

A woman with blonde hair and a man with a beard are looking at a laptop screen. The woman is holding a pen and pointing at the screen. The man is resting his chin on his hand, looking intently at the screen. The background is a blurred office environment.

Banking & Compliance

Key GRC Trends You Need to Know

Is Your Organization Prepared for
the Future of Governance, Risk, and Compliance?

NRI

Contents

1.



Page 2-9

Regulatory Focus in US

2.



Page 10-12

Regulatory Focus for Asian Banks

3.

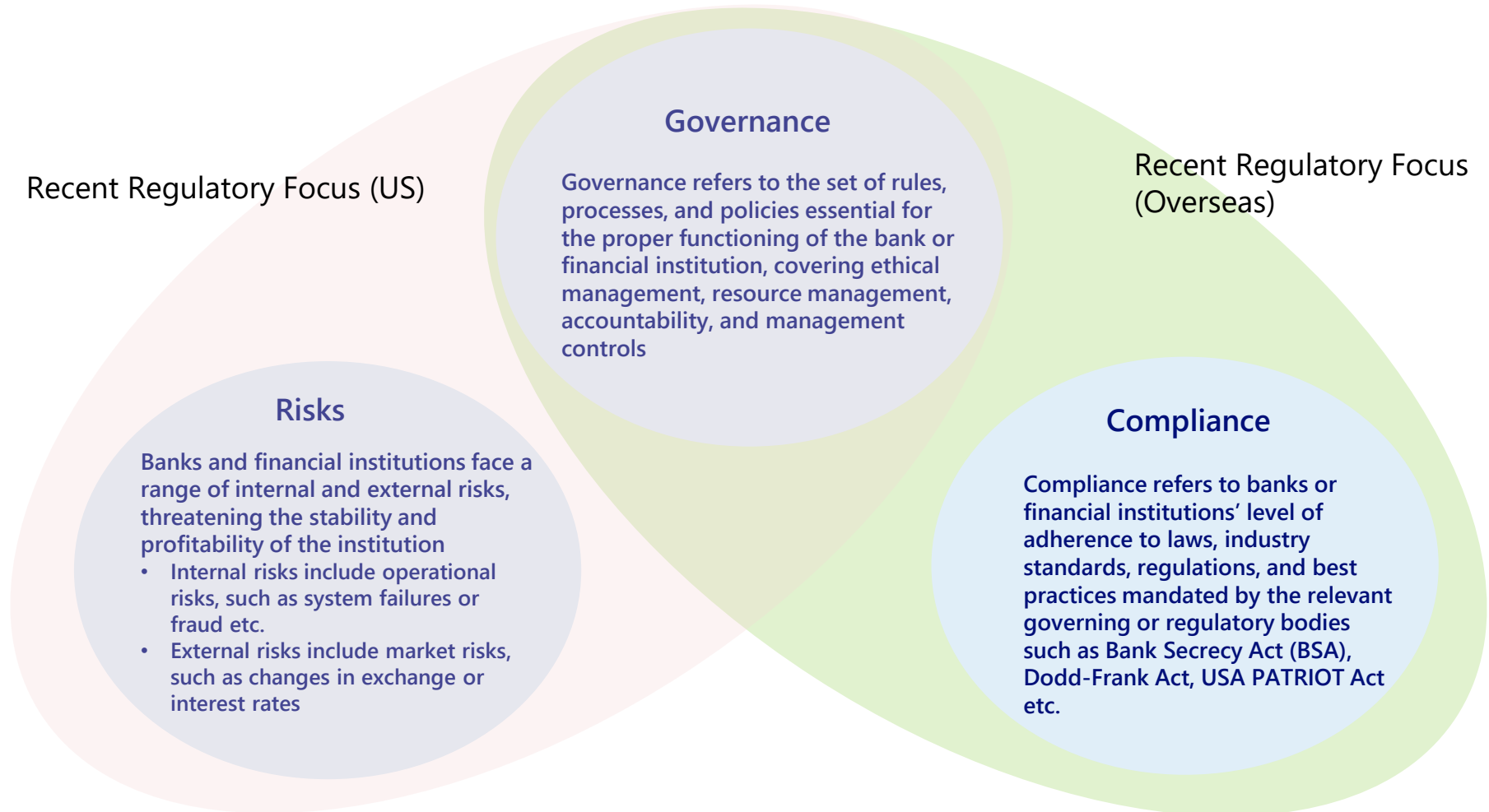


Page 14-17

About NRI

GRC helps increase visibility and mitigate various risks to meet ongoing industry and regulatory standards.

