Deloitte.

12th Energy Industry Compliance Survey

Deloitte & Touche LLP | Energy & Resources

July 2024

We are pleased to present to respondents the results of
Deloitte's 12th Energy Industry Compliance Survey

We continue to strive to provide respondents with an effective method to get up to speed with the latest compliance trends and leading practices in the energy industry. The survey results are intended to provide insights into what your peers in the industry are doing to improve their compliance programs with an underlying objective to help you become more effective and efficient at proactively managing compliance risks. The survey results provide insights to help your organization in enhancing your enterprise's compliance programs.

The results represent the compilation of responses from 39 energy companies across the industry. The online survey was completed during the months of January 2024 through March 2024. The types of entities that responded include a range of companies across the power & utility, independent power producers, and oil and gas & sectors. Respondents include Chief Ethics and/or Compliance Officers, Senior Ethics and/or Compliance Directors, Compliance Specialists and Managers, and Associate/General Counsels. This report presents the collective results for all respondents and highlights year-over-year trends, where applicable. The survey results are aggregated and displayed as collective responses to preserve anonymity. This document is only shared with respondents and respondents can request for a detailed discussion of the potential implication of these results for their individual organizations. Please note that such discussions will continue to preserve the anonymity of respondents. The survey was hosted by Qualtrics, a secure, proprietary, survey service within Deloitte & Touche LLP. Deloitte & Touche LLP did not audit the responses from survey respondents for accuracy or validity nor did we benchmark the responses. These survey results are to be kept confidential and should not be shared without Deloitte's permission.

We hope you find the results of this year's survey insightful as you are leading your respective programs.
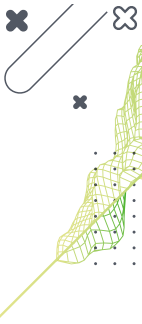
As the regulatory environment surrounding the energy industry continues to evolve, energy companies are expected to bolster and scale programs with adequate controls to proactively manage compliance risks from emerging areas. In the face of this shifting landscape, Deloitte Risk & Financial Advisory's Energy Industry Compliance Survey focuses on capturing insights into how organizations stay abreast of the evolving compliance environment across four key areas; (1) Compliance Program Governance, (2) Compliance Risk Assessments (CRA), (3) Information Governance (IG), and (4) Risk, Controls, and Assurance. The 2024 survey was carefully curated to highlight specific regulatory and compliance matters across these four major areas of interest. These areas were identified based on feedback and preferences of a subset of legacy survey respondents.

The following themes emerged across the four key areas and are echoed throughout this report:

- Organizations need to retain a holistic approach to their compliance management activities as emerging areas like Generative AI (GenAI) get integrated with traditional enterprise and regulatory compliance matters. Compliance organizations need to proactively balance the scope of CRAs to manage the increased share of emerging risk areas such as data privacy and cybersecurity with the traditional risk areas - without allowing traditional compliance program reviews to slip.

- Digitization on the operational and commercial front, with more widespread adoption of smart technology such as GenAI, has shifted how compliance approaches the risks associated with data and information management. Organizations are focusing on revamping policies and controls to accommodate digitization of information to reach maturity in IG programs, however much of the control infrastructure is still more manual in nature.

As risks facing the industry continue to grow and become more complex, especially in the current geo-political and socio-economic environment, we truly hope the insights captured through this survey help you keep a pulse on emerging ethics and compliance developments enabling you to power up growth and performance.

Sincerely,

Howard Friedman

Howard Friedman
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
hfriedman@deloitte.com

Holly Wenger
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
howenger@deloitte.com

Connor Murphy
Senior Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
connmurphy@deloitte.com

Overview

Respondent demographics

Compliance and ethics program governance

Compliance risk assessments

Information governance

Risk, controls, and assurance

Selecting the icons on this page will take you to the respective section.
You can also use the arrows in the bottom left-hand of the page to navigate throughout the report.

Power & utilities	Independent power producer	Oil & gas company	Other*
72%	13%	5%	10%
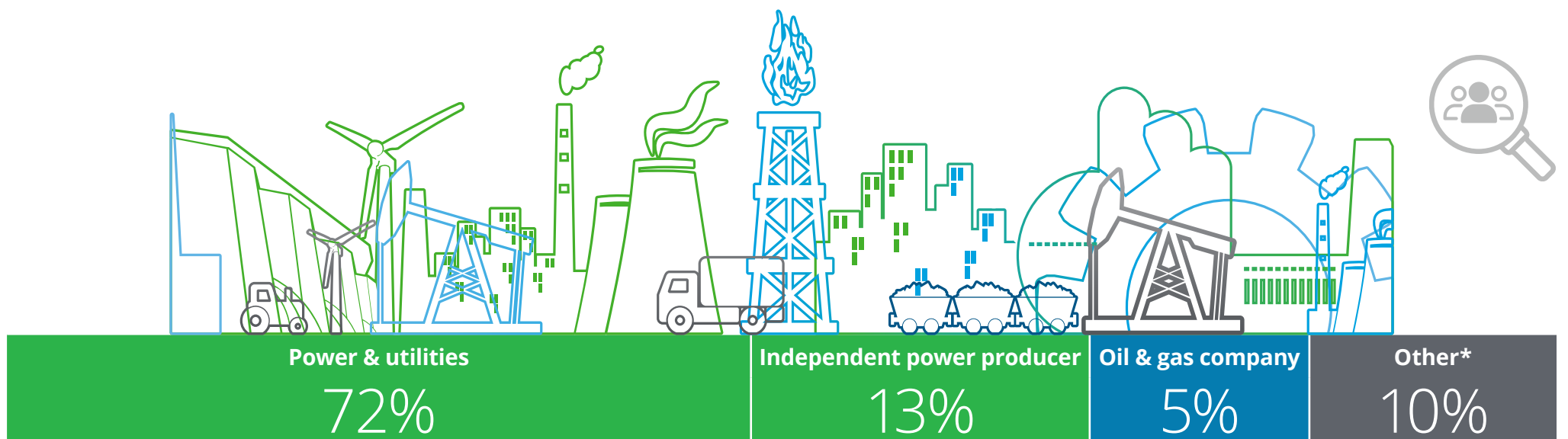
Power & utility service offerings

Service	%
Power generation, transmission and distribution	85%
Gas generation, transmission and distribution	44%
Generation, transmission and distribution for water and other utilities	4%
Nuclear power	37%
Renewable energy and energy storage	70%
Others include, but not limited to: transmission, distribution, and power generation	11%

N = 39
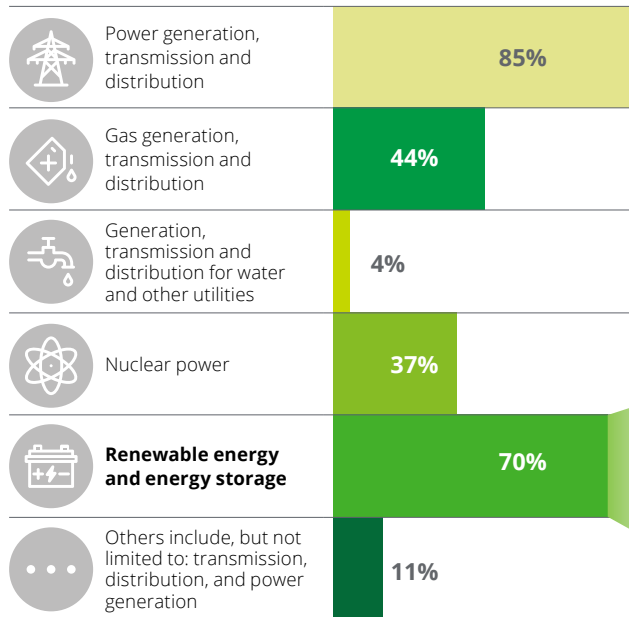
Generating portfolio overview

- 3%
- 16%
- 28%
- 44%
- 9%

- Less than 1,500 Megawatts (MW)
- Between 1,500 and 5,000 MW
- Between 5,000 and 10,000 MW
- More than 10,000 MW
- Do not own generating assets
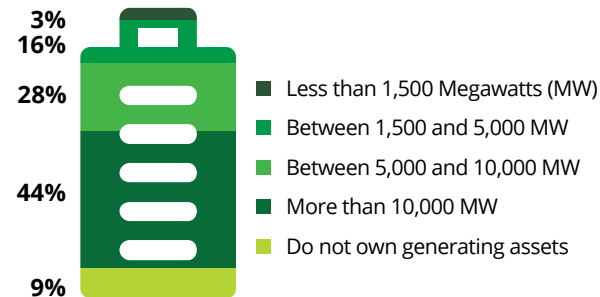
Renewable energy technology offerings

- Solar **95%**
- Energy Storage **53%**
- Wind **79%**
- Geothermal **11%**
- Hydropower **84%**
- Other **11%**
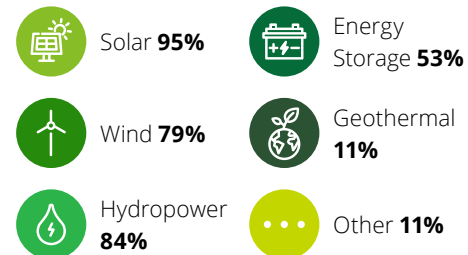
No respondents participate in the **upstream value chain**

50% of respondents participate in the **midstream value chain** operating between 2,000 and 3,000 miles

50% of respondents participate in the **downstream value chain** and have refinery capacity of more than 200,000 barrels of oil per day

*Others include, but not limited to:
- Transmission and distribution
- Trading around assets/Asset optimization

5

Applicable energy regulators

Types of energy regulators*

43% **Nuclear Regulators**
(e.g., Nuclear Regulatory Commission (NRC);
Institute of Nuclear Power Operations (INPO))

96% **Accounting & Financial Regulators**
(e.g., Internal Revenue Service (IRS))

93% **US Government Agencies**
(e.g., Department of Energy (DOE);
US Department of Agriculture)

93% **Cybersecurity Regulators**
(e.g., Cybersecurity and Infrastructure
Security Agency; Payment Card Industry
Data Security Standard (PCI DSS))

79% **Transportation Regulators**
(e.g., Transportation and Security
Administration (TSA); Federal
Aviation Authority(FAA))

100% **Electric Regulators**
(e.g., Edison Electric Institute;
North American Electric Reliability
Corporation (NERC))

79% **Telecommunications Regulators**
(e.g., Federal Trade Commission
(FTC); Federal Communications
Commission (FCC))

79% **Industrial & Engineering Regulators**
(e.g., US Corps of Engineers;
American National Standards
Institute (ANSI))

100% **State Regulators**
(e.g., State Departments of Labor;
State Commerce Commissions)

100% **Labor Regulators**
(e.g., Human Rights Commission
(HRC); Occupational Safety and
Health Administration (OSHA))

