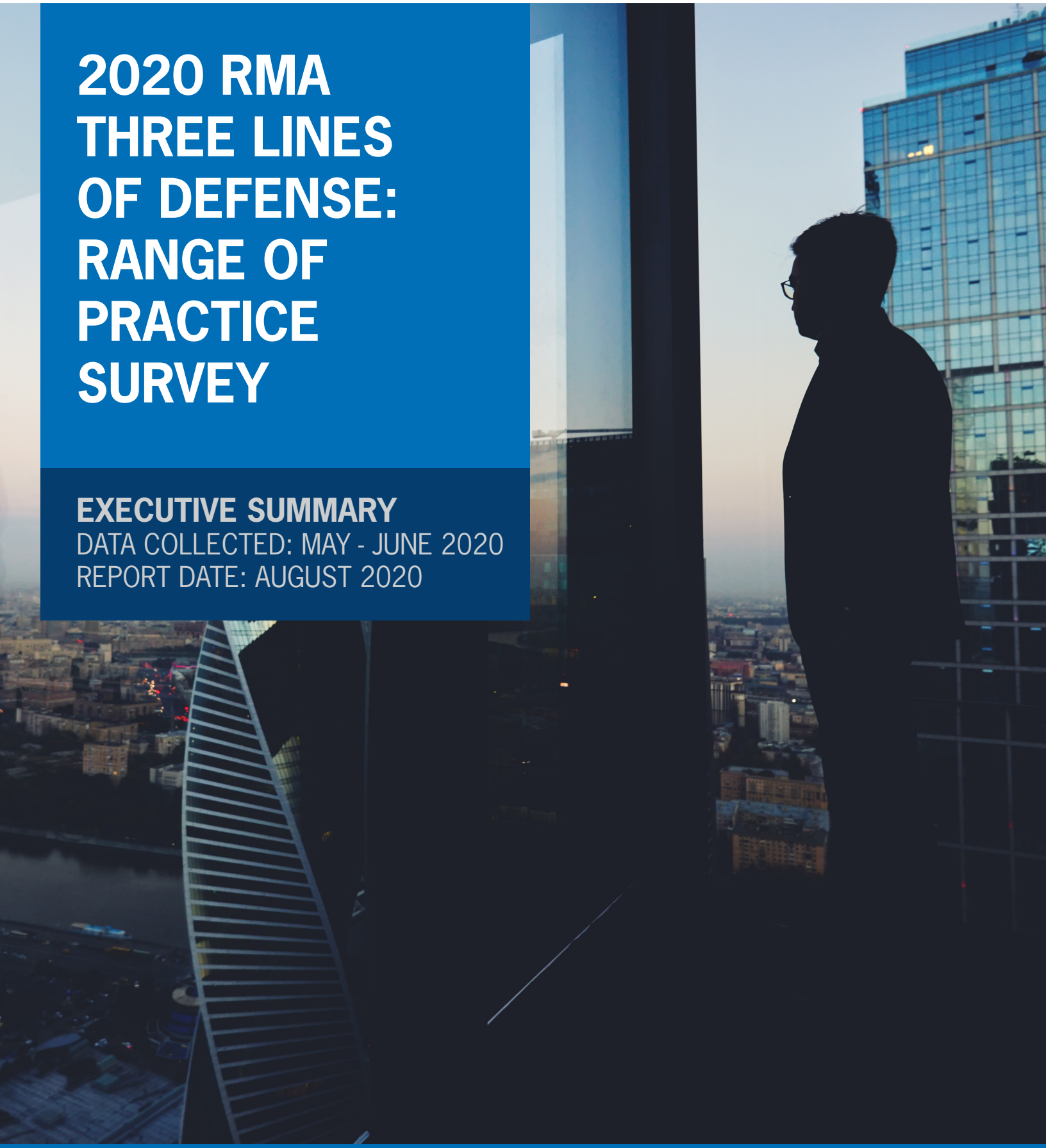
rma®
THE RISK MANAGEMENT ASSOCIATION

JOIN. ENGAGE. LEAD.

