Deloitte.

Saudi Central Bank (SAMA)

Third-Party Framework

October 2023

SAMA's draft third-party framework on baseline requirements for third-party/outsourcing arrangements

In order to ensure effective & responsive risk management, SAMA has proposed draft baseline requirements on third-party/outsourcing arrangement

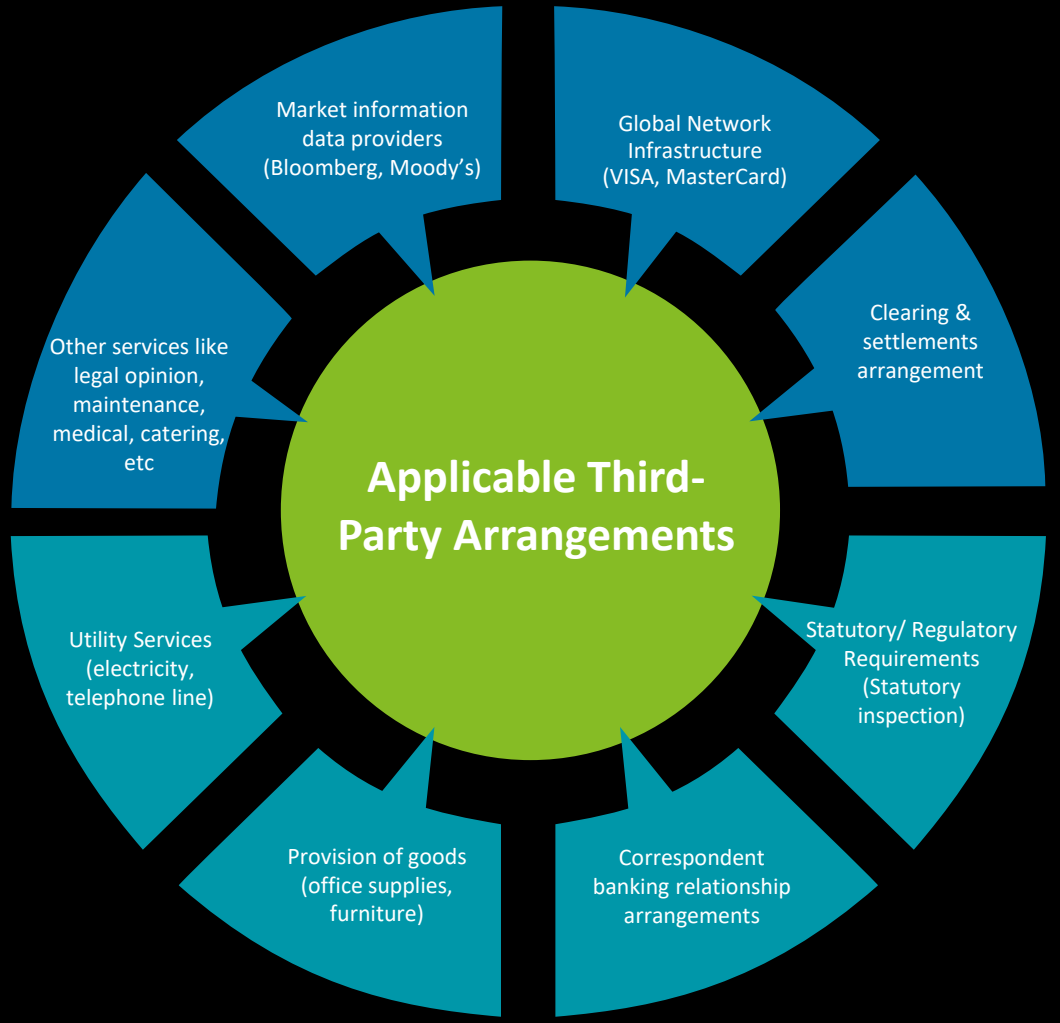
Applicable entities

Any regulated entity supervised by SAMA, including but not limited to Banks, Insurance companies, Finance Companies, FinTech, Aggregators, Payment Service Providers (PSPs), Financial Market Infrastructures (FMIs).