75% **Gas & Pipeline Safety Regulators**
(e.g., American Gas Association;
Pipeline and Hazardous Materials
Safety Association (PHMSA))

21% **Other***

N = 28

*Others include, but not limited to:
- Municipalities
- Local governmental agencies
- Canadian,
- Regulators for those noted above
  as well as competition regulators.
- SEC
- DOJ
- FERC
- State Regulatory Commissions

Number of energy regulators

Category	Value
Fewer than 10 regulators	8%
10 - 20 regulators	24%
20 - 30 regulators	8%
30 - 40 regulators	8%
40 - 50 regulators	6%
More than 50 regulators	35%
Unsure	11%

N = 37
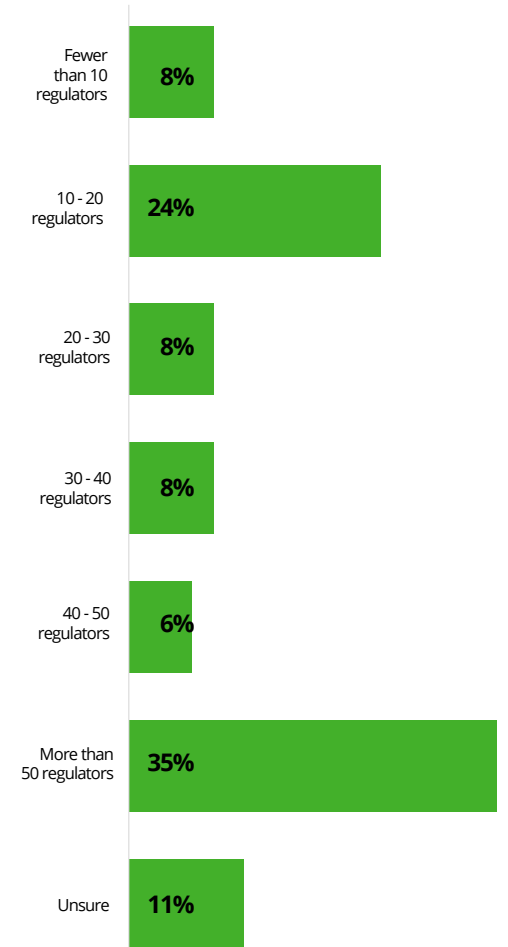
Respondents were asked to select all applicable options.

Annual revenue

5%
8%
22%
24%
41%

- Less than $250 Million
- Between $250 Million and $1 Billion
- Between $1 Billion and $5 Billion
- Between $5 Billion and $15 Billion
- More than $15 Billion

N = 15
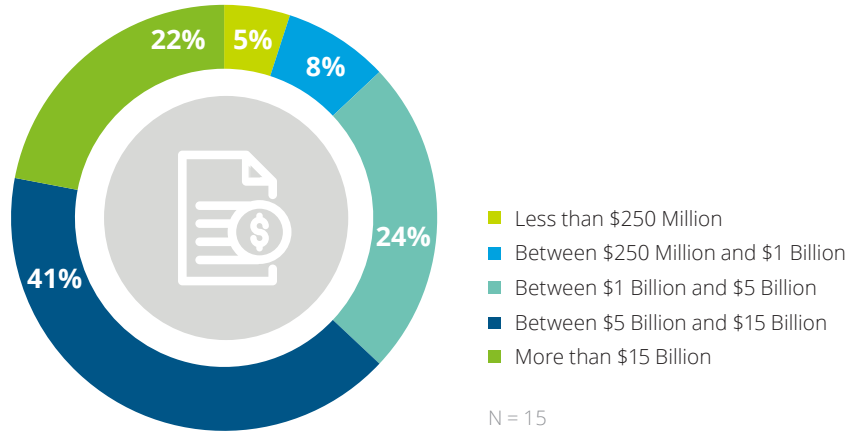
Annual operating income

5%
8%
8%
32%
46%

- Less than $250 Million
- Between $250 Million and $1 Billion
- Between $1 Billion and $5 Billion
- Between $5 Billion and $15 Billion
- More than $15 Billion

N = 37

Employee headcount

17%	14%	14%	24%	32%
Less than 1,000 employees	Between 1,000 and 3,000 employees	Between 3,000 and 5,000 employees	Between 5,000 and 10,000 employees	More than 10,000 employees

N = 37

Operational footprint

Respondent demographics
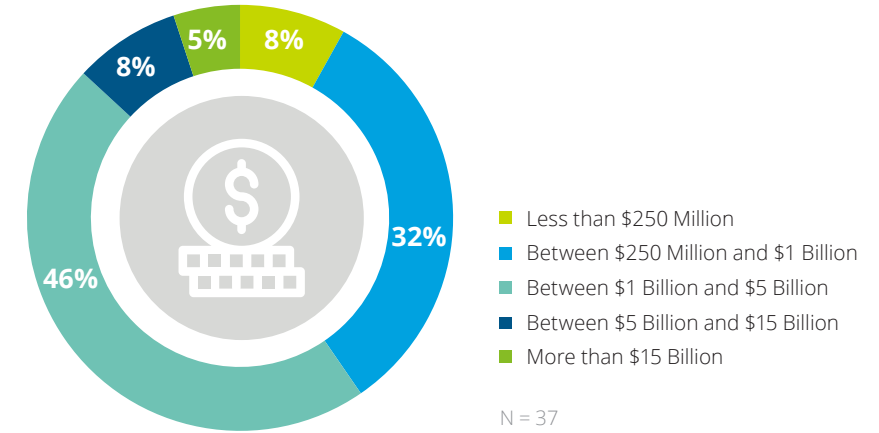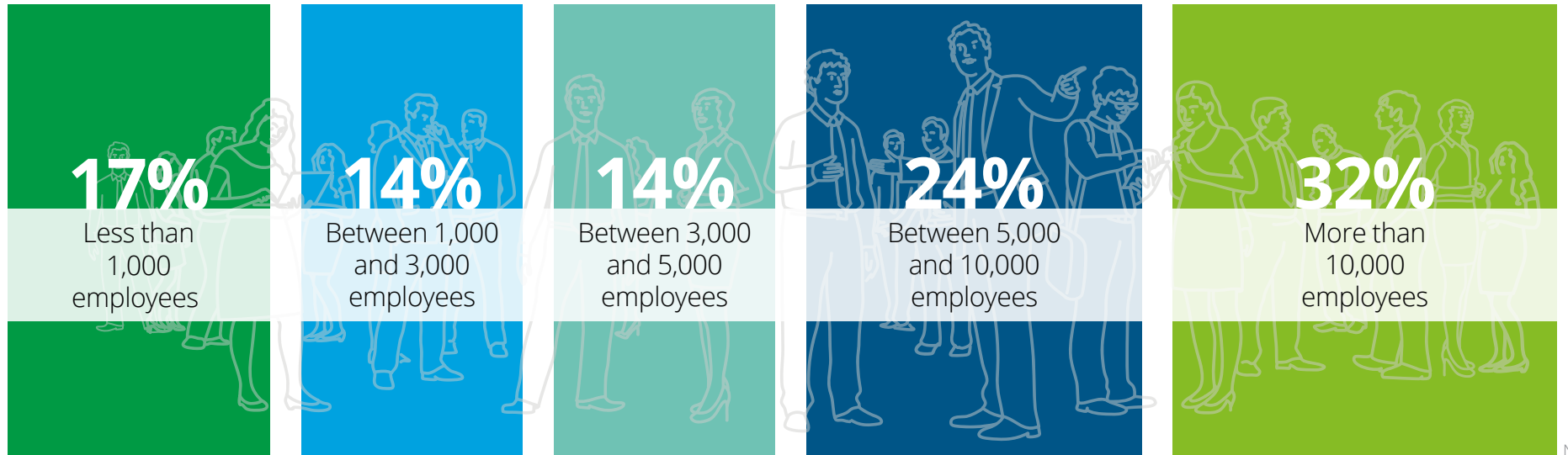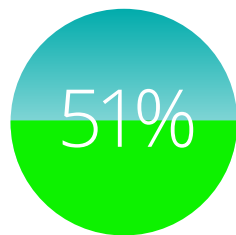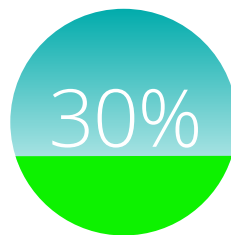
51%	30%	14%	3%	3%
Domestic in the US only	Domestic and international (beyond Canada and the US)	Across Canada and the US	Domestic in Canada only	International only
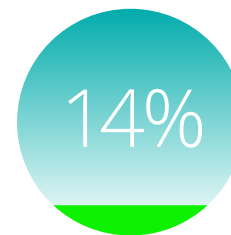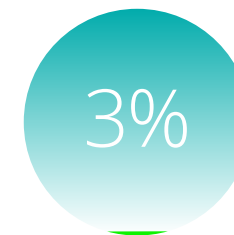
US map percentages: 13%, 17%, 8%, 21%, 29%, 17%, 17%, 17%, 21%, 17%, 21%, 29%, 13%, 21%, 17%, 8%, 13%, 29%, 25%, 33%, 25%, 38%, 8%, 8%, 8%, 17%, 25%, 13%, 29%, 42%, 17%, 21%, 21%, 8%, 17%, 17%, 25%, 25%, 25%, 17%, 13%, 17%, 21%, 21%, 25%, 13%, 8%, 50%, 29%, 13%, 4%

