XV REUNIÓN DE AUDITORES INTERNOS
DE BANCOS CENTRALES

“Perspectivas sobre tendencias, desafíos y temas de actualidad de la auditoria interna”

BANCO CENTRAL DE CHILE, SANTIAGO, CHILE

SEPTIEMBRE 25 - 27, 2019

BANK FOR INTERNATIONAL SETTLEMENTS

Perspective on Trends, Challenges and Hot Topics of Internal Audit

The views expressed in this presentation are those of the presenter and not necessarily those of the BIS.

Overview

- What is the CBIA?
- Some recent topics of focus:
  - SWIFT Customer Security Program (CSP) Compliance
  - Cyber Resilience
  - Three Lines of Defense
  - Outsourcing Risks

What is the Central Bank Internal Auditors?

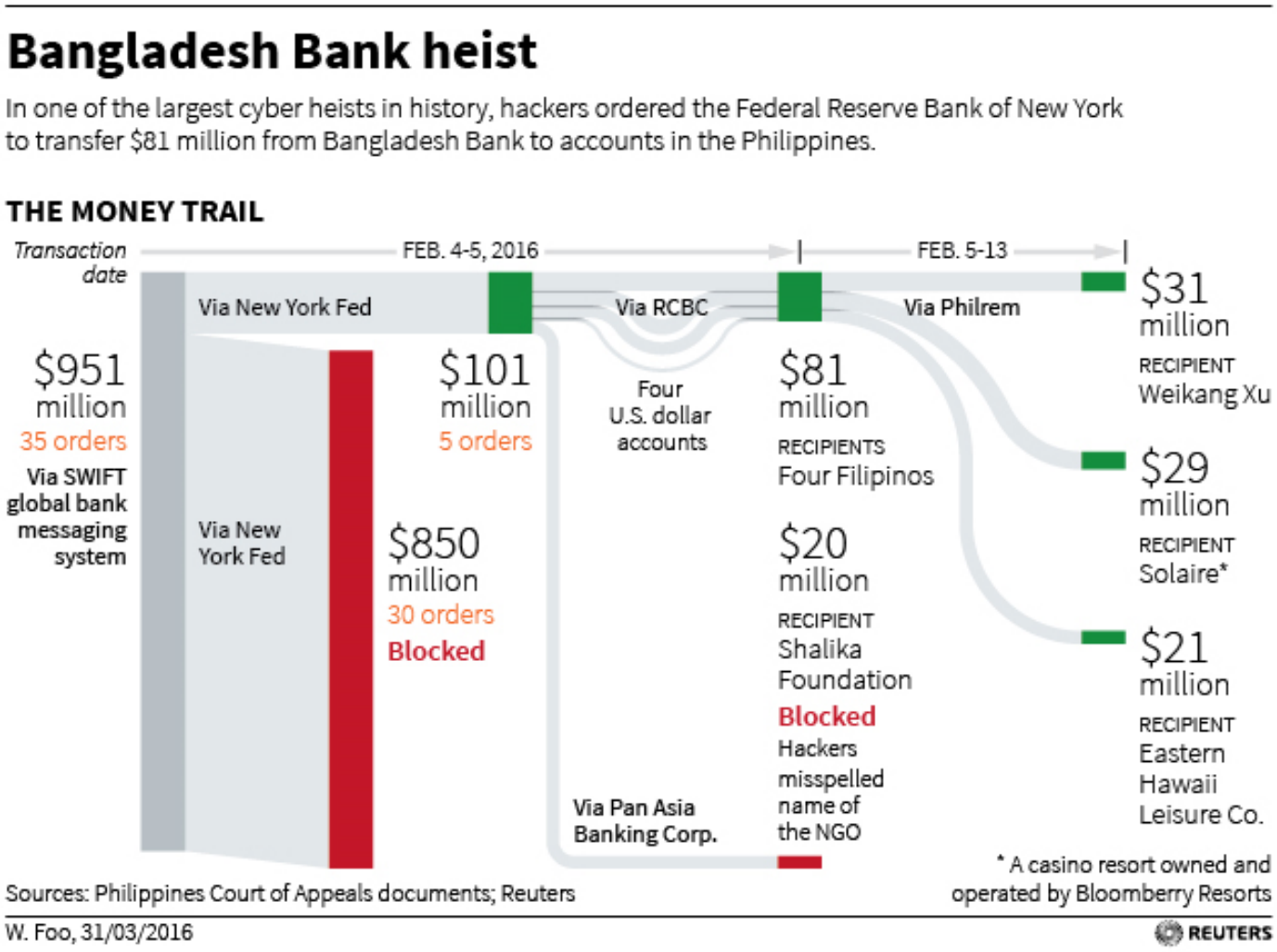
- Heads or Deputy Heads of Internal Audit
- Composition reflects the BIS Economic Consultative Committee
- Mandate
  - share and foster best practice for internal audit within central banks;
  - contribute to discussions on issues related to corporate governance, risk management, control and compliance in central banks, as appropriate;
  - identify, research and report on emerging risks; and additionally analyse key trends affecting internal auditing in central banks;
  - provide input to relevant BIS based groups and/or committees; and
  - contribute to the advancement and development of internal auditing in the financial sector.