Foreign branches & subsidiaries operating in Saudi Arabia
(Not applicable if outsourcing to their head office)

Responsibility of Financial Institutions

- Compliance and Reporting
- Governance
- Risk Assessments throughout third-party lifecycle
- Continuous risk based third-party management



Summarized view of SAMA's draft third-party framework

The framework is intended to mitigate most common risks FIs may identify when entering in any arrangements with a third-party. It also includes set of principles and requirements to be used as a baseline by all FIs and its subsidiaries.

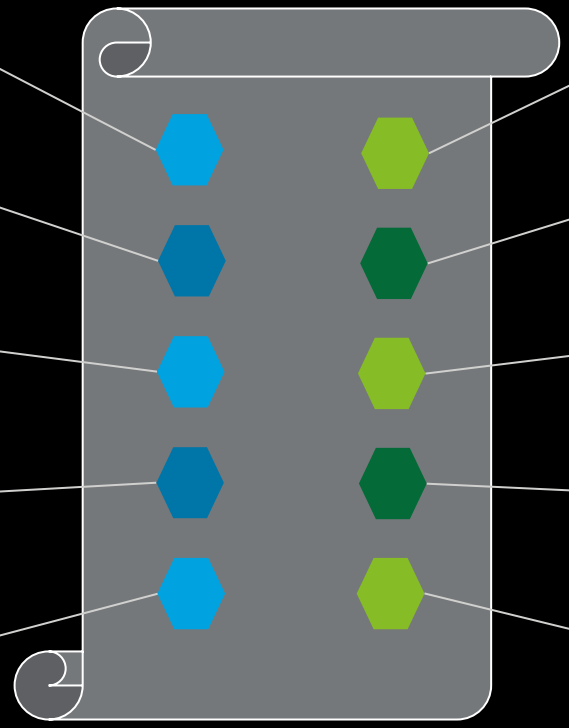
Third Party Risk Management **Policy and Framework**

Perform third party **Materiality Assessment, Risk Assessments** across risk domains and **Due Diligence**

Approval from SAMA for **Material Outsourcing**

Compliance to **Regulatory and Legal requirements** at the time of outsourcing

Notify SAMA in case of **Breach of Legal/ Regulatory** requirements



Clearly defined **Roles & Responsibilities** of BoD and/ or its delegated authority

Establish **Governance Mechanism** for third party risk management

Establish **Legally Binding Contract** including provisions around sub-contracting of services

Establish **Termination Process** for third-party arrangements

Establish process around **Continuous Monitoring** of third party arrangements

Risk domains addressed in the Framework

- **Cyber Security**
- **Resilience**
- **Legal & Regulatory**
- **Reputational**
- **Privacy**
- **Concentration**
- **Financial & Operational**
- **Anti-Money Laundering**

Third Party Framework Principles and requirements to be used as baseline by all FIs/subsidiaries

SAMA's draft third-party framework consists of three domains (i.e., Governance, third-party arrangement lifecycle and ongoing third-party management)

Third Party Framework

Governance

The domain emphasizes the importance of implementing effective controls within a financial institution concerning third-party relationships and outsourcing. The FI's governance model should establish a comprehensive approach to managing these third-party arrangements. This involves incorporating strong practices for governance, documentation, and reporting to gain a complete understanding of its third-party arrangements, enabling informed risk management decisions and the proper implementation of risk mitigation measures.

Following are the controls under this domain, which FIs needs to implement:

- Proportionality
- Sound Governance
- Intragroup Arrangement
- Business Continuity
- Third-Party Arrangement Register

Third Party Arrangement Lifecycle

The domain outlines the controls that FIs should implement throughout the lifecycle management process of third-party arrangements. Before entering into any arrangements and periodically thereafter, FIs should implement the risk controls associated with using a third-party (such as cyber, technology, privacy, resilience, concentration, financial, operational, legal, regulatory, and reputational risks), and perform due diligence on the third-party. Additionally, when the third-party provides a critical service for the financial institution, a risk assessment should be conducted on the critical asset underlying the service, considering specific requirements set by SAMA.