Canada map percentages: 50%, 33%, 17%, 17%, 50%
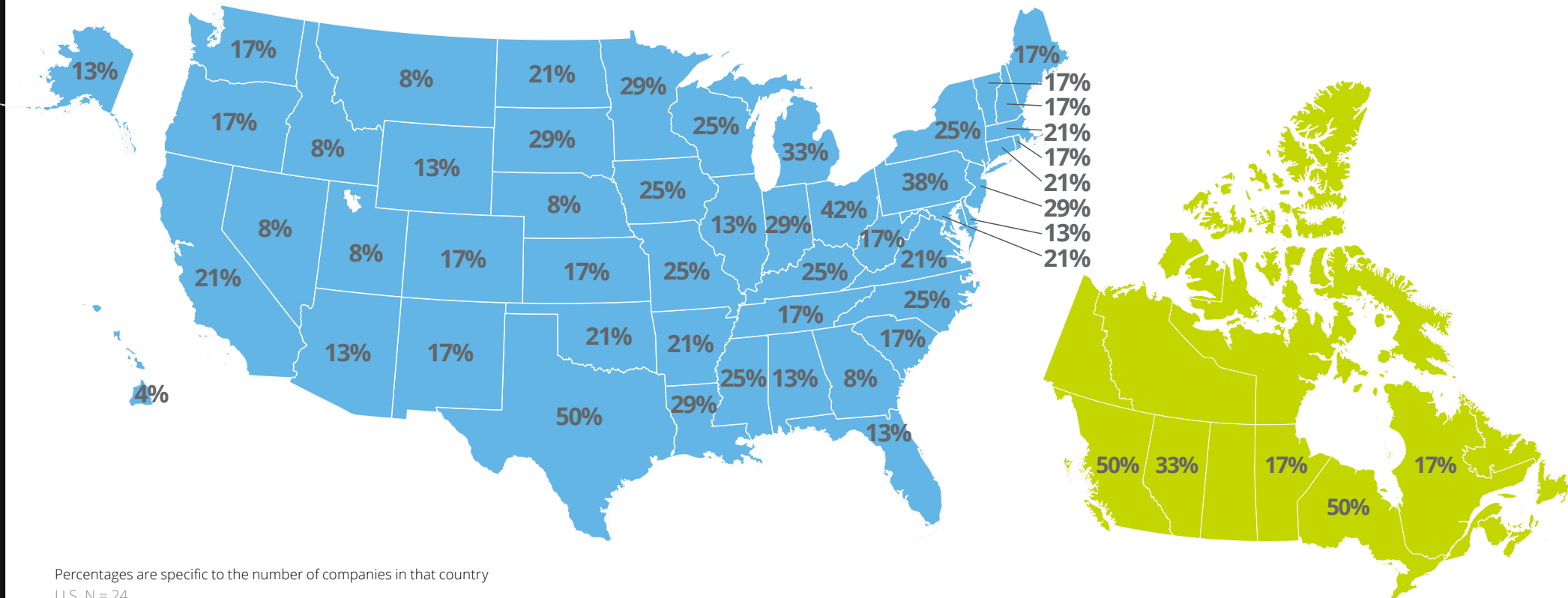
Percentages are specific to the number of companies in that country
U.S. N = 24
Canada: N = 10

Respondents were asked to select all applicable options.

8

This section focuses on compliance program governance, reporting, resources and metrics. The questions distinguish between enterprise and regulatory compliance in recognition that they may be separate within many organizations. For purposes of this survey, enterprise compliance is defined as the coordinated approach to ethics and compliance program design and assessment that cuts across multiple business units within an organization. Regulatory compliance is defined as the design, assessment and oversight of processes, controls, and infrastructure that are in place to support targeted business unit level compliance obligations.

Compliance and ethics program governance

Key takeaways:

At 73% of organizations, the Chief Compliance Officer (CCO) takes on **additional leadership roles**, such as acting as the General Counsel, Chief Risk Officer or another position. Other roles taken on by CCOs include Chief Sustainability Officer, Corporate Secretary, and Chief Financial Officer, among others.

The most **common responsibilities of the enterprise compliance function** are compliance training (92% of organizations), issue escalation and reporting (86%), code of conduct (81%), and compliance strategy processes (81%).

Compliance related metrics that boards of directors and audit risk committees found **most valuable** were results from risk and maturity assessments at an enterprise level, internal and external audit findings, compliance management metrics (scorecards, dashboards, KPIs, Code of Conduct compliance metrics, etc.), and incident management metrics (number of incidents, rate of incident reporting, anonymous reporting rate, etc.).
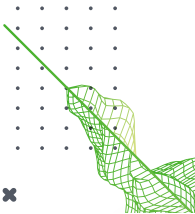
Compliance program overview

At least 90% of respondents continue to have a largely centralized or mixed structure for their enterprise compliance and ethics program. There is a noticeably increasing shift in respondents' regulatory compliance programs toward a mixed oversight model, indicative of a more collaborative management approach between enterprise compliance and business units.

Enterprise compliance organizational structure

	Largely centralized	Mixed	Largely decentralized
Enterprise compliance	15% / 41% / 32%	67% / 47% / 59%	18% / 12% / 8%
Regulatory compliance	16% / 50% / 14%	48% / 45% / 65%	36% / 5% / 22%

Largely centralized
Refers to a centralized function, under the oversight of a single senior leader who provides oversight over the majority (or all) of applicable compliance activities

Mixed
Such that certain unique areas are overseen centrally, while several areas are handled in a decentralized way

Largely decentralized
With the majority (or all) of compliance oversight being handled by various separate functions within the company

■ **2020** ■ **2022** ■ **2024**

Ethics governance model

- **70%** Ethics is combined with enterprise compliance
- **5%** Ethics is part of Internal Audit
- **11%** Ethics is part of Human Resources
- **8%** Ethics is a stand-alone function
- **5%** Other

N = 37

10
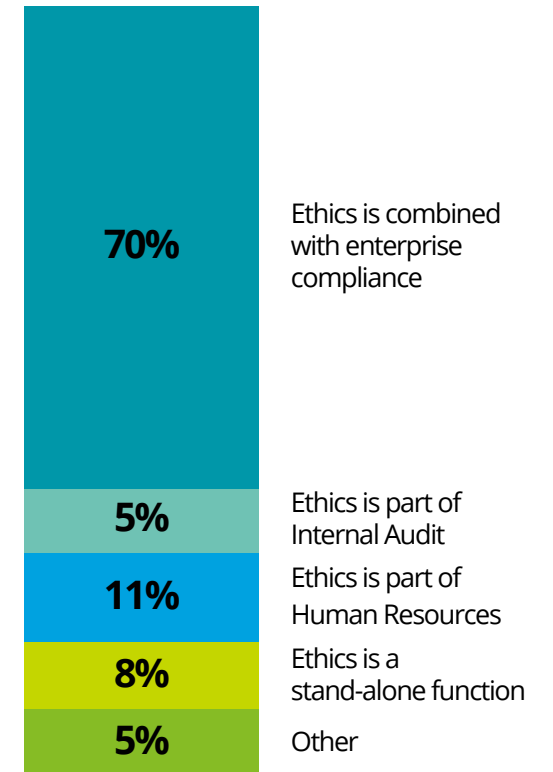
Compliance program overview *continued*

Budget for enterprise-wide compliance functions year over year
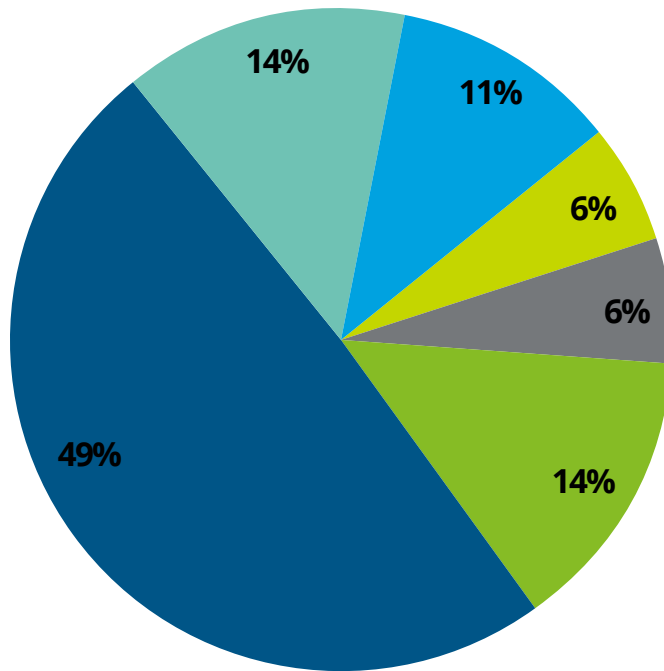
2024

Legend:
- $10 million or more
- $5 Million - $6.99 Million
- $3 Million - $4.99 Million
- $1 Million - $2.99 Million
- $500,000 - $999,999
- Less than $500,000

N = 35

2024 values: 14%, 11%, 6%, 6%, 14%, 49%
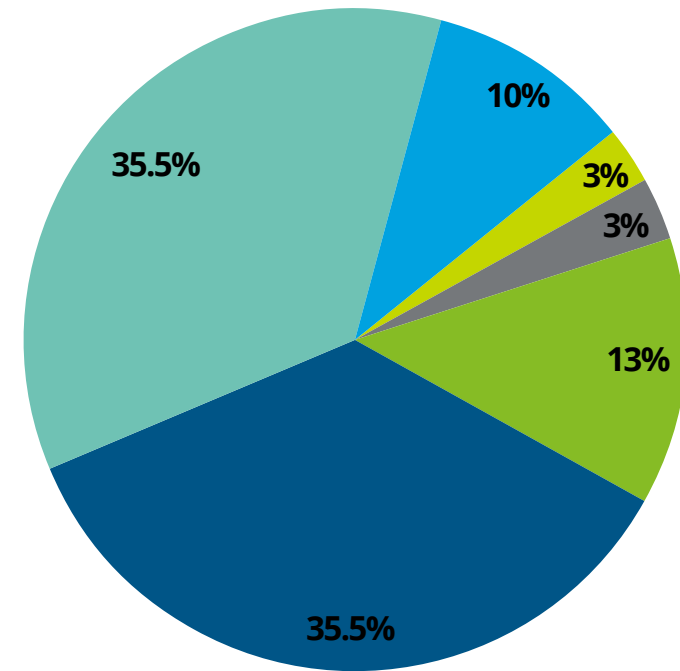
2022

Legend:
- $10 million or more
- $5 Million - $6.99 Million
- $3 Million - $4.99 Million
- $1 Million - $2.99 Million
- $500,000 - $999,999
- Less than $500,000

N = 31

2022 values: 35.5%, 10%, 3%, 3%, 13%, 35.5%

Note that not all respondents responded to this question.

Chief Compliance Officer responsibilities

The following provides an overview of responsibilities and reporting lines of Chief Compliance Officers.

CCO responsibilities*

27% of respondents have a designated stand-alone CCO position, a 15% decrease from the last survey, indicating a shift in expanding the responsibilities of compliance officers across the industry.

Category	Percentage
Also the General Counsel	30%
A stand-alone position separates from another function	27%
Also the Chief Risk Officer	11%
Also the Chief Audit Executive	3%
Other**	32%
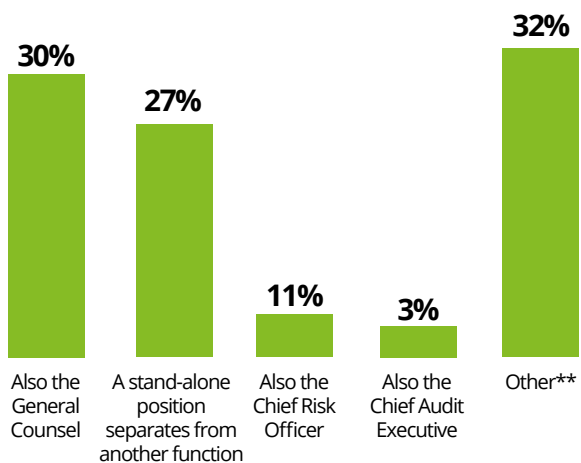
**Others include, but not limited to:
- Ethics
- Legal
- CFO
- Corporate Secretary
- Labor & Employment
- SVP, Safety
- SVP, Planning and Operations
- No CCO

N = 38   *Respondents were asked to select all applicable options.