BANK FOR INTERNATIONAL SETTLEMENTS

Recent Topics of Focus

SWIFT CSP Compliance

Thefts via SWIFT or other financial messaging / payment systems



SWIFT CSP Compliance

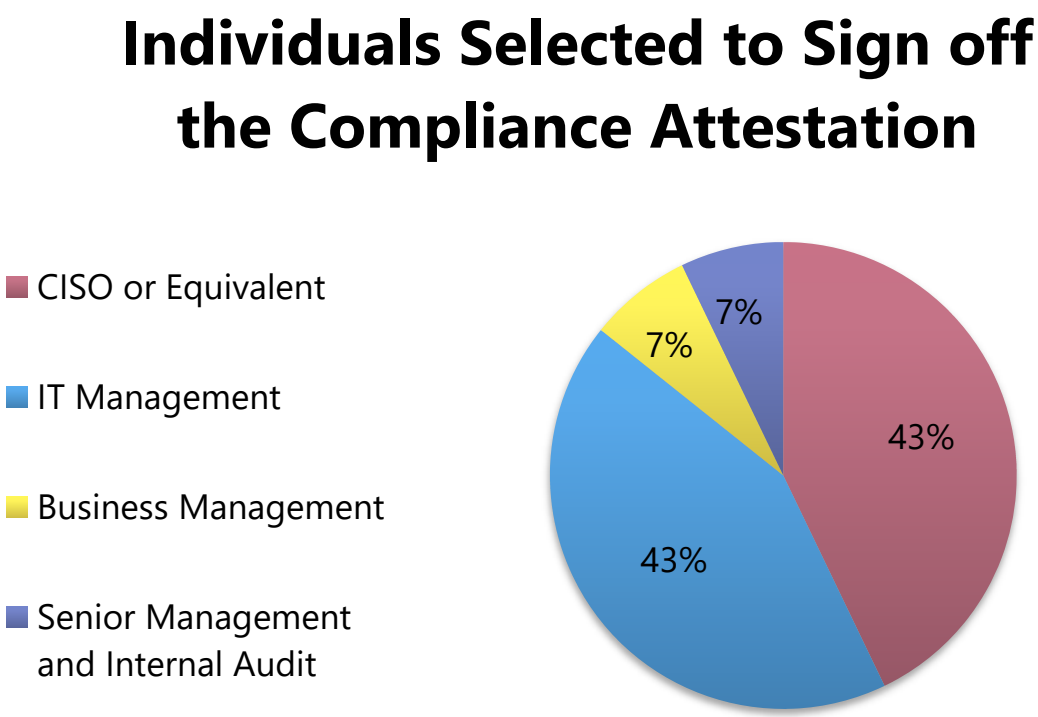
The Controls Framework

SWIFT Customer Security Controls Framework		
Secure Your Environment	1.	Restrict Internet access
	2.	Protect critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