GRC (Governance, Risk and Compliance)



US banks face a wide spectrum of financial and non-financial risks, necessitating robust and comprehensive governance and risk management strategies.

Type of Risks

Risk & Governance	Descriptions
Credit Risk	The risk of financial loss resulting from a borrower's failure to meet contractual obligations
Market/ Interest Rate Risk	The risk of adverse financial impact due to fluctuations in market conditions or interest rates
Liquidity Risk	The risk of being unable to meet short-term financial obligations due to insufficient cash or liquid assets
Enterprise Risk	The risk of material losses arising from strategic decisions or external factors affecting the organization as a whole
Data Risk	The risk associated with the loss, breach, or unauthorized use of sensitive or critical information
Third Party/ Vendor Risk	The risk of operational disruptions or financial losses arising from failures or non-compliance by external vendors or service providers
Compliance Risk	The risk of financial penalties, legal liabilities, or reputational damage resulting from regulatory non-compliance
IT/Cybersecurity Risk	The risk of financial and operational harm from cyber threats, data breaches, or IT system failures
Operational Risk	The risk of loss due to failures in internal processes, systems, or human error, impacting daily operations
Reputation Risk	The risk of deterioration in stakeholder confidence and financial performance due to negative public perception
Model Risk	The risk of financial losses stemming from errors, inaccuracies, or limitations in financial models used for decision-making
Internal/Audit Testing	Evaluates the effectiveness of a bank's internal controls, governance, and risk management processes.

Recent shortcomings in risk & compliance have led to increased scrutiny from regulators, placing a greater emphasis on risk governance and management.

Regulatory Focus Areas by Risk Type

Priority : ◎ - High ○ - Medium △ - Low

Type of Risks	Regulatory Focus	Key Areas
1 Enterprise Risk Management	◎	<ul style="list-style-type: none"> Risk and Control Self Assessment (RCSA) Reporting (KRIs/KPIs) Issue Management Assurance (QC/QA/Monitoring/Testing)
2 Credit Risk Management	◎	<ul style="list-style-type: none"> Credit Analysis Loss Reserves
3 Internal/ Audit Testing	◎	<ul style="list-style-type: none"> Coverage Issue Validation
4 Third Party Risk Management	○	<ul style="list-style-type: none"> Due Diligence and Quality Control Ongoing Monitoring
5 Financial Crimes Compliance	○	<ul style="list-style-type: none"> Model Risk Management
6 Data Governance	○	<ul style="list-style-type: none"> Data Classification and Retention



Bank Considerations
<ul style="list-style-type: none"> Making changes and trimming costs around the edges aren't effective responses to regulatory pressure. Implementing upgraded risk and compliance infrastructure can help instill regulatory confidence Current cost pressures can trigger organizations to streamline disconnected governance and controls systems and manual processes residing in different departments. Streamlining processes can lower costs and free up valuable talent Foreign Banking Organizations (FBOs) with smaller asset sizes are expected to have the same level of risk and compliance measures as the large US banks

Enterprise risk management framework takes following risk governance and management components into account.