CCO reporting lines

Under half of responding organizations' CCOs report directly to the CEO, giving compliance a direct line to the highest company leadership.

Category	Percentage
Chief Executive Officer	44%
General Counsel	33%
Board or a board committee	6%
Chief Risk Officer	3%
Chief Financial Officer	3%
Other***	11%
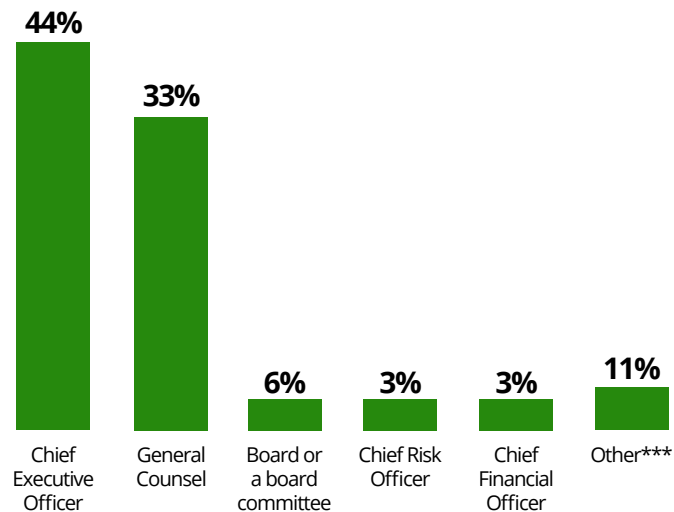
*** Others include, but not limited to:
- Executive Vice President of Compliance, Audit, ERM, and Chief Legal Officer
- Executive Vice-President and Chief External Affairs and Sustainability Officer, Chief Strategy and Sustainability Officer

N = 37

CCO representation on Executive Management Committees

Over half of responding companies' CCOs hold a seat on the Executive Management Committee (EMC).

Category	Percentage
Yes	54%
No	38%
Not applicable / don't know	8%

N = 36

12
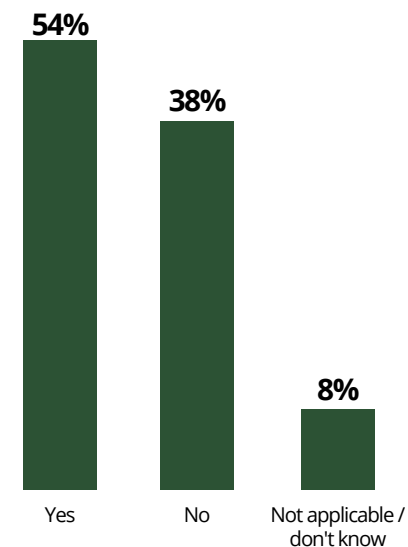
Executive compliance committee

Compliance committees of responding organizations are comprised of C-suite, Senior Vice President and President level representatives. One-third of respondents do not have an executive compliance committee. Compliance committees at almost 80% of the respondent companies meet quarterly.

Executive compliance committee composition*

- Officer: **47%**
- Senior Vice President: **56%**
- Vice President: **56%**
- Manager: **24%**
- Director: **38%**
- No executive compliance committee exists: **26%**
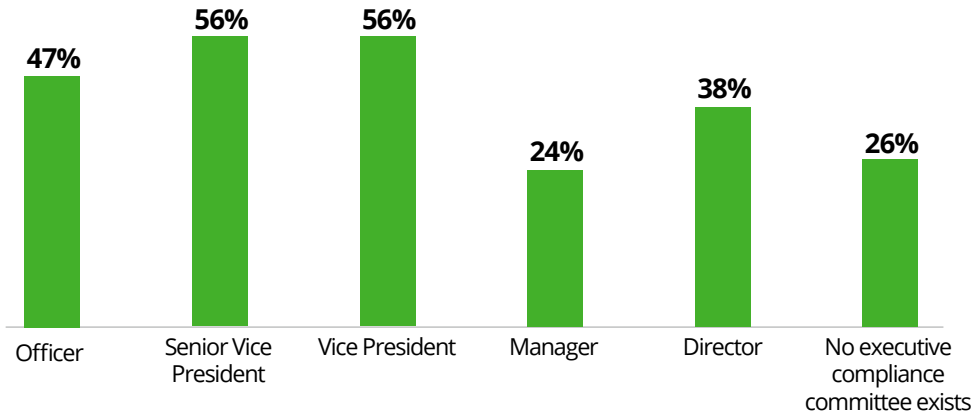
Executive compliance committee cadence

	2024	2022
Monthly	15%	13%
Quarterly	78%	74%
Bi-annually	4%	4%
Annually	0%	0%
No executive compliance committee exists	4%	9%

■ 2024 **■ 2022**
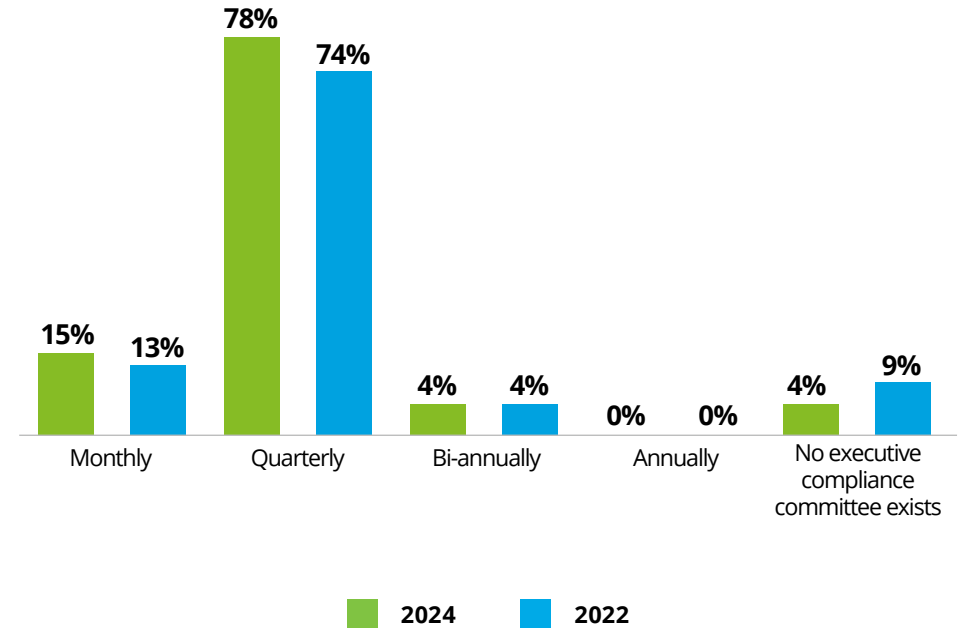
*Respondents were asked to select all applicable options.

N = 34

N = 27

13

Executive compliance committee *continued*

Emergent and priority issues and compliance management activities continue to be considered the most beneficial topics discussed at executive compliance committee meetings. With a strong desire to include discussions on leading practices of compliance programs in the industry and opportunities to enhance culture and prevention of future non-compliance events, organizations are concentrating on forward-looking topics to prepare compliance programs for what's to come.

Leading Executive Compliance Committee meeting topics

Topic	2024	2022
Dealing with emergent and priority issues (e.g., workplace harassment, data privacy)	63%	64%
Compliance management activities including, but not limited to, metrics, KPIs, maturity and program reviews, risk assessment results, communications, and trainings	67%	55%
Understanding trends and sharing leading practices within the organization	50%	39%
Governance and decision-making activities including, but not limited to, risk management, resource management, and strategic direction	40%	39%
Discussion on root cause and resolution of complex, cross-functional compliance issues requiring subject matter expertise	37%	30%
Impact analysis of upcoming regulations and compliance obligations within the industry	33%	27%
Not applicable	7%	27%

■ 2024 ■ 2022

Additional valuable Executive Compliance Committee meeting topics not currently discussed

Topic	%
Opportunities to enhance culture and prevention of future noncompliance events	48%
Leading practices for compliance programs in industry	45%
Perform gap assessment to identify enterprise-wide compliance items with no direct owner	34%
In-depth discussion of root cause analysis	31%
In-depth discussion of compliance issue resolution	31%
In-depth discussion of the preventability of past compliance issues	31%
Regulatory issues affecting key business units	21%
Current performance of the compliance program	10%
Other	10%
Identification for enterprise-wide compliance area ownership	7%

N = 30

Respondents were asked to select all applicable options.

CCOs' compliance program reporting priorities for board and/or executive management

Compliance violations, emerging compliance risks, compliance program structure and performance metrics appear to be the top priority items that Chief Compliance Officers report to their board and/or executive management.

Leading types of compliance program reporting*

89%
Compliance violations

89%
Structure and performance of the compliance program

86%
Information on emerging compliance risks

78%
Regulatory fines and penalties

76%
General reports on ethics and culture

70%
Compliance performance metrics

70%
Information on new laws and regulations

65%
Compliance issue resolution tracking status

62%
Results of regulatory compliance auditing or examinations

46%
Employee disciplinary actions

30%
Budget concerns

14%
Other**

3%
None or Not Applicable / don't know

N = 37

*Respondents were asked to select all applicable options.

**Others include, but not limited to:
· Enterprise Risk Management
· FERC SOC training to the Board

Compliance program reporting cadence

	Monthly	Quarterly	Bi-annually	Annually
2024	8%	75%	8%	8%
2022	9%	67%	12%	12%

2024
2022
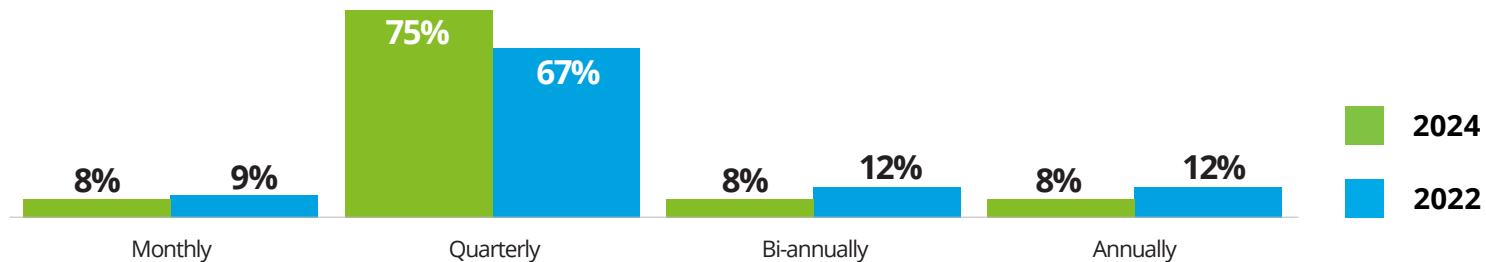
N = 36

Enterprise compliance program reputation

61% of respondents feel heir company characterizes the enterprise compliance organization as a centralized compliance function that acts as an oversight authority or a coordination and administrative support function.