2020 RMA THREE LINES OF DEFENSE: RANGE OF PRACTICE SURVEY

EXECUTIVE SUMMARY

DATA COLLECTED: MAY - JUNE 2020
REPORT DATE: AUGUST 2020



Enterprise Risk • Credit Risk • Market Risk • Operational Risk • Regulatory Affairs • Securities Lending • Internal Audit

ACKNOWLEDGEMENTS

The survey was conducted by The Risk Management Association between May and June 2020. Most of the questions were multiple choice with many opportunities to provide comments. Some questions were open text and designed to provide insight into challenges and best practices in the Three Lines of Defense.

A total of 135 responses were collected covering a range of financial institutions from three asset sizes: $250 billion or greater, $60 billion to $249,999, billion and less than $60 billion, including community, regional, super-regional, and investment banks. Primary functions of each institution ranged from retail, commercial, broker-dealer, as well as others. These results will allow for additional analysis by asset size and subject matter for future articles in *The RMA Journal*.

The survey was created with help from members of the ORM and ERM Councils. Special thanks to:

- Joanne Aron, Head of Governance and Risk, HSBC
- Didier Blanchard, Head of ERM, Societe Generale
- George Buchanan, EVP, CRO, Regions Bank
- Lori Calhoun, Chief Risk Officer, Dollar Bank
- Stephen Carmichael, VP, Strategy, Corporate Risk, Discover Financial Services
- James Dunne, SVP, Director of Enterprise Risk Management, TCF National Bank
- Kenzel Fallen, SVP, Enterprise Risk Program Manager, First Horizon Bank
- Allyson Kidik, Manager, KeyBank
- Tom O'Hara, EVP, Huntington National Bank
- Brent Poley, VP, Enterprise Risk Management, Charles Schwab & Co.
- Edward Schreiber, EVP, Chief Risk Officer, Zions Bancorporation

The survey is intended to capture and share the following:

- Maturity and Development of the Three Lines of Defense
- Organizational Structure
- Roles and Responsibilities
- Best Practices

The final report provides participants' responses, while protecting the confidentiality of individual institutions by masking the source of responses. Note: Due to rounding, percentages in the tables may not add up to 100.

RMA staff members contributing to the study were Elena Noverola and Edward J. DeMarco Jr. The final report was written by RMA.

RMA would like to thank the institutions that contributed to this study. Credit for participation was given to all 135 institutions regardless if respondents skipped certain questions, yet we feel they provided valuable data to the majority of the questions.

We respectfully request that these materials not be shared with any consultants or service providers. The material contained in this document is exclusive to RMA and contributing members.

The following results include responses from institutions listed below as well as many others.

- Bank of Montreal
- BankUnited
- Berkshire Bank
- BMO Financial Group
- BNY Mellon
- Capital One
- CIT Group
- Citibank
- Citizens Bank
- Columbia State Bank
- Desjardins Group
- Fidelity Bank
- First Republic Bank
- Frost Bank
- Gateway First Bank
- Hancock Whitney Bank
- Hawaii National Bank
- HSBC
- Iberia
- JPMorgan Chase & Co.
- KeyBank
- Lincoln Savings Bank
- Maine Community Bank
- Middlesex Savings Bank
- M&T Bank
- NatWest Group
- Ozona Bank
- Peoples Trust
- Scotiabank
- Stetler
- TCF Bank
- The American National Bank of Texas
- Third Coast Bank, SSB
- Truist
- UBS
- Voya Financial
- Wells Fargo
- Zions Bancorporation

Disclaimer

JOIN. ENGAGE. LEAD.

About RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, more than 18,000 of these individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Members actively participate in the RMA network of chapters. These chapters are run by RMA Associates on a volunteer basis and they provide our members with opportunities in their local communities for education, training, and networking throughout all stages of their financial services career. Chapters are located across the U.S. and Canada as well as in global financial centers.