Risk Governance Process

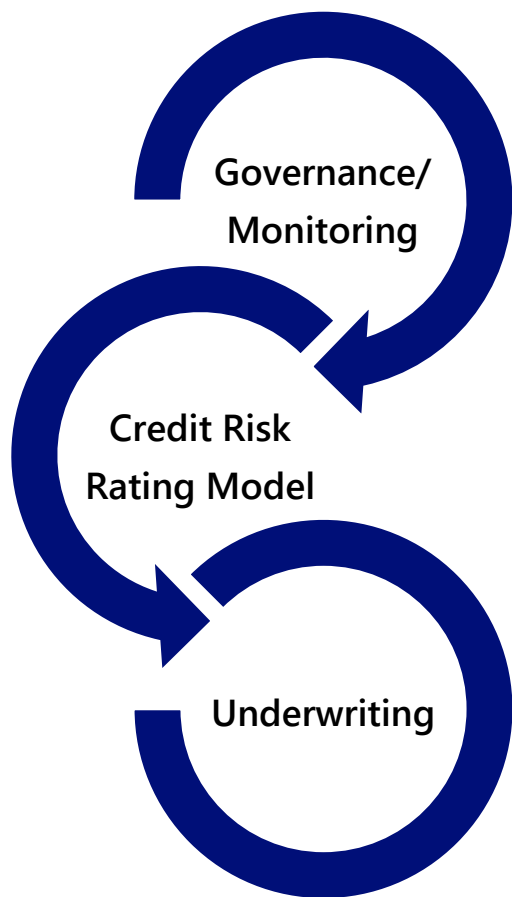
1. Risk Governance & Structure		2. Risk Identification & Assessment	3. Risk Measurement & Control	4. Monitoring & Reporting	
Corporate Governance / Committee Structure	Risk Management Framework and Policy	Risk Taxonomy & Ownership	Control Standards, Taxonomy & Inventory	Risk Reporting & Framework / MIS (Management Information System)	Risk Monitoring
Risk Organizational Structure	Risk Appetite Statement and Metrics	Risk Identification & Inventory	Risk Acceptance Framework	Risk Data and Risk Technology (e.g., GRC)	Escalation Protocols
Risk-specific Policies, Procedures, & Frameworks	Change Management	Risk Assessment (e.g., RCSA)	Control Testing and Monitoring	Issue Management and Issue Resolution Tracking	

Management Component

Components	Component Management
Governance and Reporting	<ul style="list-style-type: none"> Reporting is voluminous and does not include reporting across the risk types (e.g., KRIs, KPIs, emerging risks, project updates, etc.) Minutes do not evidence effective check and challenge with tangible action items and takeaways
Risk Appetite	<ul style="list-style-type: none"> Does not include both qualitative statements and quantitative metrics; thresholds for metrics should be supported with rationale Lack of defined process to manage breaches of metric thresholds
RCSA	<ul style="list-style-type: none"> Lack of support to substantiate inherent risks, control effectiveness, and residual risks Lack of check and challenge by 2LoD of coverage and results Not supported by a complete risk and control taxonomy
KRI/KPI	<ul style="list-style-type: none"> Lack of definitions of KRI and KPI at the Board- and Management-levels; thresholds are not supported, similar to risk appetite metrics
Change Management	<ul style="list-style-type: none"> Change intake process does not have a defined methodology for assessing the materiality of the change
Issues Management	<ul style="list-style-type: none"> Inconsistent framework for raising, tracking, and closing issues, including management reporting and ongoing monitoring
Ops. Risk Events	<ul style="list-style-type: none"> Does not include both financial and non-financial risk events as well as near misses
QC/QA/Monitoring and Testing	<ul style="list-style-type: none"> Lack of defined minimum standards for execution of assurance activities such as issue management, thresholds, sampling, root cause analysis, etc. Insufficient oversight of 1LoD assurance activities as well as 1LoD control execution
Complaints Management	<ul style="list-style-type: none"> Lack of clearly defined definitions for complaints and risk rating methodology Insufficient escalation and review process (e.g., root cause analysis)

The Credit Risk Management framework is based on three key principles: governance and monitoring, underwriting, and the credit risk rating model.