Following are the controls under this domain, which FIs needs to implement:

- Assessment of Materiality
- Risk Assessment
- Due Diligence
- Contractual Phase
- Sub-Contracting
- Termination

Ongoing Third-Party Management

The domain highlights the importance of implementing relevant processes and controls at different stages of the third-party lifecycle within FIs. These controls are designed to manage the risks associated with third-party arrangements effectively. The framework emphasizes the significance of second level controls and independent reviews to ensure that potential risks related to third-party engagements are adequately mitigated. Monitoring based on key risk indicators and comprehensive reporting are essential components of the process to gain a holistic view of third-party risk. Periodic independent reviews of the process are also necessary to maintain its effectiveness.

Following are the controls under this domain, which FIs needs to implement:

- Continuous monitoring and reporting
- Independent Review

Principles and requirements to be used as baseline by all FIs/subsidiaries

SAMA's draft third-party framework consists of three domains (i.e., Governance, third-party arrangement lifecycle and ongoing third-party management)

1. Governance

Proportionality

***FIs to implement & perform proportionate evaluation for all third-party arrangements considering:**

- Nature of customer data
- Third-party experience and risk profile
- Cost & complexity of arrangement
- Affiliation between third-party and financial institution
- Financial, operational, regulatory & reputational impact in case of third-party failure
- Potential losses to FIs customers/affected parties

***Determine resource/activity for third-party or outsourcing arrangement based on above outcome**

***Annually (at least) evaluate governance & implementation**

Sound Governance

***FIs to clearly define nontransferable roles & responsibilities w.r.t third-party arrangement to ensure:**

- Board of Directors has ultimate responsibility to approve & implement strategies
- Third-party policy is reviewed & updated periodically
- Third-party policy must include at minimum, defined components as per SAMA third-party framework
- Conflict of interest check covering:
  - Financial interest
  - Responsibilities
- Classification of third-party relationship
- Benchmarking of third-Party policy & integrate into internal polices

Intragroup Arrangement

***For third-party arrangement, governance over intragroup arrangements shall be established & cover the following:**

- Conflict of interest check
- Governance structure and allocation of Board of Directors
- Financial interest, dependency, control and influence
- Group wide internal policies and procedures
- Risk identification and mitigation strategy
- Compliance with respect to intragroup entity
- FIs participation in third-party policy making process

***For outsourcing arrangement only, cover the following:**

- Compliance with regulatory framework
- Identity risks & mitigation measures
- Higher level of control

Business Continuity

***FIs must establish business continuity plans for outsourcing arrangement prior Board of Directors approval, in conjunction with Business Continuity Management Framework & document the following:**

- Possible event of failures
- Alternate third-party service providers & in-house transition plans
- Timeline & procedure to select alternate third-party
- Service Level Agreements
- Transition plans for another third-party for new arrangement
- Recovery time objective, recovery point objective & resumption of operations

Third-Party Arrangement Register

***FIs must document all third-party arrangements in dedicated repository**
***FIs to perform annual review of the register**
***FIs to update the register for critical third-parties periodically & share with SAMA annually**
***FIs to update the register for non-critical third-parties annually**
***The register must include:**

- Reference number for arrangement
- Description of the function
- Classification of arrangement
- Materiality assessment & Past assessment outcome
- Severity of third-party
- Severity of the service
- Risk assessment outcome
- Geographical location of third-part and sub-contractor, if involved

Principles and requirements to be used as baseline by all FIs/subsidiaries for material outsourcing

SAMA's draft third-party framework consists of three domains (i.e., Governance, third-party arrangement lifecycle and ongoing third-party management)