RMA members also avail themselves of benefits offered through headquarters in Philadelphia, Pennsylvania. To assist members in advancing sound risk management principles, RMA keeps members informed and provides access to industry information at this site; publishes The RMA Journal and a variety of newsletters, podcasts, books, and statistics; conducts workshops and seminars; holds conferences, including an annual convention (Annual Risk Management Conference); and has numerous committees working on a variety of projects.

Visit RMA at www.rmahq.org.

Note: As a not-for-profit, professional association, RMA does not lobby on behalf of the industry.

EXECUTIVE SUMMARY

The survey was conducted by The Risk Management Association between May and June 2020. Most of the questions were multiple choice with many opportunities to provide comments. Some questions were open text and designed to provide insight into challenges and best practices in the Three Lines of Defense.

A total of 135 responses was collected covering a range of financial institutions from three asset sizes: $250 billion or greater, $60 billion to $249,999 billion, and less than $60 billion, including community, regional, super-regional, and investment banks. Primary functions of each institution ranged from retail, commercial, broker-dealer, as well as others.

Participating institutions were asked to provide their primary regulator for context and further analysis. As expected, all participating institutions are regulated by one or more of the following: OCC, FRB, FDIC, State, FINRA, and OSFI (Canada).

This is the breakdown of participation by asset size:

Asset Size	Number of Institutions	Percent
Less than $60 billion	91	68%
$60 billion to $249,999	17	12.5%
$250 billion or greater	27	20%

THE SURVEY WAS DIVIDED INTO THE FOLLOWING SECTIONS:

- Maturity and Development of the Three Lines of Defense
- Organizational Structure
- Roles and Responsibilities
- Challenges and Best Practices

Three Lines of Defense (3LOD)

In the financial industry, identifying, managing, and controlling risk continues to evolve. Guidance issued by the Office of the Comptroller of Currency (OCC) upholds the trend in today's regulatory environment. The Three Lines of Defense are adopted by firms as the foundation of the risk framework. Each line of defense serves a specific purpose in the risk structure.

1. First Line of Defense consists of the "business or risk owners" who operate within the specific job function and execute the day-to-day activities. The first line is also responsible for the risk within their function.
2. The Second Line of Defense is the oversight function. This independent role ensures risks are identified, documented, and mitigated within reasonable tolerance. This group of partners provides oversight to the First Line of Defense.
3. The Third Line is the internal audit department.

Challenge – how to coordinate risk and control functions effectively and efficiently throughout the organization while not duplicating duties and oversight unnecessarily.

Maturity of Three Lines of Defense (Q5-Q9)