Credit Risk Management Framework



- Defined credit risk appetite
- Sufficient reporting of credit risk management, including risk appetite metric and other KRI monitoring
 - General and specific reserves
 - Concentration (e.g., single borrower, industry, product, country)
- Policy exceptions approvals and tracking
- Us operation should have its own defined written policy limits

- Models should be validated in accordance with US regulatory expectations as outlined in SR11-07
 - Regardless of who developed the model (e.g., Head Office)
 - If Head Office performed the model validation, it should still meet SR11-07 expectations
- Rationale for qualitative adjustments should be improved; over-reliance on risk rating model output should be avoided
- Model risk management framework should be defined to govern the credit risk rating model (e.g., development, validation, tuning, ongoing monitoring, etc.)

- Credit analysis should sufficiently consider factors, such as amortization, liquidity, and repayment sources, parent company/guarantor financials, etc.
- Amortization should be considered; avoid evergreen lending practices
- Maximum amortization years and Loan to Value (LTV) for CRE loans, minimum DSCR, other ratios etc.
- Documentation in English

In-house auditors might lack the expertise for specialized audits or compliance, thus hiring an outsourced firm can offer crucial insights for GRC.

Internal Audit Assessment and Quality Assurance Review Scope

Scope

- In-house internal auditors **might lack necessary expertise for specialized audits** or regulatory compliance matters, and an outsourced internal audit firm can offer insight into industry-specific and general issues that an organization may not be aware of
- Regardless of usage of in-house auditors or external firm, **coverage should include all risk-relevant areas**
- Given the focus of regulators, internal audit should also ensure to include appropriate topics such as **enterprise risk management, third party risk management, etc.**
- Controls developed by Head Office that is applied to the Branch needs to be reviewed (e.g., Head Office developed models)

Issue Validation

- Scope of issue validation by internal audit should include all issues; while certain larger banks have a risk-based process where internal audit reviews certain (e.g., high risk) issues, regulators expect internal audit to validate all issues including **issues stemming from model validations, self-identified issues, regulatory issues, etc.**
- The Bank should develop an issue validation process that ensures consistency in how validations are performed. 2LoD and 3LoD may have different processes but we have seen instances where regulators expect **consistency across the lines of defense**
- Ensure **appropriate coverage of design effectiveness, operating effectiveness, and sustainability in all issue validations**

Quality Assurance & Improvement Program (QAIP)

- Quality assurance review spans the **entire audit body of work, comprise ongoing monitoring and periodic assessment, and is incorporated into the day-to-day practices of the audit activity**
- Given focus on the quality of issue validation, **issue validations should also be included** in the QAIP process and utilize a checklist to evidence review

In 2023, FRB, FDIC & OCC jointly issued 3rd party risk management guidance which replaces each agency's prior guidance for all supervised banking orgs.

Interagency Guidance on Third Party Relationship Risk Management (2023)

Regulations	<ul style="list-style-type: none">• Interagency Guidance on Third Party Relationship Risk Management issued in 2023 replaces the Board's 2013 guidance, the FDIC's 2008 guidance, and the OCC's 2013 guidance
Authority	<ul style="list-style-type: none">• The Board of Governors of the Federal Reserve System or FRB (Federal Reserve Board) is the central banking system of the United States• The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the United States government that aims to protect depositors and maintain stability in the financial system by insuring deposits in banks and thrift institutions• The Office of the Comptroller of the Currency (OCC) is a US Treasury Department bureau responsible for regulating and supervising national banks and federal savings associations
Key Provisions	<ul style="list-style-type: none">• The guidance states that it is the responsibility of each banking organization to analyze the risks associated with each third-party relationship and to calibrate its risk management processes accordingly• As part of sound TPRM, banking organizations would:<ul style="list-style-type: none">✓ Analyze the risks associated with each third-party relationship and tailor risk management practices, commensurate with the banking organization's size, complexity, and risk profile and with the nature of the individual third-party relationship✓ Maintain "complete" inventories of third-party relationships and periodically conduct risk assessments for each third-party relationship to support changes in risk determinations over time and to update risk management practices accordingly✓ Engage in "more comprehensive and rigorous oversight and management" of third-party relationships that support "higher-risk" activities, including "critical activities". "Critical activities" include those that could:<ul style="list-style-type: none">- Cause the banking organization to face significant risk if the third party fails to meet expectations- Have significant customer impacts- Have a significant impact on the banking organization's financial condition or operations

The regulators supervise guidance on model risk management for banking organizations focusing on all aspects of model development and data.