Source: Swift.com

SWIFT CSP Compliance

Individuals Signing off the Attestation - 2017

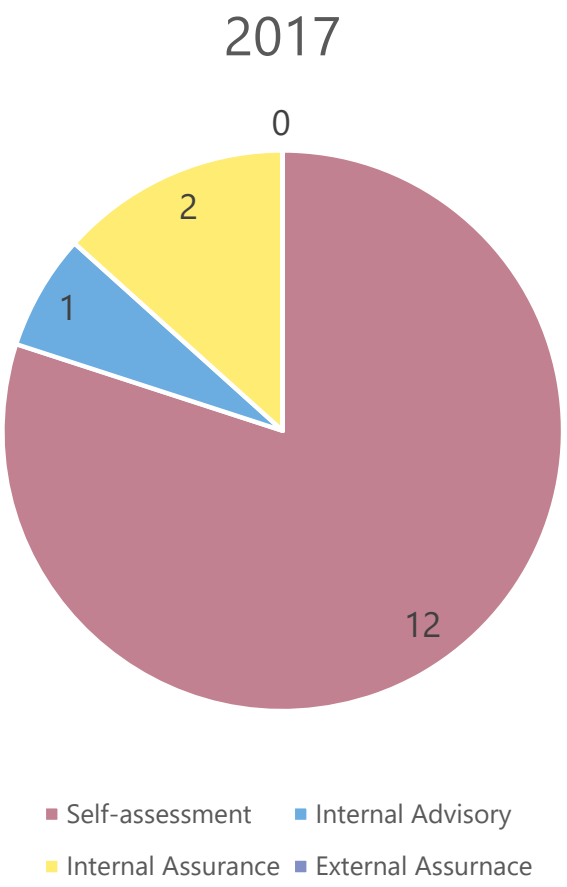


- In all respondent institutions, the Board (or at least some members or other top managers) have been kept informed of the process and/or content of the attestation.
- All attestations have been submitted in 4-eyes in the KYC application. More frequently by IT people, but also by business people.

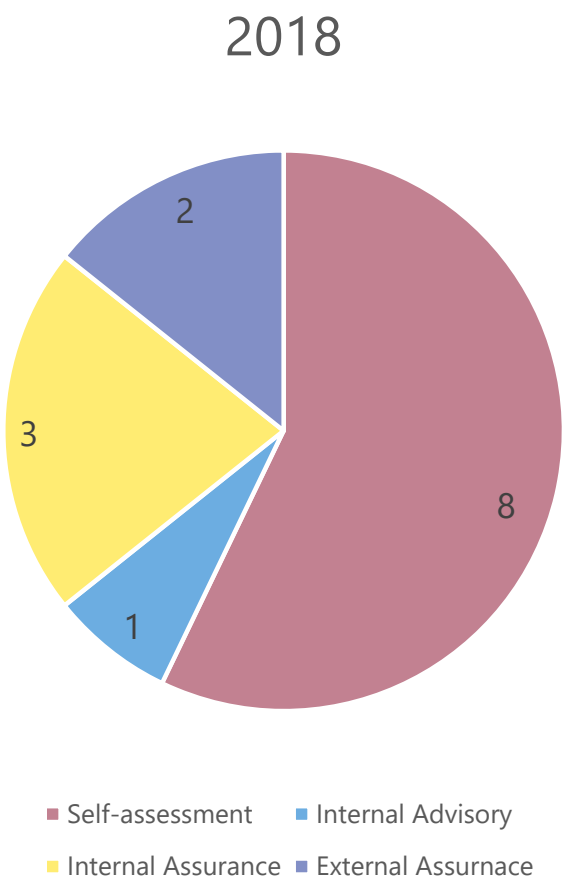
Source: CBIA: 2018, Implementing the SWIFT Customer Security Program

SWIFT CSP Compliance

Central Bank Assessment Types



Source: CBIA: 2018, Implementing the SWIFT Customer Security Program



Source: CBIA: 2019 Survey

SWIFT CSP Compliance

CBIA Main Takeaways and Conclusions - 2017

CSP security controls implementation

- Variety of methods to achieve CSP control objectives
- Mandatory controls reported largely in compliance
- Advisory controls were less compliant than mandatory
- Projects were mainly limited to the local SWIFT infrastructure to achieve compliance