2. Third-Party Arrangement Lifecycle (1/2)

Assessment of Materiality

***FIs to classify outsourced function as material', if disruption affects the following:**

- Financial stability of Saudi Arabia's financial sector
- Operational resilience and reputation
- Compliance with regulations
- Profitability of customers and affected parties
- Protection and CIA of customer data

***FIs must perform materiality assessment prior to entering in an outsourcing arrangement considering:**

- Pre-defined annual monitoring plan is in place
- Change in the nature of the arrangement/parties

Risk Assessment

***FIs must perform risk assessment to identity potential risk from third-party arrangement & determine mitigation measure**

***Risk assessment requirements for all third-party arrangement:**

- Identify potential cyber, security, privacy, resilience, & concentrations risk etc. & assess their impact on FI's risk profile
- Evaluate risk assessment result as following:
    - Prior to entering a third-party arrangement
    - Pre-defined annual assessment
    - Change in the nature of the arrangement/parties

Implement risk mitigation by considering the following, but not limited to:

- Contractual agreement with other third-party
- Shorter duration of contractual agreement
- BCP and incident management plan

***Risk assessment requirements for all outsourcing arrangement only, addition to above requirements:**

- Potential risks such as operational, regulatory etc.
- Concentration risks – Level of dependency or multiple contracts
- Risk mitigation plans
- Location, political stability, intragroup connection, data and security measures, sub-contractor arrangement
- Scenario analysis and document the same in third-party register

Due Diligence

***FIs must perform due diligence before entering third-party arrangement as per risk appetite**

***Due diligence for all third-party & outsourcing arrangements must consider the following but not limited to:**

- Level of due diligence required as per arrangement/materiality of the function
- Business model, nature, complexity, ownership
- Financial position
- Expertise & reputation
- Operational & technology resources
- Governance, incident management, BCP
- Data Privacy
- Security & Quality
- Sub-contractor security control

Principles and requirements to be used as baseline by all FIs/subsidiaries for material outsourcing

SAMA's draft third-party framework consists of three domains (i.e., Governance, third-party arrangement lifecycle and ongoing third-party management)

2. Third-Party Arrangement Lifecycle (2/2)

Contractual Phase

***FIs must establish expectations in agreed & written legally binding contract to set clear expectations, roles, responsibilities.**

***Contractual requirement for all third-party arrangement:**

- Cover relevant laws & regulations
- Obligations
- Knowledge transfer process
- NDA provisions such as:
  - Confidential information definition
  - Use of confidentialinformation
  - Duration of agreement (reviewed at least annually)

***Contractual requirement for outsourcing arrangement:**

- Policy defining SLA program
- SLA monitoring process
- Escalation process
- Non-performance & resolution process
- Right of SAMA to access the subcontractor in the same capacity
- To include provisions regarding:
  - CIA
  - Data privacy and security of data
  - Sub-contractor security
  - NDA provisions similar to third-party arrangement

Sub-Contracting

***FIs must consider supply chain risks if third-party transfers performance of activities to an additional third-party service provider**

***Sub-contracting requirement for all third-party arrangement:**

- To be onboard only if no undue operational or other risks
- Identify potential risks from sub-contractor through risk assessment & due diligence activities
- To obtain list of all sub-contracting service providers from third-party
- Ownership is with third-party even if sub-contractor is involved
- Concentration risk (E.g., level of dependency)

***Sub-contracting requirement for outsourcing arrangement:**

- Prior approval of FI before sub-contracting
- Ensure third-party has performance reporting & monitoring for sub-contractor
- SAMA approval for 'material' sub-contractor activities
- Sub-contractor consent to cooperate with SAMA

Termination

***FIs must establish termination processes, including exit strategies and rights of the parties stated in the agreed contract**

***Termination requirement for all third-party arrangement:**

FIs to ensure that contract can be terminated in accordance with applicable law and regulations, including in the following situations:

- In case of any legal & regulatory breach
- Non-performance
- Material changes
- Identification security weakness,
- SAMA instruction