Model Risk Management Guidelines

- Model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates
- Office of the Comptroller of the Currency (OCC) and Federal Reserve guidance expanded their focus beyond model validation to cover all aspects of model risk management, emphasizing that banks should align internal policies with these principles, tailoring practices to their specific risk exposures, activities, and model complexity

Model Development, Implementation and Use

- Model risk management requires disciplined development & implementation processes aligned with model's intended use & organizational policies
- Effective development involves robust methodologies, thorough testing, and a demonstrated understanding of model uncertainty, with appropriate adjustments to account for potential inaccuracies



Model Validation

- Evaluation of Conceptual Soundness: Assess the quality of model's design, methods, and variables, ensuring alignment with research & standards
- Ongoing Monitoring: Ensure the model is properly implemented & performing as intended, adjusting for changes in conditions, & benchmarking
- Outcomes Analysis: Compare model outputs with actual outcomes through back-testing & other methods to assess performance accuracy



Governance, Policies and Controls

- Effective model risk management requires strong governance, including clear policies, resource allocation & adherence to procedures
- Governance involves documentation, board oversight ensuring model risk within tolerance & internal audits assessing framework effectiveness
- When using external resources, activities must be clearly defined & align with guidance, organizations should maintain an updated model inventory

Asian banks are motivated to invest in GRC services because of heavy penalties imposed by US regulators.

Asian Banks fined for failing US Regulations


RISK & COMPLIANCE JOURNAL

Fined \$32 Million by New York's Financial Regulator and Fed for Compliance Failures

NYDFS alleged the bank's New York branch had deficiencies in its anti-money-laundering and Bank Secrecy Act compliance programs

fined \$25M for repeat AML compliance failures

By  Kyle Brasseur | Fri, Sep 29, 2023 4:06 PM

The American branch of  agreed to pay \$25 million across settlements with three separate regulators for admitted violations of the Bank Secrecy Act (BSA) and anti-money laundering (AML) requirements.

GRC Trends

- Multiple Asian banks have already been penalized for failing compliance (AML/BSA) in the US and thus looking to strengthening their compliance system
- Since these banks are already investing in such services, they plan to strengthen their compliance system globally instead of solely focusing on the US
 - Financial hubs like EU, Singapore etc. already follow FATF guidelines for compliance, same as US
 - Other countries like Korea, Japan etc. are also moving in the same direction

US follows FATF guidelines for compliance controls. Financial hubs follow FATF guidelines strictly and non-financial hubs are moving in the same direction.

FATF (Financial Action Task Force) Guideline Adoption Trends

Current level of acceptance : ◎ - High ○ - Medium △ - Low

Target	Current level of acceptance of US model		Compliance (AML)
Asian Banks in US	○		<ul style="list-style-type: none"> All foreign banks have to abide by FATF guidelines that are followed by US banks
Subsidiaries in financial hubs	European Union	◎	<ul style="list-style-type: none"> European Commission closely works with FATF to prevent money laundering and counter the financing of terrorism at international level aligning with the US
	Hong Kong	○	<ul style="list-style-type: none"> Hong Kong is compliant on majority recommendations made by FATF for AML like the US
	Singapore	◎	<ul style="list-style-type: none"> Singapore ranked third in the Global Financial Centres Index 2023, after New York and London. The global FATF verifies its robust legal and institutional frameworks to tackle money laundering
Subsidiaries in non-financial hubs	China	△	<ul style="list-style-type: none"> The efforts of Chinese financial institutions to expand globally has been met with scrutiny from Europe and the US. After being issued several warnings regarding AML regulation, China's regulators are pushing for international guidelines
	Korea	○	<ul style="list-style-type: none"> Subsidiaries of Korean banks like Shinhan Bank had to face heavy penalties in the US for repeat AML compliance failures, thus these banks are moving towards adoption of stricter international guidelines like the FATF
	Japan	○	<ul style="list-style-type: none"> The Office of the Comptroller of the Currency in the US has warned Japanese banks like MUFJ Group on their long-running inability to weed out illegal transactions, thus Japanese banks plan on moving towards stricter international guidelines like the FATF
	Thailand	△	<ul style="list-style-type: none"> Five Thai banks were caught with facilitating Myanmar's illegal weapons. Thus, Thai government intends to adopt Singapore's AML model, which is similar to the US
	Philippines	△	<ul style="list-style-type: none"> The Philippines has been in the FATF's grey list since 2021, and a deadline to improve AML/CFT policies has been set to the end of 2024. Their progress and policy improvement has been acknowledged by FATF
	India	△	<ul style="list-style-type: none"> India got certified for high level of technical compliance by FATF in 2024, but it needs to strengthen itself in areas of cryptocurrency etc.
	Taiwan	○	<ul style="list-style-type: none"> Taiwan has a decent standing on compliance acceptance by FATF

