services; c. a defined methodology to analyze the threat information periodically; d. the relevant details on identified or collected threats, such as modus operandi, actors, motivation and type of threats; e. the relevance of the derived intelligence and the action-ability for follow-up (for e.g., SOC, Risk Management); f. sharing the relevant intelligence with the relevant stakeholders (e.g., SAMA, BCIS members).	

3.3.17 Vulnerability Management

Principle

The Member Organization should define, approve and implement a vulnerability management process for the identification and mitigation of application and infrastructural vulnerabilities. The effectiveness of this process should be measured and the effectiveness should be periodically evaluated.

Objective

To ensure timely identification and effective mitigation of application and infrastructure vulnerabilities in order to reduce the likelihood and business impact for the Member Organization.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.3.17-1	1. The vulnerability management process should be defined, approved and implemented.	
3.3.17-2	2. The effectiveness of the vulnerability management process should be measured and periodically evaluated.	
3.3.17-3.a.,3.b.,3.c.,3.d.,3.d., 3.e.,3.f.	3. The vulnerability management process should include: a. all information assets; b. frequency of performing the vulnerability scan (risk-based); c. classification of vulnerabilities; d. defined timelines to mitigate (per classification); e. prioritization for classified information assets; f. patch management and method of deployment.	

3.4 Third Party Cyber Security

3.4.1 Contract and Vendor Management

Principle

The Member Organization should define, approve, implement and monitor the required cyber security controls within the contract and vendor management processes.

Objective

To ensure that the Member Organization’s approved cyber security requirements are appropriately addressed before signing the contract, and the compliance with the cyber security requirements is being monitored and evaluated during the contract life-cycle.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.4.1-1	1. The cyber security requirements should be defined, approved, implemented and communicated within the contract and vendor management processes.	
3.4.1-2	2. The compliance with contract and vendor management process should be monitored.	
3.4.1-3	3. The effectiveness of the cyber security controls within the contract and vendor management process should be measured and periodically evaluated.	
3.4.1-4.a.,4.b.,4.c.	4. These contract and vendor management processes should cover: a. whether the involvement of the cyber security function is actively required (e.g., in case of due diligence); b. the baseline cyber security requirements which should be applied in all cases; c. the right to periodically perform cyber security reviews and audits.	
3.4.1-5.a.,5.b.,5.c.,5.d.,5.e.,5.f.,5.g.	5. The contract management process should cover	

	requirements for: a. executing a cyber security risk assessment as part of the procurement process; b. defining the specific cyber security requirements as part of the tender process; c. evaluating the replies of potential vendors on the defined cyber security requirements; d. testing of the agreed cyber security requirements (risk-based); e. defining the communication or escalation process in case of cyber security incidents; f. ensuring cyber security requirements are defined for exiting, terminating or renewing the contract (including escrow agreements if applicable); g. defining a mutual confidentiality agreement.	
3.4.1-6.a.	6. The vendor management process (i.e., service level management) should cover requirements for: a. periodic reporting, reviewing and evaluating the contractually agreed cyber security requirements (in SLAs).	

3.4.2 Outsourcing

Principle

The Member Organization should define, implement and monitor the required cyber security controls within outsourcing policy and outsourcing process. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.

Objective

To ensure that the Member Organization's cyber security requirements are appropriately addressed before, during and while exiting outsourcing contracts.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
	1. The cyber security requirements within the outsourcing policy and process should be defined, approved, implemented and communicated within Member Organization.	
	2. The cyber security requirements regarding the outsourcing policy and process should be measured and periodically evaluated.	
	3. The outsourcing process should include: a. the approval from SAMA prior to material outsourcing; b. the involvement of the cyber security function; c. compliance with the SAMA circular on outsourcing. *The SAMA Outsourcing circular notes specifically: Principle 6:	

	Consumers’ financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties).	

3.4.3 Cloud Computing

Principle

The Member Organization should define, implement and monitor the required cyber security controls within the cloud computing policy and process for hybrid and public cloud services. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.
Please note that this requirement is not applicable to private cloud services (= internal cloud).

Objective

To ensure that all functions and staff within the Member Organization are aware of the agreed direction and position on hybrid and public cloud services, the required process to apply for hybrid and public cloud services, the risk appetite on hybrid and public cloud services and the specific cyber security requirements for hybrid and public cloud services.

SAMA CSF Control Consideration	SAMA CSF Language	Company Enables
3.4.3-1	1. The cyber security controls within the cloud computing policy for hybrid and public cloud services should be defined, approved and	

	implemented and communicated within Member Organization.	
3.4.3-2	2. The compliance with the cloud computing policy should be monitored.	
3.4.3-3	3. The cyber security controls regarding the cloud computing policy and process for hybrid and public cloud services should be periodically measured and evaluated.	
3.4.3-4.a.1.,4.a.2.,4.a.3.,4.b.,4.d.1.,4.g.1.,4.g.2.,4.g.3.,4.h.1.	4. The cloud computing policy for hybrid and public cloud services should address requirements for: a. the process for adopting cloud services, including that: 1. a cyber security risk assessment and due diligence on the cloud service provider and its cloud services should be performed; 2. the Member Organization should obtain SAMA approval prior to using cloud services or signing the contract with the cloud provider; 3. a contract should be in place, including the cyber security requirements, before using cloud services; b. data location, including that: d. security, including that: 1. the cloud service provider should implement and monitor the cyber security controls as determined in the risk assessment for protecting the confidentiality, integrity and	

	availability of the Member Organization’s data; g. audit, review and monitoring, including that: 1. the Member Organization has the right to perform a cyber security review at the cloud service provider; 2. the Member Organization has the right to perform a cyber security audit at the cloud service provider; 3. the Member Organization has the right to perform a cyber security examination at the cloud service provider; h. exit, including that: 1. the Member Organization has termination rights;	