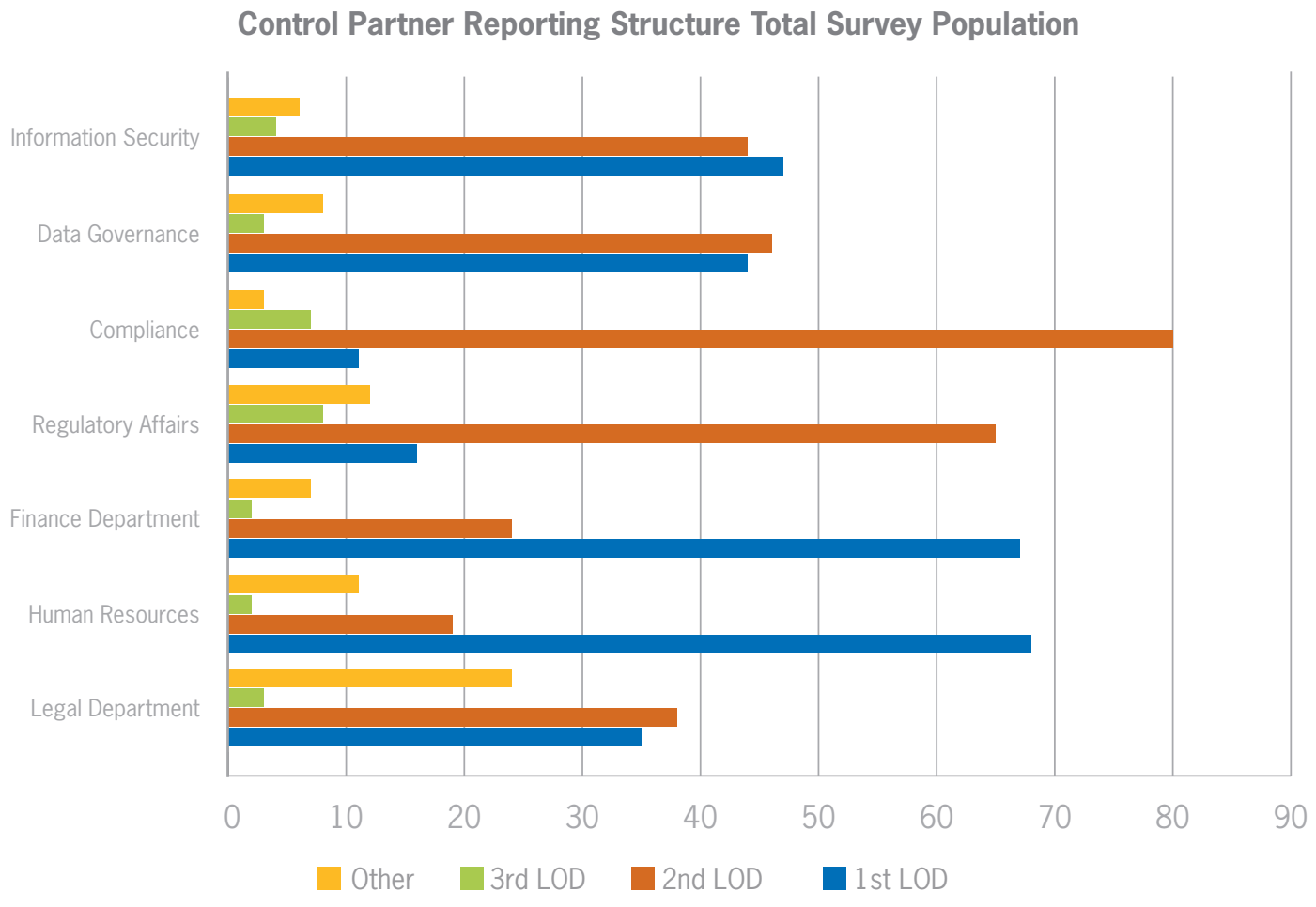
Approximately 80% of institutions have adopted the Three Lines of Defense (3LOD) risk management approach. Maturity of a formal risk management program and a successful 3LOD takes time. Results of the survey indicated the maturity process is a marathon, not a sprint. Most institutions reported 1 to 5 years to effectively establish the 3LOD within the institution.

Asset Size	Less Than 12 Months		1 to 5 years		More than 5 years	
Less than $60 billion	8	13%	46	75%	7	11%
$60 billion to $249,999	1	5.8%	15	88%	1	5.8%
$250 billion or greater	2	8%	19	76%	4	16%