In terms of AML/CFT measures, Asian Banks needs to further enhance their capabilities across various areas.

Key Points Raised in the FATF 4th Round Mutual Evaluation of Asian Banks

Issues	Key Points
Overall Framework	<ul style="list-style-type: none">Establishing systems and setting schedules for system maintenance and schedule settingRevising guidelines related to AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism)
Risk Assessment	<ul style="list-style-type: none">Improving risk assessment methods (e.g., assessments tailored to business and product characteristics)Promoting a more comprehensive understanding of money laundering and terrorist financing risks
Customer Due Diligence (CDD)	<ul style="list-style-type: none">CDD remains limited to collecting and verifying basic information, not leading to effective risk assessment
Enhanced Due Diligence (EDD)	<ul style="list-style-type: none">EDD is limited to customer identification and list screening
Sanctions Compliance	<ul style="list-style-type: none">Deficiencies observed within financial institutions and screening is not being conducted promptly and accuratelyStrengthening measures to prevent transactions with sanctioned individuals or third parties involved with them, including asset freezing
Beneficial Ownership (BO)	<ul style="list-style-type: none">Inadequate understanding of risks by corporate structure and insufficient acquisition, verification, and validation of BO informationChallenges in verifying BO in cases such as trustsInformation updates are not up-to-date
Politically Exposed Person (PEP)	<ul style="list-style-type: none">No specific measures applied to foreign PEPsDomestic PEPs are not recognized as a specific category
Customer Management	<ul style="list-style-type: none">Information updating procedures for existing customers are ongoing, but the updates are not being utilized effectively for monitoringFully implementing ongoing customer management with set deadlines (including verification of BO)
Transaction Monitoring and Suspicious Transaction Reporting	<ul style="list-style-type: none">Introducing transaction monitoring systems that accurately reflect the results of ongoing customer managementReducing false positives and increasing detection/reporting of suspicious cases through sophisticated scenariosConsidering and promoting the practical use of joint transaction monitoring systems by private sector entities

NRI is a Japan-based global consulting firm with approximately 1,100 consultants, which provides advisory/assurance consulting services to public and private sectors

Our Profile: Key Figures

Established in **1965** in Japan

Total employees of **16,500+** with **1,100** consultants

Annual revenue of **5** billion USD (FY 2022)

Global footprint of **44** offices in **14** countries

Strategic partnership
with

h&z Beratung mit
Hirn, Herz und Hand

market**xcel**

Skha Consulting
Strategy. Execution. Result.