CSP compliance assessment

- Mainly self-assessments, different degrees of evidence gathered
- For 2018 and future: more internal/external audit involvement anticipated

CSP compliance attestation

- Mainly signed-off by CISO and IT mgmt.
- Slow take-up of compliance attestation exchanges with business counterparties

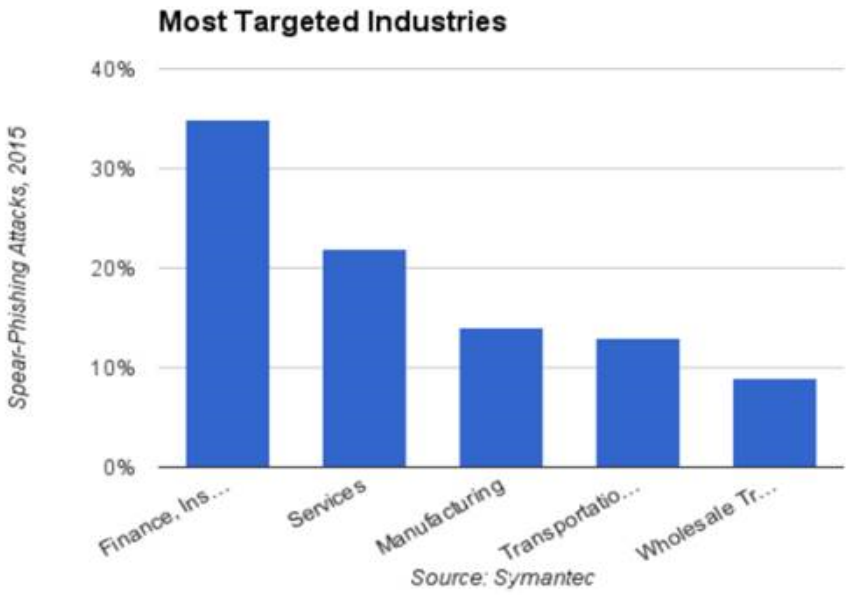
<u>Conclusions</u>

- SWIFT CSP open to interpretation & judgement, limited consistency between CBIA member Banks
- CSP seen as leverage to enhance security of the payment systems

Source: CBIA: 2018, Implementing the SWIFT Customer Security Program

Cyber Resilience

Cyber security threats are more acute in the world's financial system



Payment execution risks within Central Banks

- Insider threat issues
- Social engineering
- Malware
- Targeted attacks
- Ransomware
- Spear phishing

Source: CBIA: 2017, Cyber Risk

Cyber Resilience

Current state of information security risk management in central banks

1. Practices among central banks are diverse
2. Only a few central banks take a holistic view on information security risk management
   - the technical angle of approaching the subject is still very dominant
   - culture and awareness are underestimated as root causes for control failures
3. IT-based audit techniques are scarcely used by auditors
4. Information security breaches can have a significant impact on central banks' information integrity, business continuity, financials and reputation. It deserves to be more frequent on the agenda of management boards, audit committees and supervisory boards

Source: CBIA: 2019, Auditing Information Security Risk Management

Cyber Resilience

Detailed recommendations regarding information security risk management in central banks

1. Depending on 3 LoD maturity, continuous auditing approaches should be considered. Using IT-based audit techniques and liaising with the bank's security operations centres
2. Information security risks should more frequently be in the scope of operational audits, not simply IT audits
3. Internal Audit functions should assess their capabilities on the subject and consider hiring experts in cases of deficiencies
4. Internal Audit functions should use standards that are as close as possible to the standards used by the 1st and 2nd line control functions (NIST, SANS Top 20 Critical Security Controls)
5. Customizations to global standards are possible but should not hamper benchmarking exercises

Source: CBIA: 2019, Auditing Information Security Risk Management

Cyber Resilience

Detailed recommendations regarding information security risk management in central banks

6. Internal Audit functions should invest in an ongoing dialogue with governance bodies on the subject of information security risk management, audit outcomes and audit recommendations follow-up
7. Internal audits should focus on how the maturity levels for information security risk management are established, reported and challenged
8. Internal Audit functions should pay attention to management's incentives to properly deal with information security, e.g. through relating audit outcomes with management appraisals.