***Termination requirement for outsourcing arrangement:**

FIs to ensure that contract includes provisions regarding:

Support during transfer

- Transition period
- Audit and access rights
- Return and disposal of data

Principles and requirements to be used as baseline by all FIs/subsidiaries for material outsourcing

SAMA's draft third-party framework consists of three domains (i.e., Governance, third-party arrangement lifecycle and ongoing third-party management)

3. Ongoing third-party management

Continuous monitoring and reporting

***Financial institutions must establish a risk-based continuous monitoring process & timely report the outcome to Board of Directors**

***Monitoring process for third-party to be established considering at minimum:**

- Third-party risk raised during risk assessment
- Contract/SLA performance
- Third-party risk profile
- Quarterly performance monitoring using risk indicators, ongoing reports from third-party, information collected during inspection, certifications and independent reviews
- Reporting to Board of Directors periodically covering:
    - Risk analysis outcome & mitigation implemented
    - Independent review outcome
    - Periodic risk assessment to manage changes in risk exposure
    - Annual monitoring of concentrated risk

Independent Review

***FIs internal audit functions/external auditor must inspect third-party arrangement & third-party annually to provide information to SAMA and ensure adherence to the requirements set out in the framework**

***Independent review requirements for all third-party arrangements:**

- Periodic independent review of functions
- Compliance to third-party policy & implementation of third-party policy & ensure :
    - Involvement of governance and management bodies
    - Risk assessment reliability
    - Legal and regulatory compliance

***Independent review requirements for outsourcing arrangements:**
Inspection to be performed by internal function/external auditor/SAMA agent covering internal control framework, BCP, storage and processing of data as per regulatory requirements in addition to third-party arrangement requirements

Requirements for Foreign Branches

- Book business in Saudi Arabia unless SAMA otherwise agrees
- Hire local staff to demonstrate local control & compliance to SAMA
- Decision making, AML/Combatting Financing of Terrorism functions not to be outsourced, head office/related party functions if outsourced shall be audited & share findings with SAMA
- Establish comprehensive risk management practice & ensure record keeping
- Policy shall be designed to define SLA, data sharing consent, access,
- To outsource to an affiliate, submit letter of comfort to SAMA

Steps to comply with SAMA's Third Party Framework

Framework

Customized TPRM framework to operationalize third party risk management in line with regulatory requirements and industry leading practices

Training & Awareness

Training & awareness programs for clients and their third parties

Performance monitoring

Third party onboarding/ performance monitoring (SLA/ KPI compliance)

Risk profiling

Risk profiling of third parties across departments to identify critical third parties across risk domains

Risk assessments

Risk assessments across risk domains such as cyber security, privacy, resilience, concentration, legal & regulatory, financial & operational, reputational, anti-money laundering, etc.

Contract Management

Review/ manage contract for different third parties to ensure they are aligned with the SAMA guidelines

Managed Services

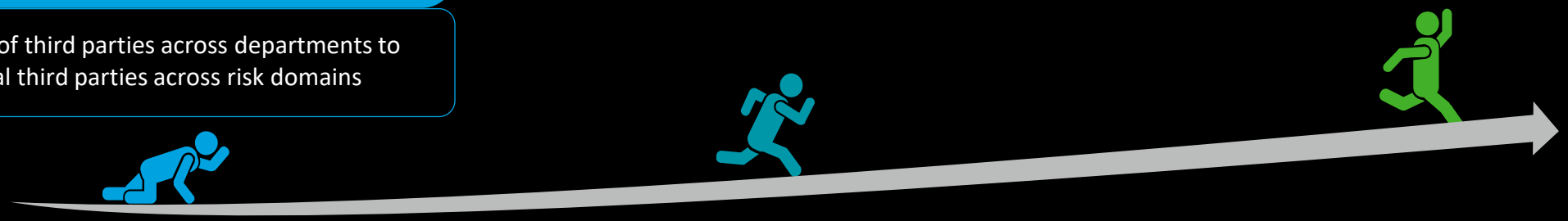
Third party risk profiling, onboarding and periodic assessments, performance monitoring across applicable risk domains