■ JAPAN

Tokyo | Osaka | Nagoya

■ EAST ASIA

Seoul | Shanghai | Beijing | Dalian |
Hong Kong | Taipei

■ SOUTH EAST ASIA

Bangkok | Manila | Jakarta |
Singapore

■ SOUTH ASIA

New Delhi

■ NORTH AMERICA

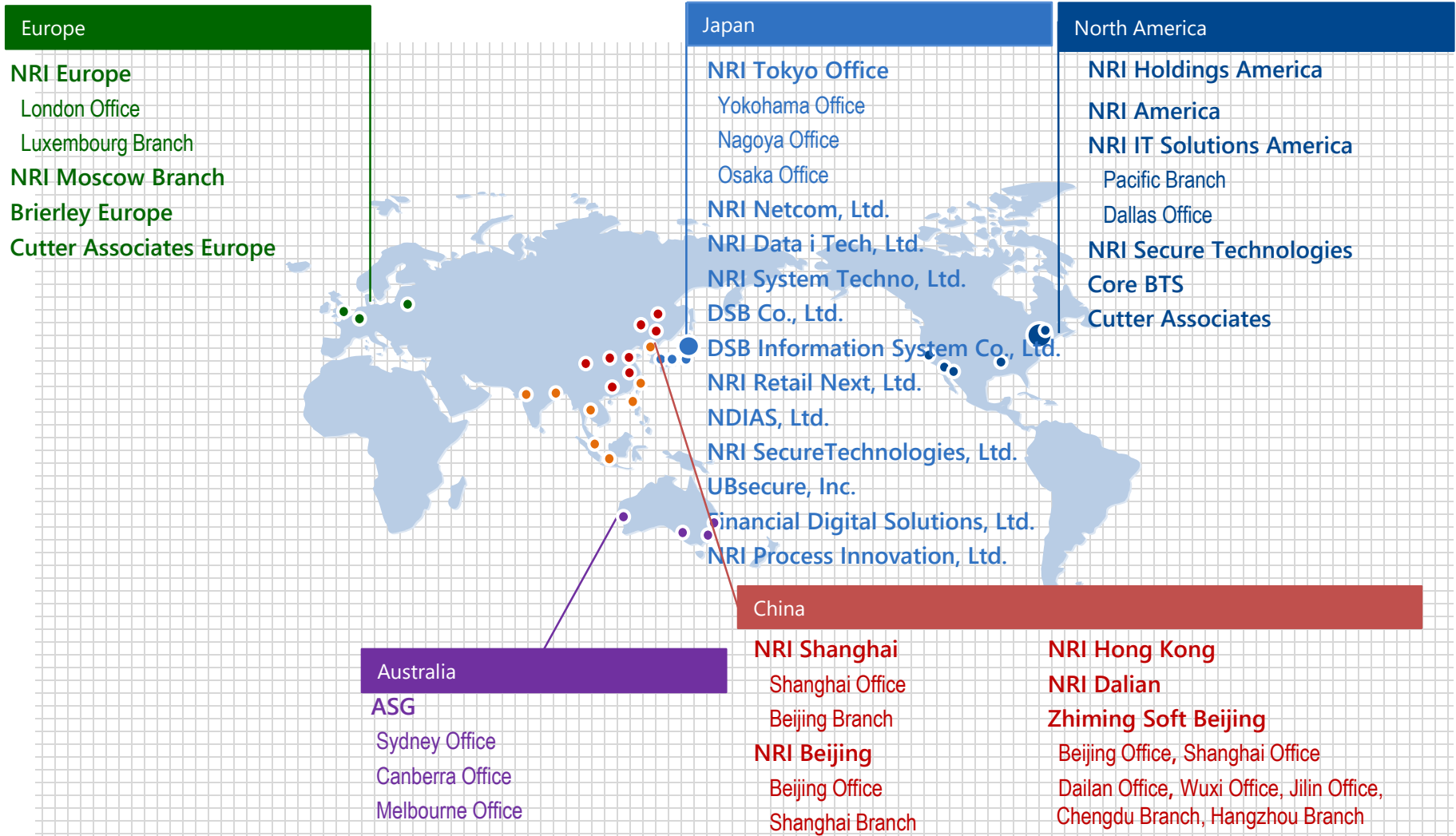
New York | Dallas | Mexico City

■ EUROPE

Moscow | London

Global Network

NRI supports clients for various business and risk issues through our Global Network with specific focus in Asian region and Asian financial institutions



NRI has substantial experience in consulting for highly-regulated financial service entities



1. Global Risk/Compliance Management

- As a leading IT/consulting firm, NRI has supported major Asian financial institutions' risk and compliance management.