Source: CBIA: 2019, Auditing Information Security Risk Management

Cyber Resilience

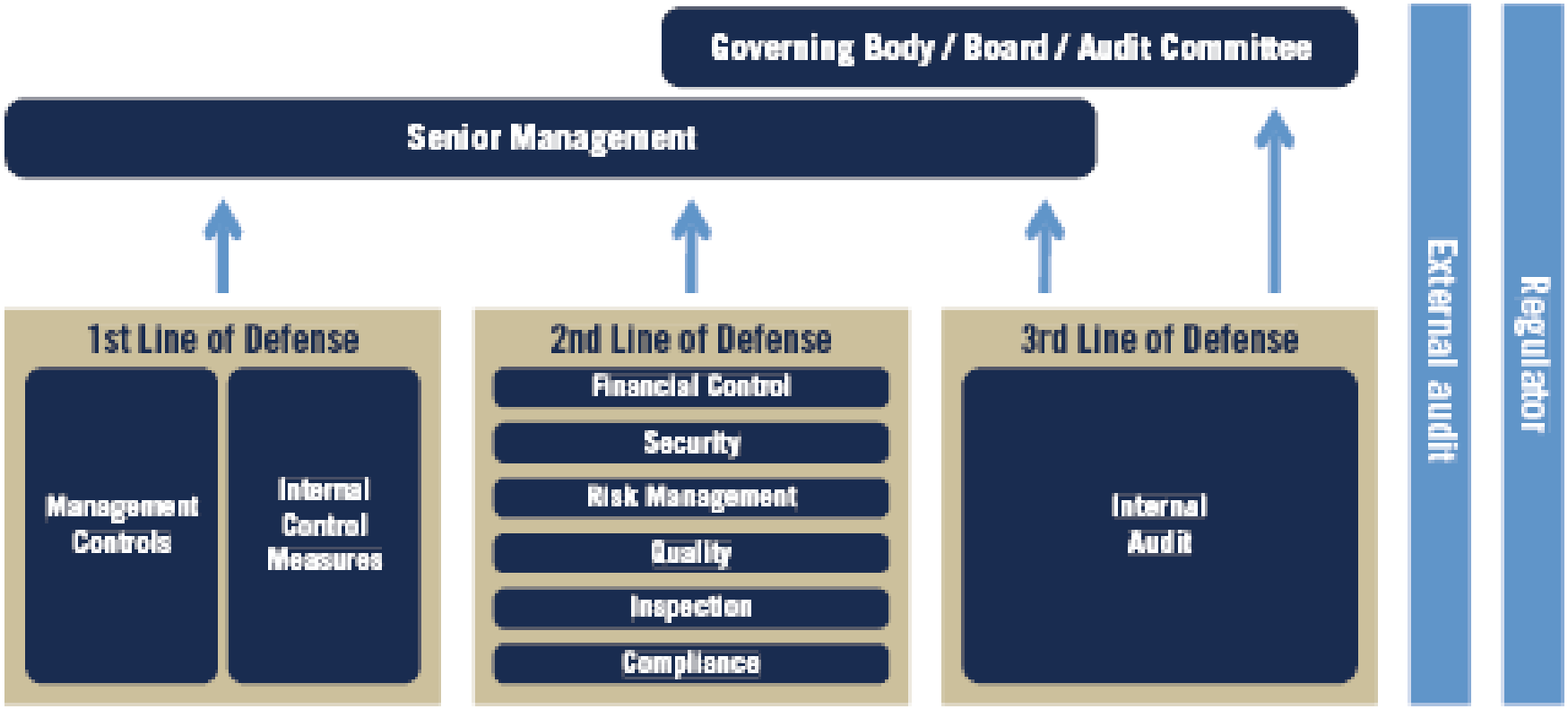
Detailed recommendations regarding information security risk management in central banks

9. Internal Audit functions could enrich their audits on information security risk management by putting more focus on investigating the impact of organizational culture on the behavior of individuals
10. Culture and awareness should be systematically investigated as potential root causes for internal control failures
11. Auditors should stress that in cases of outsourcing of critical business processes, the corresponding information security risks are not automatically outsourced as well
12. Auditors should pay extra attention in case third parties use subcontractors. On-site inspections should be considered