36%

A centralized compliance oversight authority

40%

25%

A centralized compliance coordination and administrative support function

33%

33%

A strategic advisory and enabling function for compliance matters

18%

6%

Other*

9%

2024

2022
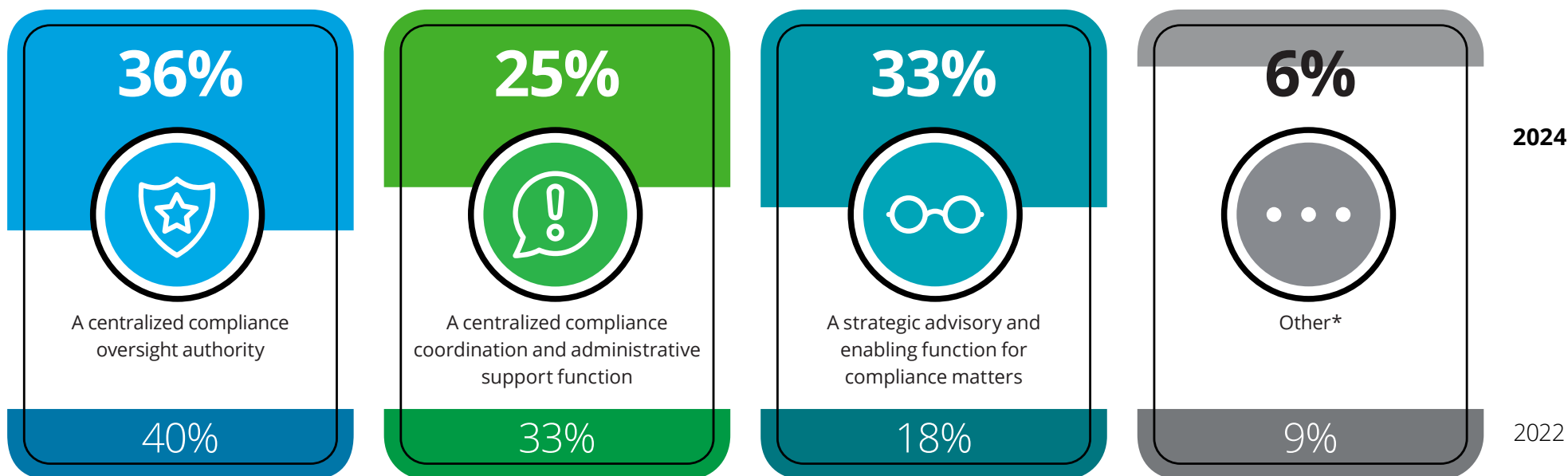
*Others include, but not limited to:
- Audit function requiring additional resources resulting in overhead
- Burden and a decentralized network of subject matter experts

N = 36

Business partner perception of compliance functions

97% of respondents indicated that the compliance function is viewed as a business partner, at least in certain aspects at their respective organizations. This sentiment aligns with previous survey responses.

Yes, in certain aspects

51%	**50%**

Yes, across the entire organization

46%	**47%**

Not Applicable

3%	**3%**

2024   2022

N = 37   N = 34

Select options from historical years are presented in the graphic above. Complete data can be found in historical Deloitte & Touche LLP Regulatory and Compliance Surveys.
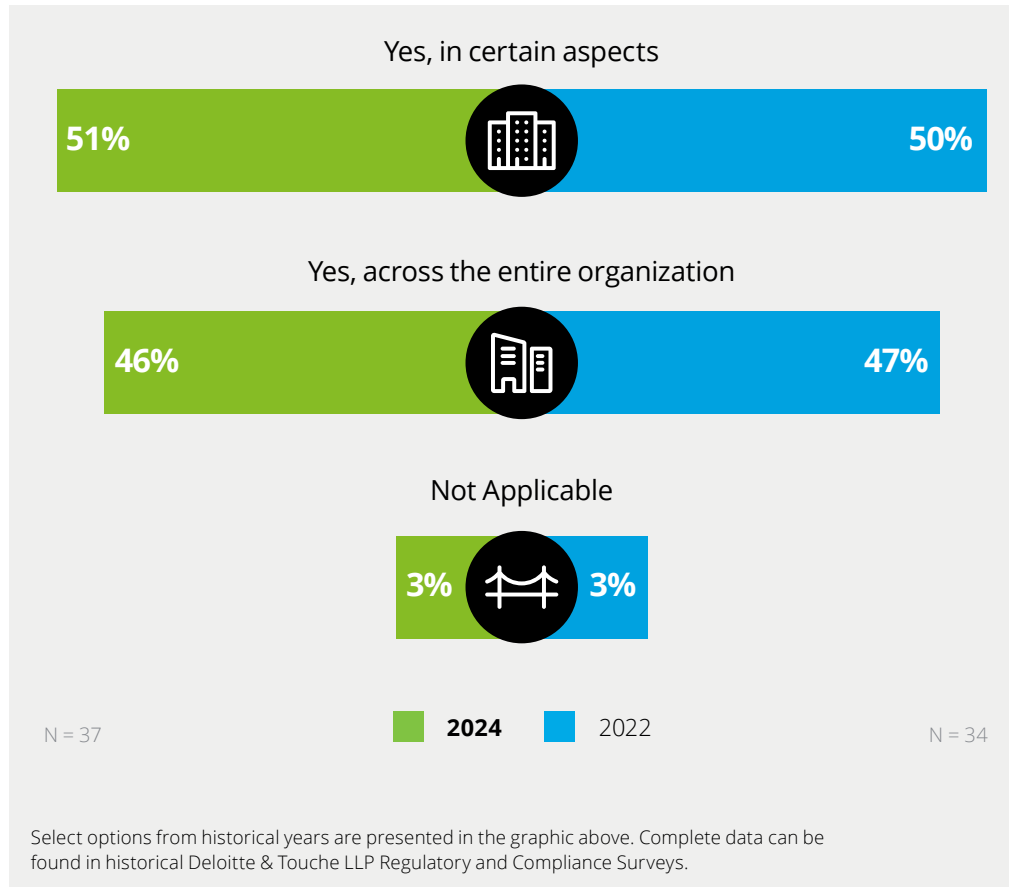
Select characteristics that fostered compliance to be viewed more as a 'business partner'

Compliance laws and regulations are engrained within the DNA of companies

Partnership with appropriate functions across the organization

Senior management support

Established relationships with SMEs in the business areas and designated contacts (e.g., Records Coordinators, Data Privacy Coordinators)

Ethics and Compliance maintains a business partnership model that is intended to increase stakeholder engagement, support, and collaboration with our internal customers, and increase customer visibility into the E&C function

Direct reporting to CEO, identified compliance liaisons across functional business areas, monthly officer-level compliance operating review

Embedded compliance personnel in relevant business areas

New organization that is working to embed ethics and compliance into the company's culture

Regulatory change management, issue assessments, and risk and controls framework are well integrated

Compliance review and enablement of new technologies or projects, such as leveraging GRC to digitize and add efficiencies to the business

Compliance resource management

Compliance programs with 5+ FTE are largely the same size on average, while smaller programs appear to have expanded personnel slightly.

Enterprise compliance resourcing

	2024	2022	2020
	N = 37	N = 33	N = 44

More than 20 FTEs: 19% (2024), 21% (2022), 14% (2020)

11-20 FTEs: 10% (2024), 9% (2022), 14% (2020)

5-10 FTEs: 33% (2024), 34% (2022), 34% (2020)

1-4 FTEs: 35% (2024), 30% (2022), 27% (2020)

Less than 1 FTEs: 3% (2024), 6% (2022), 9% (2020)
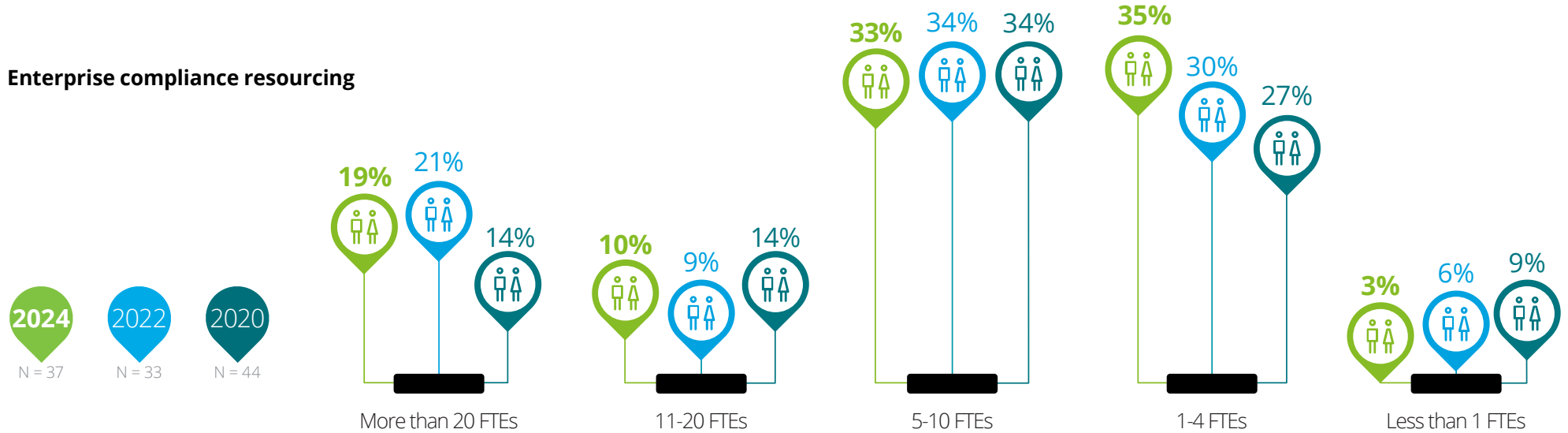
Compliance function responsible areas*

Area	%
Compliance training	92%
Issue escalation and reporting	86%
Code of conduct	81%
Compliance strategy processes	81%
Complaints and whistleblower hotlines	78%
Regulatory and internal compliance investigations	78%
Ethics program	78%
Enterprise-wide compliance risk assessment processes	76%
Conflicts of interest	70%
Establishing and monitoring standards for business conduct	70%
Policy management	68%
Advisory of emerging regulatory issues	59%
Anti-bribery, anti-corruption and anti-fraud programs	59%
Independent compliance monitoring and testing	54%
Communications	49%
Culture Assessment	43%
Monitoring resolution of audit and regulatory findings	43%
Regulatory filings and reports	43%
Records and information management	41%
Privacy programs	32%
Regulatory relationship management	27%
Third-party compliance management / mitigation	24%
Anti-money laundering programs	22%
Other**	8%

N = 34

*Respondents were asked to select all applicable options.