2. Global Investment Banking Support

- As Nomura Group's Advisory and Business Process Outsourcing ("BPO") arm, NRI has supported Nomura Holdings' global risk and compliance support, including internal audit.

3. Audit/Monitoring/Testing Outsource

- Provides BPO and audit support professional services to other financial institutions through Daiko Shoken Business Co., Ltd. (DSB), a wholly-owned subsidiary of NRI.

Ray Park

Background

2004 Yonsei University

Bachelor of Arts in English Literature and Sociology

2004 MONITOR GROUP (Current: Deloitte Consulting)

Research Analyst

2005 Korea-US Air Component Command

2nd Lieutenant, Intelligence Officer

2006 Department Of Defense (Intelligence Command)

1st Lieutenant, Senior Research Analyst

2008 Nomura Research Institute, Seoul

Manager – Business Innovation Group

2012 JUBILEE LAB (Fintech Start-up)

Director – Business Development Department

2012 Hyundai Capital

Manager – Overseas Strategy Department (US)

2013 Nomura Research Institute America

Senior Manager – Head of Business Strategy Group

2017 Nomura Research Institute America

Co-Head of Research and Consulting Division

Expertise

- Financial Services
- Fluent in Korean

Representative Projects

- Developed Korean major bank's global expansion by formulating strategy and supporting operations such as engaging and handling regulators
- Conducted Korean major financial institute's US business operation by reviewing and analyzing control areas (operational and non-operational risk factors)
- Worked with Asian Development Bank and ASEAN Secretariat to support ASEAN regulators in finance. Supported developing and implementing regulations for financial market including capital market and banking sectors
- Conducted due diligence for a major Chinese bank and performed a detailed assessment of operational risk for investing in financial institutions
- Supported a global investment bank's Korean operation by analyzing and reviewing Korea's new capital market regulations
- Supported Korean special public corporation in financial services sector to develop businesses in capital market by analyzing and reviewing US, Japan, and Europe's regulations
- Supported Asian client's acquisition of US consumer finance company which is specialized in lending business by analyzing business model and assessing risk factors
- Explored growth opportunities in the US market for a global IT company, and performed a detailed assessment of vendors in governance, risk and compliance sectors

Jin Kim

Background

- 10 years in compliance and risk management across all three lines of defense
- Senior position at boutique regulatory compliance consulting firm, responsible for managing large-scale engagements and business development
- Investment advisor, responsible for due diligence of investments, primarily asset banked lending and commercial real estate, for a family office

Expertise

- Extensive experience in financial crimes, corporate compliance, Anti-Money Laundering (AML), and sanctions-related compliance.
- Deep knowledge in assurance/internal audit through internal audit and monitoring and testing engagements.
- Knowledge of risks and controls across bank operations (e.g., treasury, credit risk, corporate compliance, trade finance, etc.).
- Knowledge and experience with banking systems such as Prime, Actimize, Archer, Mantas, FircoSoft, etc.
- Fluent in Korean

Representative Projects

- Managed and executed end-to-end internal audit engagements for multiple clients, including fully outsourced internal audit
- Performed audits and testing reviews for various control areas (e.g., liquidity risk, credit risk, trade finance operations, financial crimes compliance, broker dealer compliance, etc.)
- Assisted in the validation of articles pursuant to regulatory orders in addition to other audit issues. Conducted validations for both audit and regulatory issues and performed risk assessments and audits while acting as outsourced internal audit for several foreign banking organizations
- Held key roles in compliance program reviews for major international financial institutions pursuant to regulatory mandates, including both domestic and international operations
- Assessed key components of compliance programs such as governance, internal audit, second line testing, customer due diligence, transaction screening, transaction monitoring, and risk assessment
- Assisted and performed remedial efforts (e.g., KYC files reviews, gap analysis, policies and procedures, risk assessments, etc.) for multiple financial institutions
- Performed model validations and tuning activities for financial crimes compliance models



**Envision the value,
Empower the change**