Source: CBIA: 2019, Auditing Information Security Risk Management

Three Lines of Defense

Three Lines - a "common" picture



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Three Lines of Defense

Main Challenges

- Unclear definition of roles and responsibilities and ineffective coordination between lines; however, possible solutions include:
  - Clear mission statement/audit charter and definition of clear procedures
  - Agreements between 3rd and 2nd lines are in place
  - Discussion of audit plan with 2nd LOD
- Unclear definition of risks
- Lack of management buy-in to the model
- Cultural barriers (e.g., siloed approach, information as private property)
- Tone at the top
- Lack of integration between general and granular approach to risk

Source: CBIA: 2018, IA relationships with 2nd line of defense

Three Lines of Defense

Current state

- 3LOD model is largely adopted by Central Banks (either formally or substantially)
- Different organisational set-ups are in place to enforce the model but some common patterns could be observed
- Almost all the CBs have a 2nd line function which oversee the following risks: Operational, Financial, Compliance, Business Continuity, Cyber
- Risk management and compliance are more frequently organised as a separate staff unit (i.e. totally independent), while operational risk management is hierarchically integrated into business with entity-wide perspective

Source: CBIA: 2018, IA relationships with 2nd line of defense

Three Lines of Defense

Current state (cont'd)

- The most recurrent activities carried out by 2LoD regard: providing a risk framework, identifying current and emerging issues, providing guidance and training on risk management processes, facilitating and monitoring effective implementation of risk management practices
- In some cases, 2nd line functions provide assurance
- Extensive relations are in place among the lines but very few cases of integration of different risk information are in place (e.g. corporate risk assessment, integrated reporting)
- Several challenges are still perceived and some possible measures to address them have been identified

Source: CBIA: 2018, IA relationships with 2nd line of defense

Three Lines of Defense

Current state (cont'd)

- 2nd line risk information is used for audit planning and audit engagements
- Auditing the 2nd line functions is often a prerequisite to making use of their risk information
- Approximately 25% of CBIA banks do not make use of 2nd LOD information. In some cases this is due to: different views on risks, insufficient independence, or insufficient documentation

Source: CBIA: 2018, IA relationships with 2nd line of defense

Outsourcing Risks

Reasons for Outsourcing

Access to Best Practices

- Enable focus on core operations.
- Diverse ideas/best practices in non-core areas.

Enhanced Quality

- Accountability in the relationship can resolve quality issues more quickly.

Cost Savings

- Efficient access to specialised talent.

Flexibility & Scalability

- Greater ability to expand or contract operations.