**Others include, but not limited to: Global Trade Compliance, Harassment, Discrimination, Workplace violence.

18

Compliance expertise and qualifications

The following presents a comparative view on expertise and qualifications applicable to enterprise vs. regulatory compliance resources. 'Regulatory Compliance' and 'Legal' remain the primary expertise and qualifications for both enterprise and regulatory compliance at a majority of responding organizations. From an enterprise compliance perspective, the noteworthy expertise identified through the survey includes training and communications, Governance, Risk and Compliance (GRC) tools, Internal Audit/Controls, data analytics, and reporting. These are reflective of the compliance activities being driven in a more centralized manner from enterprise compliance functions.

92%	91%	67%	61%	64%	39%	75%	70%	56%	36%	53%	39%
Regulatory Compliance		Training and Communications		GRC tools		Legal		Ethics		Internal Audit / Controls	

53%	36%	61%	30%	25%	24%	53%	39%	11%	9%
Data Analytics and Reporting		Enterprise Risk Management		Human Resources		Technical Operations		Other*	
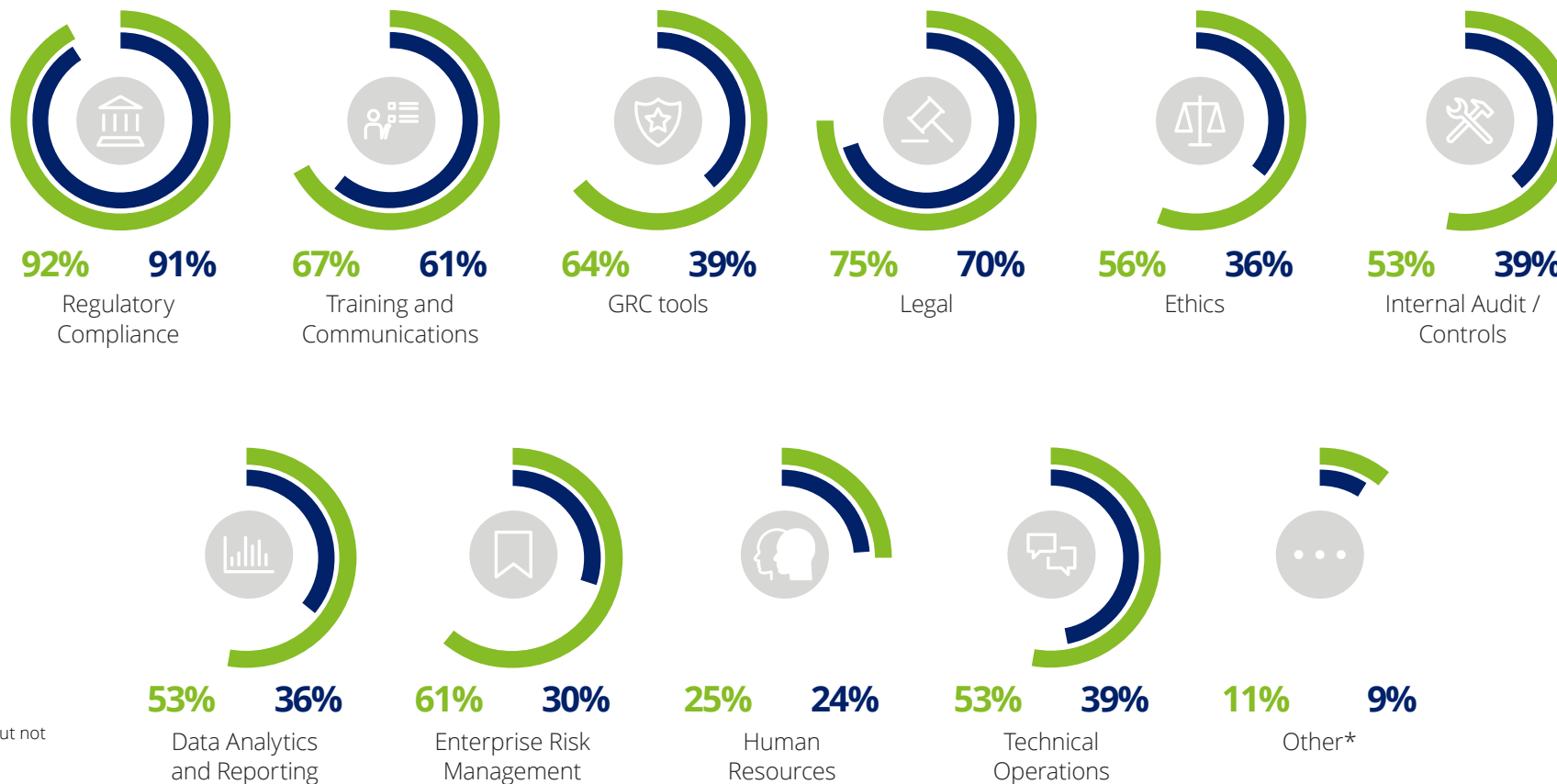
*Others include, but not limited to:
- Investigations
- Operational
- Cyber, Accounting & Engineering

N = 33

◼ **Enterprise compliance**   ◼ **Regulatory compliance**

Respondents were asked to select all applicable options.

19

Enterprise compliance expertise and qualifications

The following presents a comparative view of the expertise and qualifications of the enterprise compliance resources year over year. This comparison demonstrates significant overlap between the compliance aspects areas such as "Regulatory Compliance" and "Ethics." It also shows that there are areas that are more tailored to either enterprise or regulatory compliance such as "Technical Operations" and "Human Resources".

75% **85%**
Regulatory Compliance

67% **76%**
Legal

83% **82%**
Ethics

44% **N/A**
Cyber

58% **58%**
Enterprise Risk Management

28% **36%**
Human Resources

42% **45%**
Technical Operations

11% **12%**
Other*
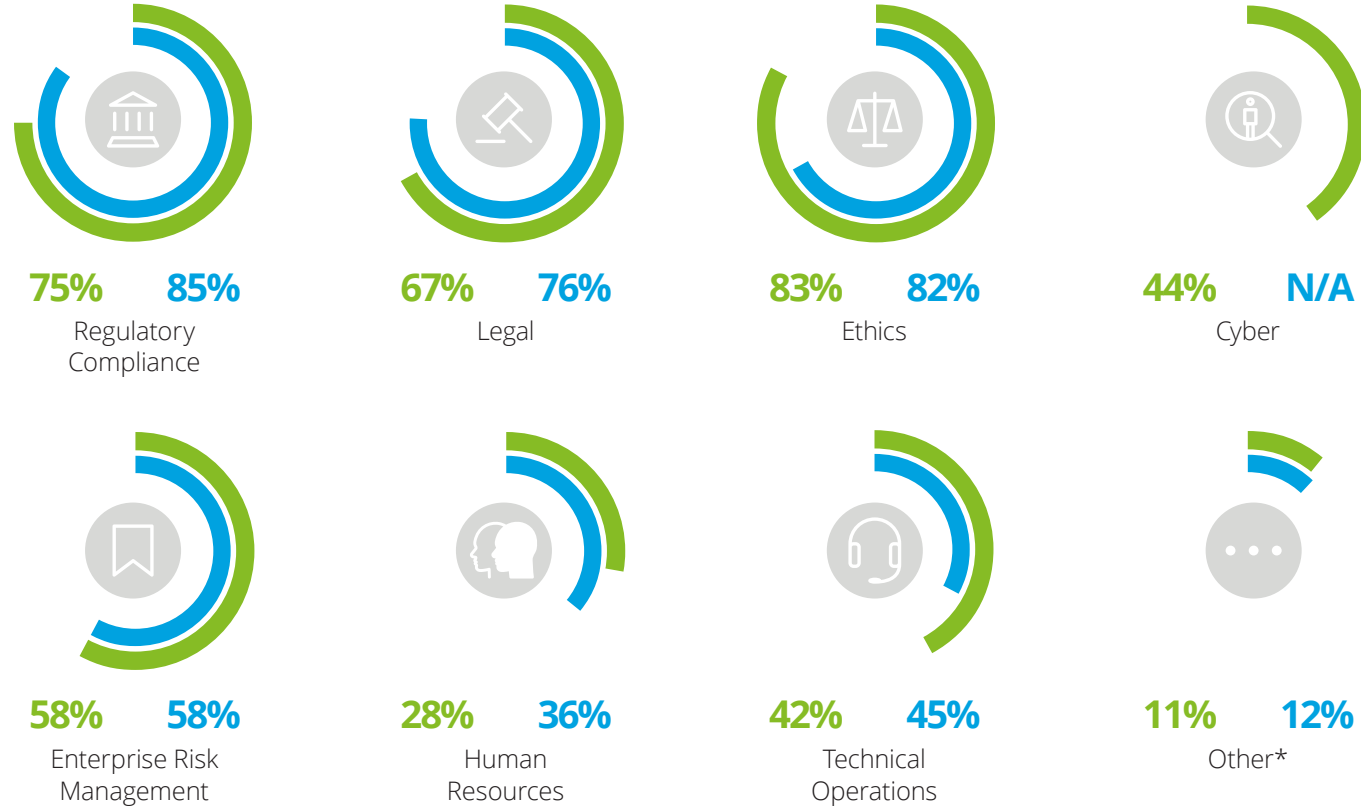
*Others include, but not limited to:
- Diversity, Inclusion, and Equity; Learning Management Systems
- Corporate Culture, Customer Service, Labor Relations
- Corporate governance
- Investigations

N = 36

■ **2024**   ■ **2022**

Respondents were asked to select all applicable options.

20

Enterprise compliance desired skill sets

The following shows the skillsets that our respondents responded would be the most beneficial if they had the opportunity to increase their enterprise compliance headcount. "Analytics and Data Science" continued to be in high demand, likely because of the increasing prevalence of large data sets that provide the opportunity for new insights. The largest change in our respondents came in technology central areas, and we are now tracking "Cyber" and "Information Technology" to follow this trend in the future.

53% **58%**
Analytics and data science

44% **45%**
Culture and change management

42% **27%**
Technology and digital transformation

31% **27%**
Root cause analysis

31% **24%**
Understanding of legal and regulatory requirements applicable to the organization

28% **12%**
Technical / commercial operations

25% **30%**
Strong deadline and outcome-oriented project or program management skills

25% **9%**
Audit and assurance frameworks and practices

22% **24%**
Forensic analysis

22% **9%**
Customer-centric and customer satisfaction mindsets focused on internal stakeholders

22% **24%**
Training, learning, and knowledge management

19% **18%**
Enterprise risk management

19% **30%**
Agile, scrum, creative / design thinking, and other innovative practices

17% **0%**
Information Technology*

8% **0%**
Cyber*

3% **0%**
HR compliance*

*These skillsets were not included in the 2022 survey.

N = 36

2024

2022

Respondents were asked to select all applicable options.