Automation

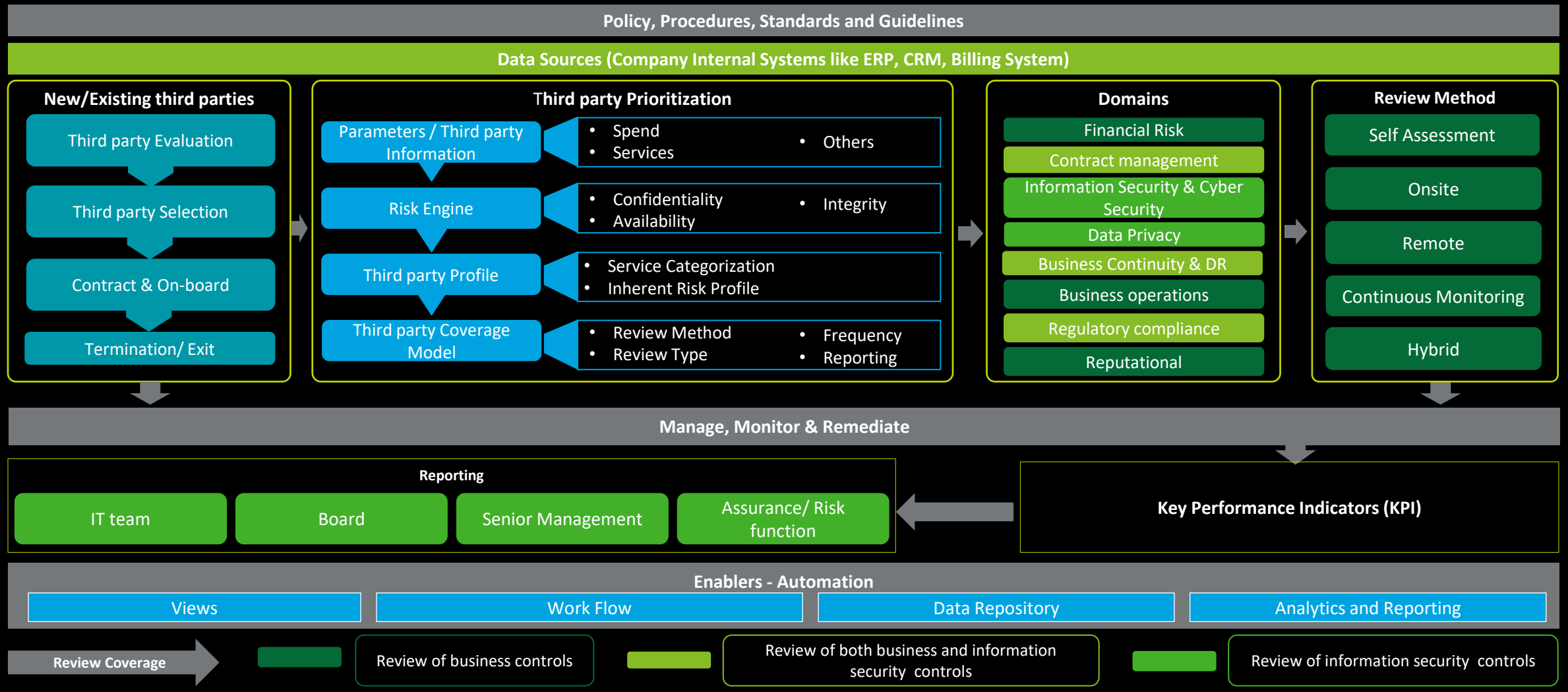
- "TRYGNA" Deloitte's Third-party risk management and monitoring tool
- Risk sensing and continuous monitoring

Remediation

Post assessment follow ups for remediation along with remediation tracking mechanism