Top 5 Third Party Services

1. Bank Notes
2. Information System Management
3. Real Estate Administration
4. Communications
5. Human Resources

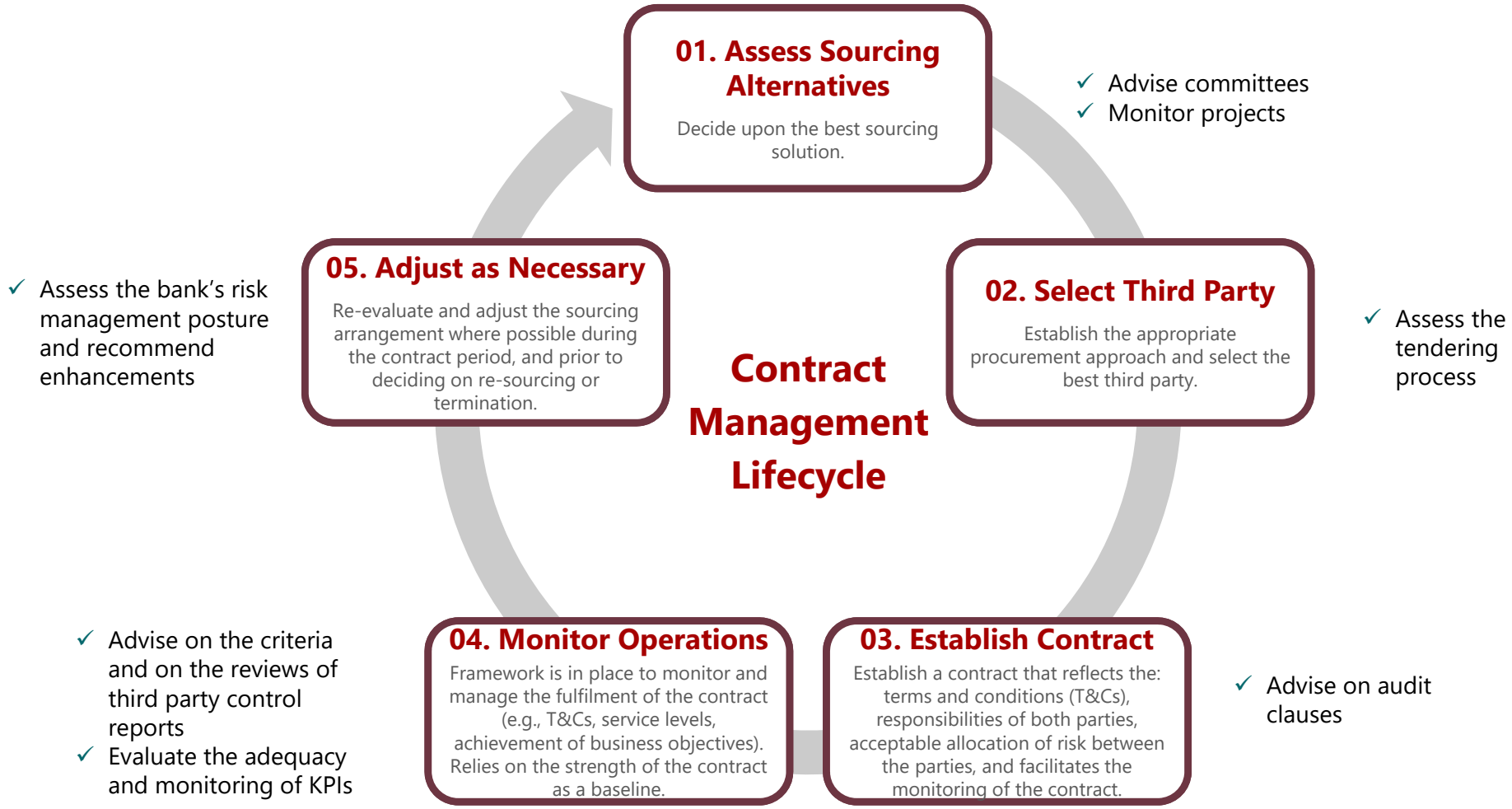
Top 5 Key Risks

1. Security of Information
2. Security of Assets
3. Reputation
4. Execution
5. Compliance

Source: CBIA: 2018, Managing Third Party Risks

Outsourcing Risks

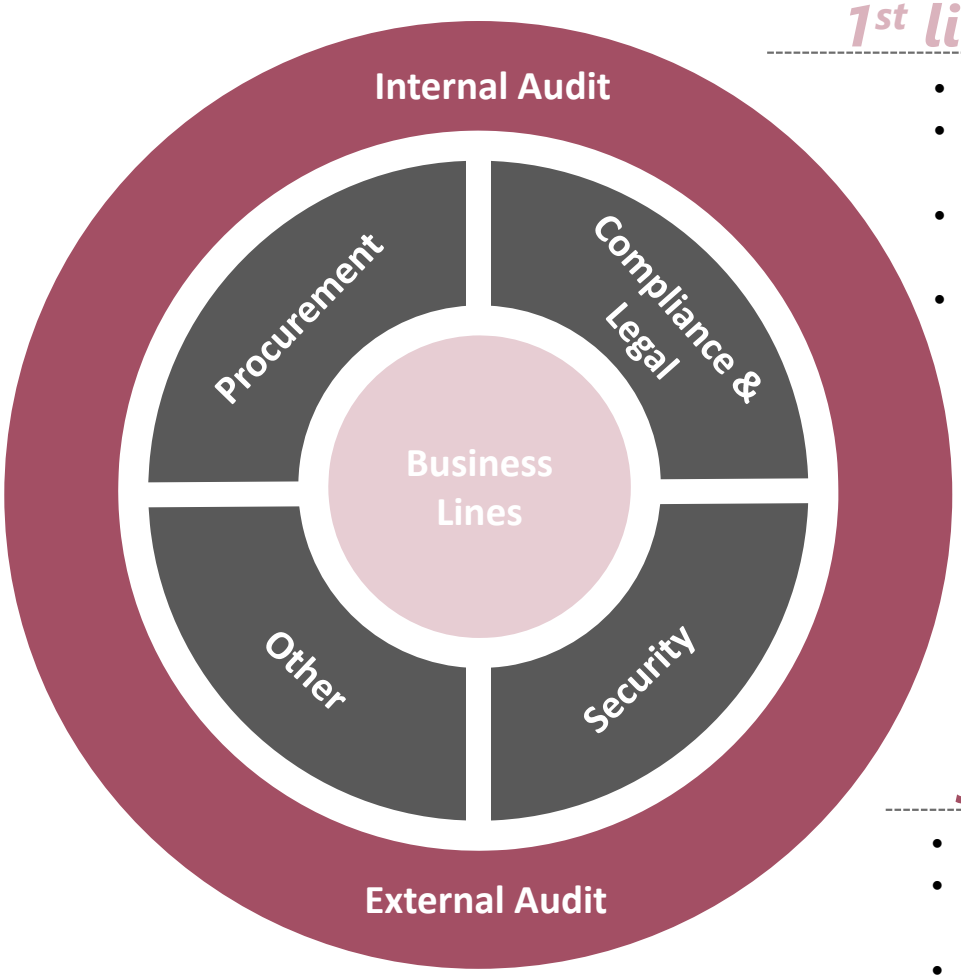
The contract management lifecycle and audit's involvement



Source: CBIA: 2018, Managing Third Party Risks

Outsourcing Risks

Accountabilities



1st line of defence

- Implements established policies
- Execute the contract, manage the third party, and ensure quality
- Ongoing monitoring, escalation, reporting to other lines of defence or stakeholders
- Reviews 3rd party control reports

2nd line of defence

- Enables contracting
- Establishes policies and standards focusing on risk
- Advises and challenges 1st line
- May perform operational monitoring & oversight
- Reviews 3rd party control reports
- Conducts targeted reviews

3rd line of defence

- Performs focused audits
- Provides independent and objective assurance over 1st & 2nd line activities
- Reviews 3rd party control reports in less mature organizations

Source: CBIA: 2018, Managing Third Party Risks

Outsourcing Risks

How can Internal Audit further enhance the value add in the areas of TP/outsourcing?

- Better understand scope of use of TPs across the CB & the strategic and tactical decisions for outsourcing
- Understand risks & have centralized list of respective TP control reports