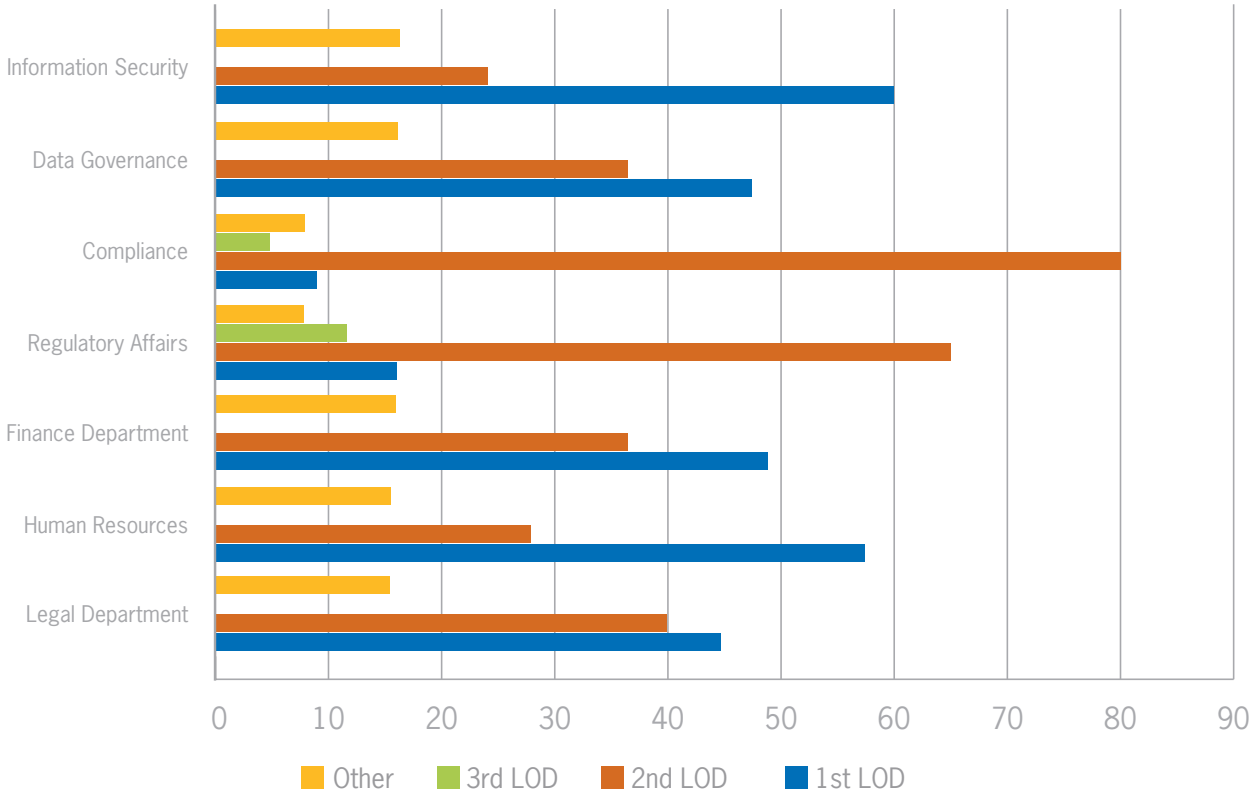
Organizational Structure (Q10 – Q15)

Risk management requires partnership and collaboration from various departments within an organization. Some organizations consider oversight and/or control partners to live in the Second Line of Defense while others consider them to live in the First Line of Defense. A majority of institutions consider Compliance and Regulatory Affairs to be a Second Line function. Institutions are evenly split between Data Governance and Information Security being a First Line or Second Line function. Finance and Human Resources predominantly are considered to be a First Line function. In the asset size of less than $60 billion, the institutions considered more functions to be part of the Third Line of Defense or outside of the Three Lines of Defense.