Third Party Risk Management (TPRM) Framework in line with SAMA's Third Party Framework



Deloitte's Capability - Overview of Deloitte's Vendor Intelligence Center (VIC)

10,000+ assessments delivered to clients. We have a pool of risk management professionals who can address multiple domains of TPRM

DOMAIN COVERAGE

- Cyber/Information Security
- Data Privacy
- Contract Management
- Sub-contracting / 4th Party
- Regulatory Compliance
- Operational / SLA Performance
- ESG
- Health and Safety
- Reputation
- Financial Viability

HEADCOUNT

300+ professionals

SERVICE PORTFOLIO

- Framework design
- Program management
- Third-party risk assessments
- Third-party profiling
- TPM GRC tools implementation
- Transformation and enhancements
- Risk sensing and monitoring

DELIVERY CENTERS

- India
- Middle East

CAPABILITY

End to end Third-Party Lifecycle

- Plan, evaluate and select
- Contract & on-board
- Manage & monitor
- Discontinue & de-board

DELIVERY MODELS

- **Remote**
- **Onsite**
- **Hybrid**

TECHNOLOGY

1. GRC-TPM solutions

Service now, One Trust, Coupa Risk etc

- Design, Implement, Operate

2. Inhouse TPRM Tool

Trygna

• Scalable • Flexible • Secure

- Designed for Managed Service
- Cloud ready
- Access anytime on any device

Frequently Asked Questions (FAQ's)

1

Who is covered under SAMA's third-party framework?

- Any regulated entity supervised by SAMA, including but not limited to Banks, Insurance companies, Finance Companies, FinTech, Aggregators, Payment Service Providers (PSPs), Financial Market Infrastructures (FMIs).
- Foreign branches & subsidiaries operating in Saudi Arabia *(Not applicable if outsourcing to their head office)*

What are the key third-party arrangements applicable to SAMA framework?

- Global network infrastructure, clearing & settlement arrangement, statutory / regulatory requirements, corresponding banking relationships
- Provision of goods, utility services, market information data providers, legal opinion, maintenance services, medical services, catering services etc.

2

3

What are the key domains to be covered under SAMA Framework?

- Cyber Security
- Data Privacy
- Legal & Regulatory
- Resilience
- Financial & Operations
- Anti-money Laundering
- Reputational
- Concentration, etc.

What is 'Materiality Assessment' & 'Material Outsourcing' ?

- **Materiality Assessment :** Evaluation of the service provided by vendor to determine the significance & impact on organization's operations, goals, reputation & identify potential risks
- **Material Outsourcing :** Outsourcing of significant or critical business functions, services or processes to external vendor

4

Frequently Asked Questions (FAQ's)

5

What is the difference between Saudi or foreign branch & Saudi legal entity?

- **Saudi or foreign branch** is an extension of foreign company's operations in Saudi Arabia, that shall be subject to regulations of both the parent company's home country & Saudi Arabia (SAMA)
- **Saudi legal entity** is a separate & independent company registered under Saudi Arabia laws & will be governed by SAMA guidelines

Are there any special requirements for the foreign branches?

- Book business in Saudi Arabia and hire local staff to demonstrate local control & compliance to SAMA
- Decision making, AML/Combatting Financing of Terrorism functions not to be outsourced, head office/related party functions if outsourced shall be audited & share findings with SAMA
- Establish comprehensive risk management practice & ensure record keeping

6

7

Is it mandatory to seek SAMA approval prior to onboarding the outsourcing service provider?

- Different type of services might have varying regulatory requirements. We need to identify whether the planned service falls under SAMA's jurisdiction
- Access potential risks associated with outsourcing without SAMA approval
- Engage external consultants / industry experts / legal counsel to review & advise on the outsourcing plans

What are the key phases in a third-party risk assessment lifecycle?

- Assessment of Materiality
- Risk Assessment
- Due-diligence
- Contracting and Sub-contracting
- Continuous monitoring and reporting
- Termination

8