- Contribute to increase awareness of the importance of a clear and effective governance of the process
- Further develop relationships with 2nd LODs [to clarify roles and responsibilities]; open up lines of discussion between business lines (e.g., experiencing similar issues) or with 2nd lines of defense (e.g., when Security or other should be consulted); get involved at the onset
- Determine with management where other audit assurance may be beneficial and how to obtain it (e.g., using IA, external auditors).
- Allocate more resources to this topic ("audit where the risk is")

Source: CBIA: 2017, Third Party/Outsourcing Risks & the Role of Internal Audit

Outsourcing Risks

How can Internal Audit further enhance the value add in the areas of TP/outsourcing?

Provide advisory services on

- what should be included in TP assurance reports, and on where the report is and is not providing assurance
- establishing and monitoring key performance indicators / key risk indicators
- audit clauses in contract

Provide assurance services on

- outsourcing risk management at a Bank-wide level
- adequacy of the framework and its application
- reasonableness of risk appetite of the 1st & 2nd LODs
- adequacy and effectiveness of 1st & 2nd LODs
- outsourcing (thematic audits or continuous auditing)
- vendors and their processes - system based approach with extensive testing; exercising rights to audit clauses

Source: CBIA: 2017, Third Party/Outsourcing Risks & the Role of Internal Audit

Thank you