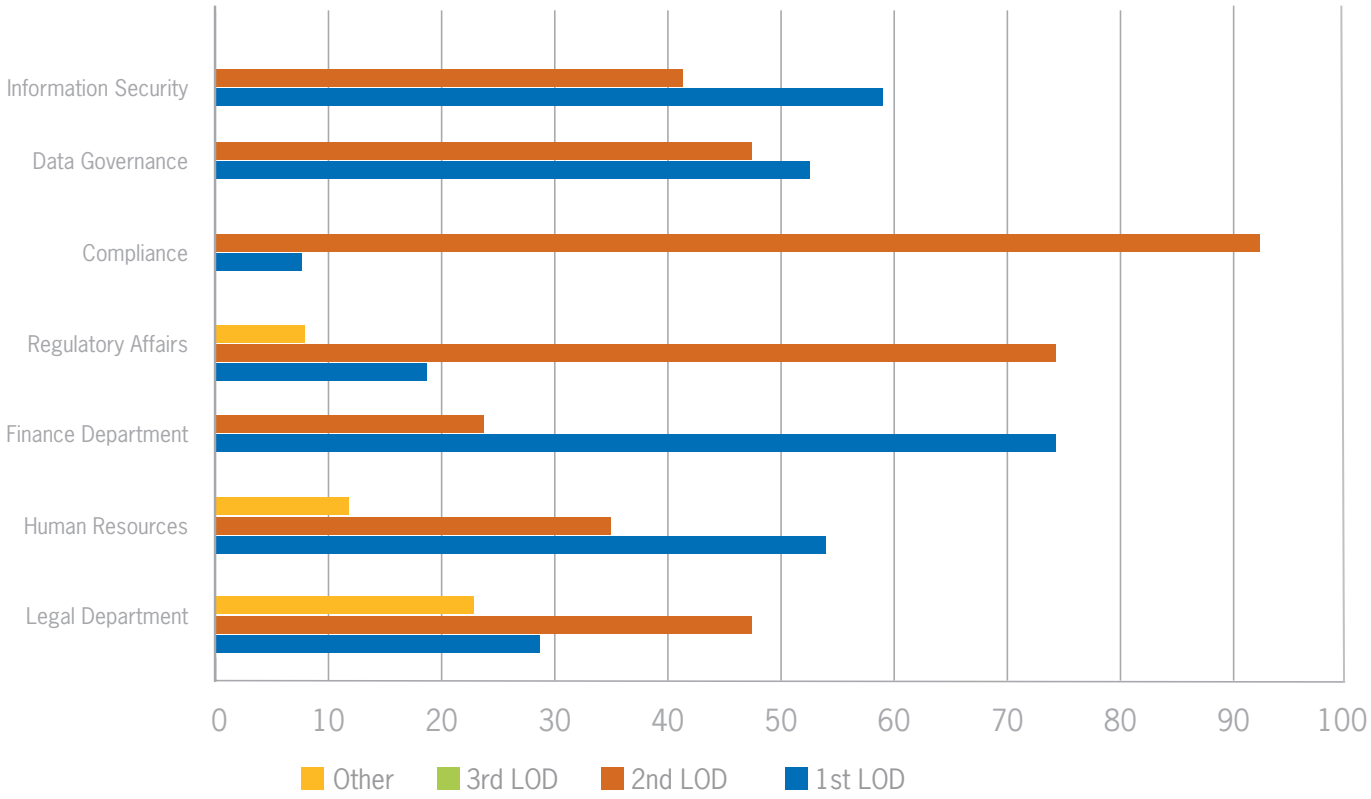
Responses	1st LOD		2nd LOD		3rd LOD		Other	
	Count	Percent	Count	Percent	Count	Percent	Count	Percent
Legal Department	47	34.8%	52	38.5%	3	2.2%	33	24%
Human Resources	92	68%	26	19%	2	1.4%	15	11.%
Finance Department	91	67%	33	24%	2	1.4%	9	6.6%
Regulatory Affairs	22	16.2%	88	65%	9	6.6%	16	11.8%
Compliance	15	11%	108	80%	8	5.9%	4	3%
Data Governance	59	43.7%	63	46.6%	3	2.2%	10	7.4%
Information Security	64	47.4%	59	43.7%	5	3.7%	7	5.2%