21

Regulatory Compliance Desired Skill Sets

Survey respondents' demonstrate a range of preferences for desired skill sets specific to regulatory compliance. Contrary to what may be considered desirable in the past, respondents favored attributes like analytics, technology and GenAI. GenAI's prominent role on this list shows that it is not strictly a tool of the distant future, but rather something that is on the top of many of our respondents' minds.

53% **33%**
Understanding of legal and regulatory requirements applicable to the organization

42% **45%**
Analytics and data science

42% **30%**
Technology and digital transformation

33% **12%**
Audit and assurance frameworks and practices

31% **24%**
Root cause analysis

28% **24%**
Culture and change management

25% **27%**
Training, learning, and knowledge management

36%
GenAI*

*This skillset was not included in the 2022 survey.

28% **27%**
Technical / commercial operations

22% **21%**
Enterprise risk management

11% **15%**
Forensic analysis

8% **18%**
Agile, scrum, creative / design thinking, and other innovative practices

2024 N = 36   2022 N = 33

2024   **2022**

Respondents were asked to select all applicable options.

Leading indicators for compliance program effectiveness

Respondents rely on a mix of evaluation methods, the most common being self-assessments, compliance training completion rates, and external evaluations. 81% of respondents are at least somewhat confident in their programs' current measurement method.

Compliance program effectiveness evaluation methods

Method	%
Analysis of self-assessment results	53%
Completion rates for required compliance training	50%
Independent evaluations by outside counsel and/or consultants	47%
Analysis of internal audit findings	44%
Hotline call analysis	44%
Feedback from employee ethics surveys	42%
Disposition of internal investigations	42%
Analysis of regulatory reviews	33%
Size of regulatory fines or penalties	31%
Comparisons to competitors or similar organizations	31%
Exception rates in compliance testing activities	11%
Other	8%

Level of confidence in evaluation methods*

- **42%** Confident
- **39%** Somewhat confident
- **6%** Very confident
- **8%** Not confident
- **6%** Not applicable/don't know

N = 34

N = 34   *Respondents were asked to select all applicable options.

23

Compliance risk assessments
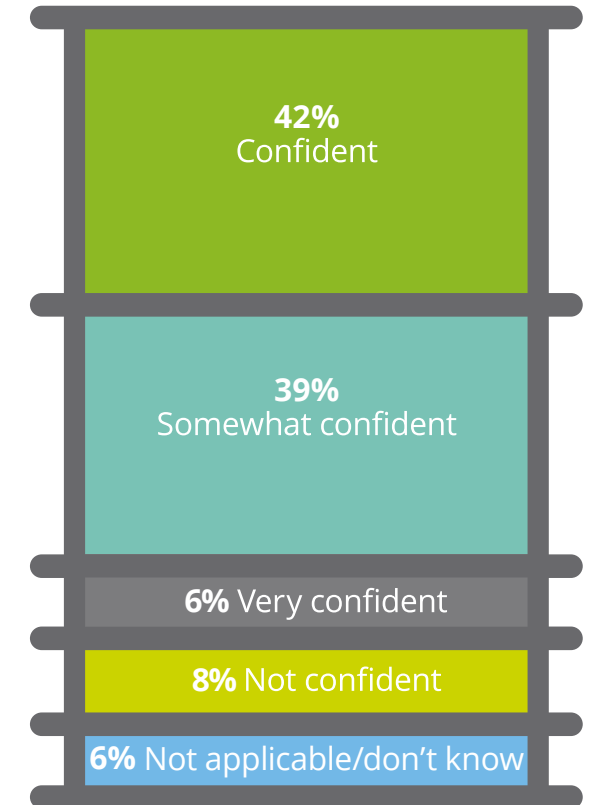
This section is focused on Compliance Risk Assessments (CRAs), which are frameworks and methodologies used identify and understand key regulatory risks for an organization. A component of larger risk management efforts, CRAs serve as a methodical procedure for discovering, evaluating, and ranking legal and regulatory risks that could harm an organization. The information in this section covers frequency, scoring, granularity, and risk areas of the CRA, as well as the process surrounding the CRA within the organization.

Key takeaways:

About half of organizations **report an annual cadence** for their CRAs, with 20% of organizations not having any set frequency, and 11% never conducting this type of assessment.

The **most common risk areas** covered in CRAs at these organizations are **anti-corruption/bribery, environmental risks, conflicts of interest, cybersecurity, and health/safety**. Compliance risk areas most commonly considered at these organizations are reputational risk, legal risk, and financial risk.

Less than 40% of participating organizations leverage a **dedicated tool or product** for CRAs at their respective organizations.

CRA framework

An integrated view of the structural and administrative elements for laying the foundation for effective CRAs.

Frequency with which organizations conduct CRAs

43%
Annually

6%
Semi-annually one or more components

6%
Every other year

20%
Ad-hoc

11%
Other

14%
Never

N = 35

Scoring framework implemented to evaluate risk

46%
Five-tiered scale

14%
Four-tiered scale

3%
Three-tiered scale

26%
Do not have criteria

11%
Other

N = 35

CRA Framework

Risk Assessment sign-off

9%
Audit Committee or equivalent under the Board of Directors

3%
Chief Executive Officer (CEO)

11%
Chief Risk Officer (CRO)

23%
Chief Compliance Officer (CCO)

43%
There is no sign off required

11%
Other

N = 35

Risk Assessment granularity

32%
Compliance risk domains

29%
Compliance program risks

24%
Compliance requirements

15%
Other

N = 34

CRA framework

When considering criteria by which to assess the level of compliance risk, respondents indicated that their organizations are commonly selecting reputational, legal and commercial/financial risk criteria. According to 85% of respondents, compliance risk scores and rating methodologies are not used in larger enterprise risk assessment scoring.

Variables to assess compliance risk impact*

76%
Reputational risk

74%
Legal risk

71%
Commercial/ Financial risk

56%
Operational risk (including reliability risk)

35%
Corporate social responsibility risk

21%
Other**

N = 34

Aggregation of CRA results into ERM process

15%
Compliance risk scores are aggregated and feed into a single compliance risk to the ERM calculations

40%
Compliance risk scores are not aggregated through a fixed methodology, but are subjectively mapped to the ERM calculations

45%
Compliance risk scores are neither aggregated nor fed into the ERM calculation as a single input

N = 33

**Others include, but not limited to:
- Safety and Security
- People
- Regulatory/Legal
- Reputational, regulatory, financial and operational, stakeholder impact
- Regulatory RIsk
- All of the above

*Respondents were asked to select all applicable options.

26

CRA scope

Risk areas covered within CRAs at responding organizations include traditional high-risk areas such as regulatory reporting, data privacy and cybersecurity. Historically prevalent risk areas such as anti-bribery and anti-corruption (ABAC), fraud, and operations are not being assessed at as many organizations, highlighting a shift in CRA scope.

The range of percentages represent the grouped respondents that selected the underlying risk areas.

77% – 60%	59% – 45%	44% – 29%	28% – 18%
• Environmental	• Licenses, Permits, and Leases	• Federal Contracting	• Anti-Corruption/Anti-Bribery
• Regulatory Reporting	• Legal and Intellectual Property	• Dam Safety	• Reliability
• Cybersecurity	• Swaps and Derivatives	• Lease Royalty Management	• Records and Information Management
• Accounting and Finance	• Sustainability	• Enterprise Compliance	• Commodity Markets
• Health and Safety	• Trade/Import/Export	• State Regulatory	• Antitrust
• Data Privacy	• Direct and Indirect Tax	• Labor and Employment/Human Resources	• Supply Chain Management
• Conflicts of Interest	• Conflicts of Interest	• Fraud and Financial Crimes	• Contract Compliance
• Other*		• Operations	

N = 34

Others include, but not limited to:
- Culture of compliance/values
- Finalizing new form
- FERC Tariff and NAESB WEQ, NERC CIP and O&P
- N/A

Respondents were asked to select all applicable options.

Compliance risk register management

Practices related to the management of compliance risk registers across participating organizations indicate a majority of respondents are undertaking collaborative efforts, internally and externally, to update the risk register on a frequent basis with approximately half of the respondents having dedicated resources accountable for identifying and assessing key risks.

34%
Risk register is updated on a frequent basis with inputs identified through existing partnerships with business units

34%
Third-party vendors and consultants are engaged on an as-needed basis to identify updates to the risk register

17%
Each risk area has a dedicated resource accountable for identifying impact of regulatory and business change for their risk area

14%
Key risks are identified and assessed on a quarterly/semi-annual basis based on input and feedback from leadership

11%
Network of compliance peers across the industry is leveraged to identify updates to the risk register

6%
Compliance Steering Committee has representation from all key business units and serves as a forum for identification and validation for addition of new risks and elimination of existing risks to/from the risk register

N = 30

Note: Respondents were asked to select all applicable options.

Compliance controls management

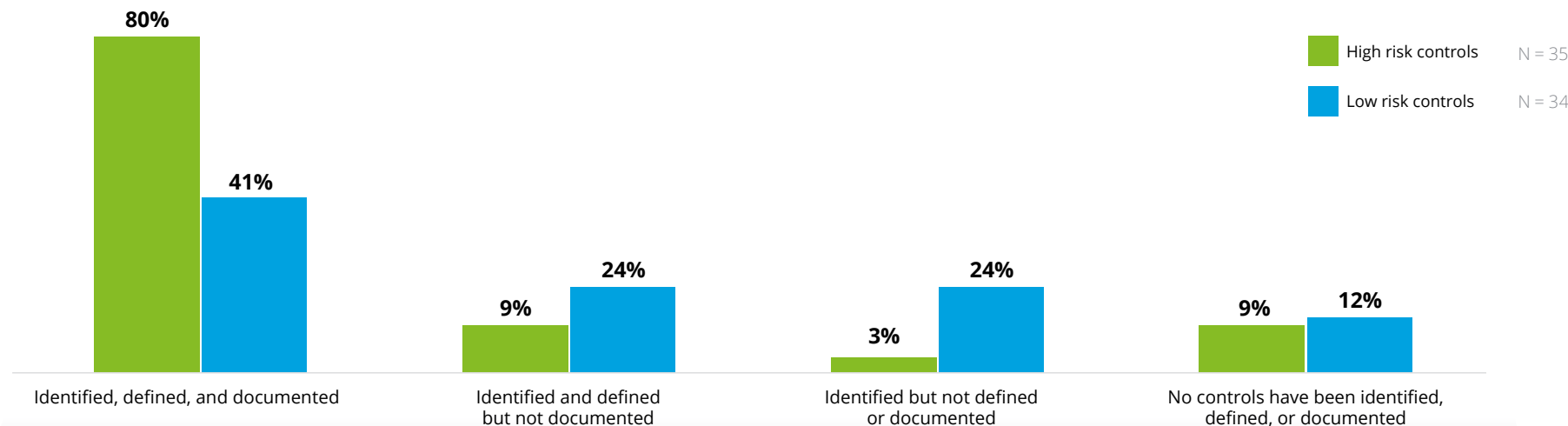A comparative view of the high versus low risk compliance controls indicates that a majority of organizations are ahead of the curve with risk controls identified, defined, and documented. Further, a majority of the organizations assess control effectiveness—either through the Internal Audit/Assurance function or through embedding this into the CRA itself.