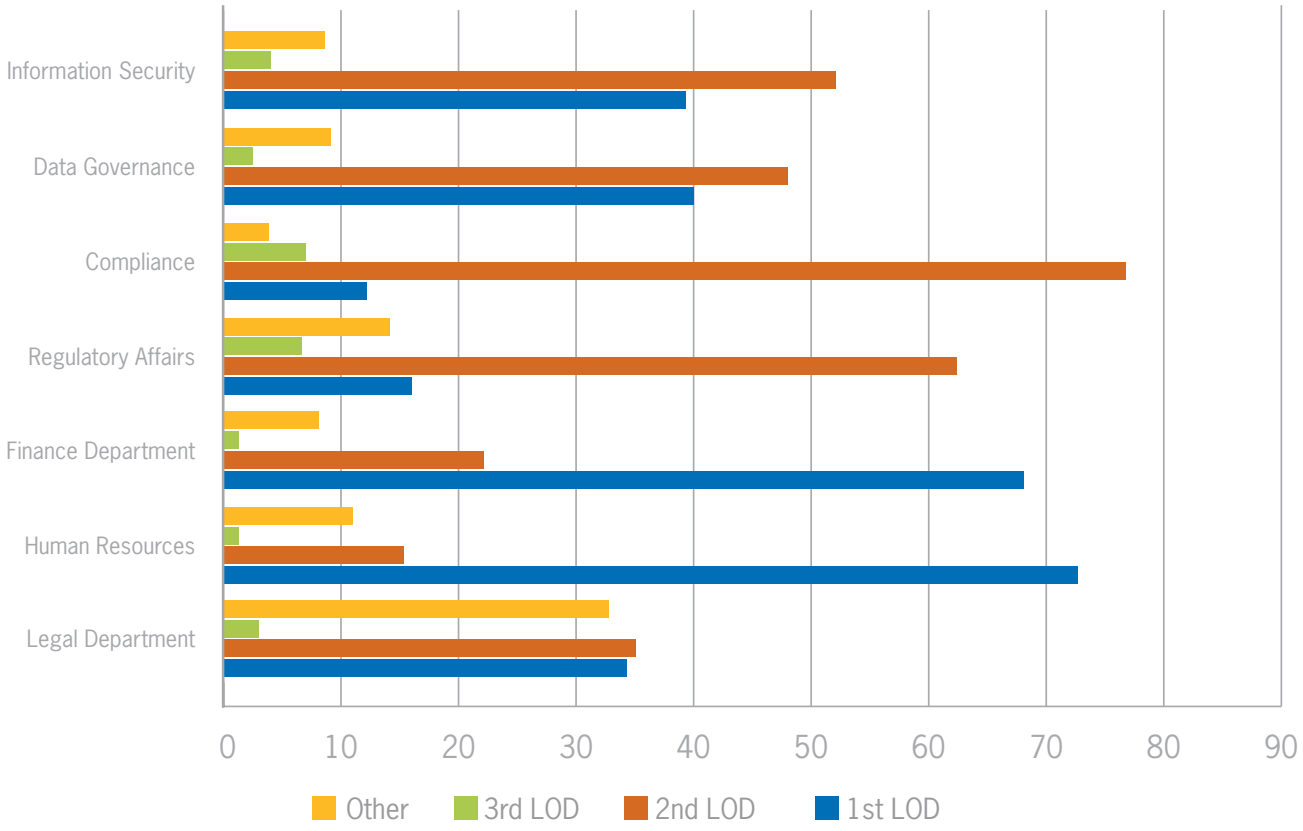
Control Partner Reporting Structure $250 Billion or Greater



Control Partner Reporting Structure $60 Billion to $249,999 Billion

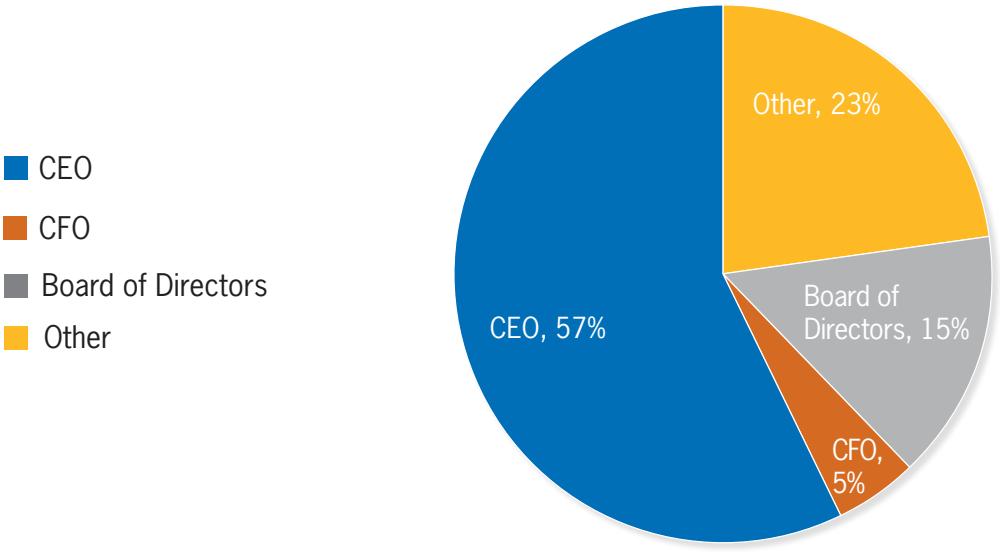


Control Partner Reporting Structure Less than $60 Billion



The Chief Risk Officer (CRO) is the primary executive responsible for an efficient and effective risk program within an organization. In most cases, the CRO reports to the CEO or Board of Directors. The CRO holds executive level discussions to include the institution's risk appetite, regulatory environment, and a holistic view of the institution's risk landscape as well as emerging and external risks. Approximately 57% of participants indicated that the CRO reports to the CEO of the company. The 23% that reported "Other" stated that the CRO reports to the COO, Risk Committee, Audit Committee, Bank President, and legal department to name a few. A majority of the "Other" selection is from the asset size of less than $60 billion. For the asset size greater than $250 billion, 75% indicated the Chief Risk Officer reports to the CEO.

The Chief Risk Officer Reporting Structure



Roles and Responsibilities (Q16 – Q24)

The purpose of the Three Lines of Defense is to provide a simple and effective way to identify risk. To accomplish this, it requires clear roles and responsibilities. One of the many challenges of managing risk is determining who performs what function. This is where clearly established roles and responsibilities play an integral part in the effectiveness of managing risk. Some responsibilities solely reside within a dedicated department and can be considered First Line or Second Line of Defense. There can also be shared responsibilities between the First and Second Line of Defense. Based on the results of the survey, many of the tasks are shared or split between the First and Second Lines of Defense.

When asked if the First Line of Defense performs Second Line of Defense duties, 78% responded "no". The remaining 22% felt that the First Line of Defense performed Second Line of Defense duties. Risk frameworks and overarching policies are generally implemented at the oversight level and reside with the Second Line of Defense. Participants shared these examples as being performed in the First Line of Defense.

When asked if the Second Line of Defense performs First Line of Defense activities, 44% responded "yes". The remaining 56% did not feel the Second Line of Defense performed First Line of Defense activities. Ordinarily, the risk owner who resides in the business unit and First Line of Defense performs risk assessments and control testing. A repeated theme in the survey is Second Line performing the control testing and risk assessments.

Some examples include:

1st LOD performing 2nd LOD duties	2nd LOD performing 1st LOD duties
Compliance, HR, legal support	Drafting policies and procedures
Change management testing	Risk and Control assessments
Risk policies, governance, and frameworks	Control gap remediation
Reporting	Assessing 1st LOD risk
Stress testing	User access reviews
TPRM	Perform RCSA
Risk appetite designs	Control testing
Chief Information Security reports to 1st LOD	Risk monitoring and reporting

Challenges and Best Practices (Q25 – Q27)

Measuring success in risk management can be tangible and intangible. It is more than assessment and overlaps into risk culture. A risk committee plays a key role in measuring the success of a firm's risk program and maturity. Some institutions measure success by results from internal and external assessments while others measure by operating within their risk appetite. Effective challenge and collaboration between First and Second Lines is an example of intangible measurement. The following are examples of some institutions measuring success and effectiveness of the Three Lines of Defense.

- Regulatory feedback
- Successful audit exams
- Audit/Risk Committee reviews
- Level of engagement and knowledge of risk owners
- Clear roles and responsibilities

Participants were asked to share a successful best practice in maturing their Three Lines of Defense. The two most common themes were tone from the top and clear roles and responsibilities.

When asked to share a practice that has not worked as well as intended while maturing their Three Lines of Defense, the lack of clear communication and accountability were two repeated responses from the survey.

Works Well	Does Not Work Well
• Clarifying roles and responsibilities within policies and proceedures • Tone from the top - Executive leadership and Board Support • Transparency and communication with stakeholders • Accountability • Strong Risk Framework	• Not holding risk owners accountable • Duplicative task/control testing • Lack of clear and effective communication • Working in silos • No collaboration between risk and control partners