Legend: High risk controls (N = 35), Low risk controls (N = 34)

Chart — High vs Low risk controls:
- Identified, defined, and documented: 80% / 41%
- Identified and defined but not documented: 9% / 24%
- Identified but not defined or documented: 3% / 24%
- No controls have been identified, defined, or documented: 9% / 12%

Assessment of **control effectiveness** as a part of the CRA process

- **44%** Control effectiveness is assessed by our Internal Audit/Assurance function
- **26%** Control effectiveness is embedded into the risk areas being assessed
- **15%** Control effectiveness is not measured
- **12%** Other*
- **3%** Control effectiveness is assessed as a separate portion of the CRA
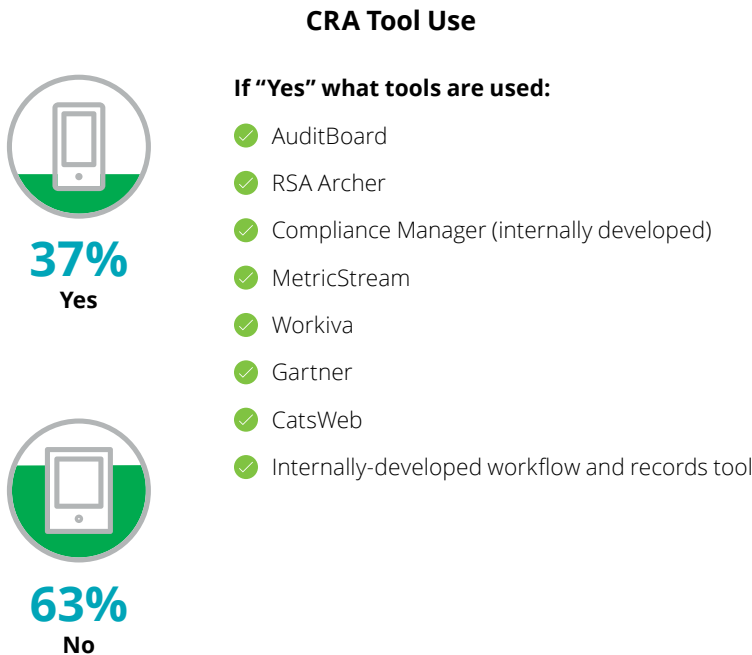
N = 34

*Others include, but not limited to:
- Control effectiveness assessed by multiple assurance functions including Reliability Standards Compliance Oversight, ERM, Internal Audit and Enterprise Compliance
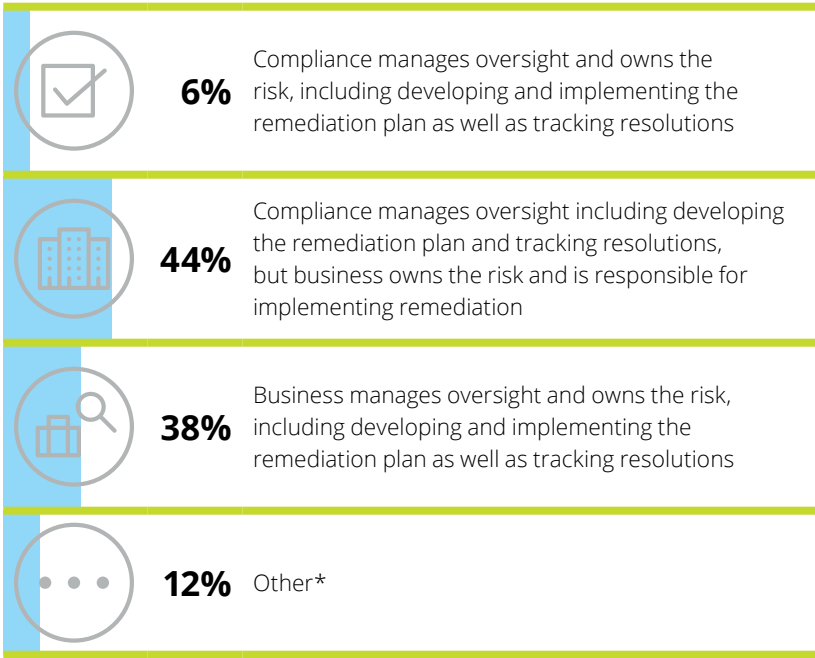- No control effectiveness measurement outside of SOX controls.

29

Compliance and technology

There appears to be a general lack of tech-enablement across a majority of participating organizations as it pertains to the technological capabilities leveraged to manage the CRA process. The lack of tech-enabled capabilities is further highlighted by only 37% of survey respondents currently leveraging dedicated tools as part of their CRA process.

CRA Tool Use

37%
Yes

63%
No

If "Yes" what tools are used:

- ✓ AuditBoard
- ✓ RSA Archer
- ✓ Compliance Manager (internally developed)
- ✓ MetricStream
- ✓ Workiva
- ✓ Gartner
- ✓ CatsWeb
- ✓ Internally-developed workflow and records tool

Compliance risk assessment roles and responsibilities

6% Compliance manages oversight and owns the risk, including developing and implementing the remediation plan as well as tracking resolutions

44% Compliance manages oversight including developing the remediation plan and tracking resolutions, but business owns the risk and is responsible for implementing remediation

38% Business manages oversight and owns the risk, including developing and implementing the remediation plan as well as tracking resolutions

12% Other*

*Others include, but not limited to:
- Making progress towards the compliance manages oversight but business owns risk framework but still in infancy.
- Compliance manages oversight including working with business owners to develop the remediation plan and tracking resolutions, but business owns the risk and is responsible for implementing remediation
- Sexual Harassment
- We are in the process of moving to option #2, but we are in option #3 now

N = 35

30

Compliance and technology

Areas of interest to the board

Technology use to manage the CRA process

36% CRAs are conducted with minimal use of technology (e.g., email, spreadsheets), but a platform is leveraged as a central data repository

36% CRAs are conducted manually with limited to no support from technology (e.g., documents, spreadsheets)

18% CRAs are facilitated through automated workflows on a platform that also serves as the central data repository

9% Other

N = 33

New Compliance areas the board is asking about

Artificial Intelligence

GenAI

Data Privacy Laws

Department of Justice Expectations / Memos

ESG

CEII

PII

US Government Engagement

Climate Change Transition

Cybersecurity

Sexual Harassment

Grants

Privacy

Information governance
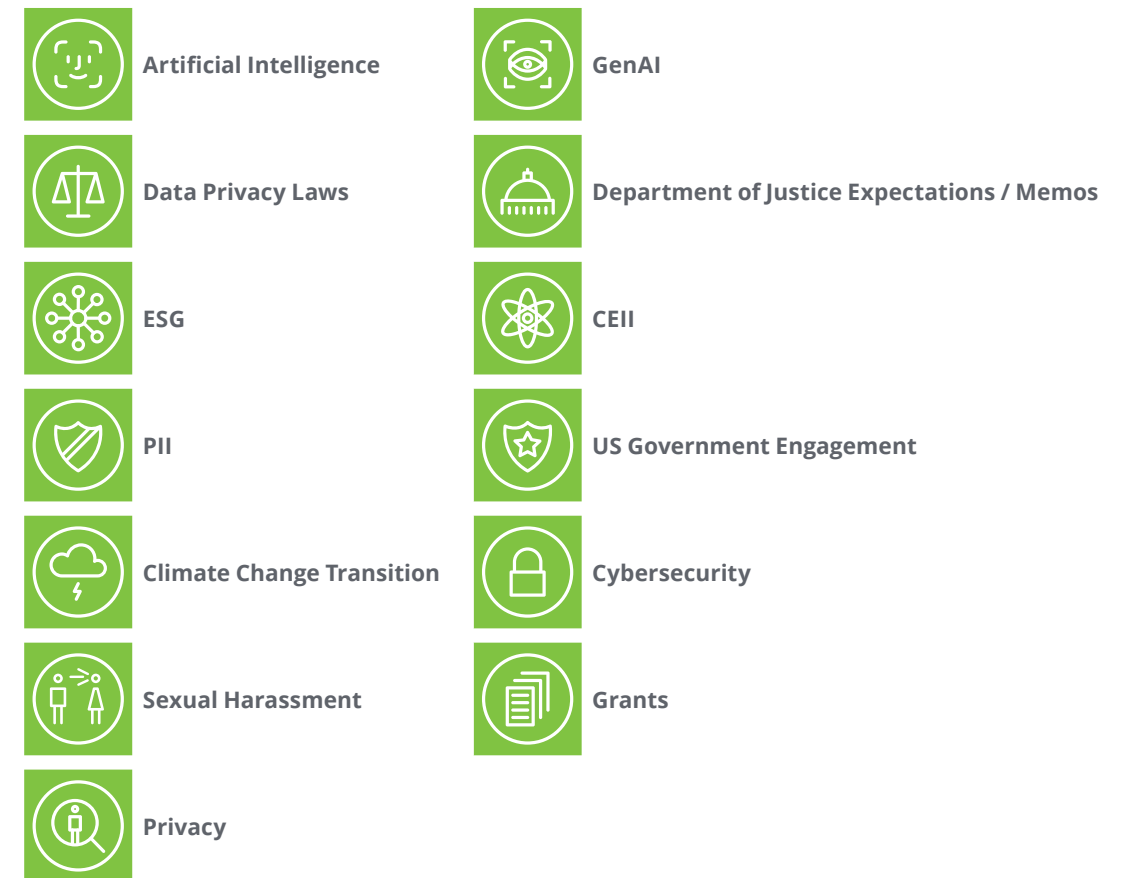
This section is focused on the controls, projects, and roles of the Information Governance (IG) program at respondents' respective organization. IG programs serve to manage information, including, but not limited to, digital data, documents, and archival records. IG programs typically involve a wide range of cross-disciplinary policies, procedures, controls, tools, and technologies that help a company meet regulatory, legal, and operational demands. Topics within this section include IG challenges, relation to compliance functions, and training.

Key takeaways:

The **most common factors** considered to prioritize IG at surveyed organizations are **compliance risk, reputational risk, litigation, and security threats/obligations.**

IG programs interact heavily with both enterprise and regulatory compliance functions at an organization. For enterprise compliance, they most commonly consulted on IG program setup and operationalization, privacy compliance, and data loss protection. **Over 50% of responding organizations** reported that their IG program supported regulatory compliance in the areas of record management obligations and responding to regulatory requests or audits.

When considering organizations' own information governance maturity, respondents noted **room for improvement**, with **71% indicating they were a work in progress**.

IG program maturity and priorities

A majority of organizations are still working to set up their IG programs, anchoring on compliance risk, litigation efforts, and security threats as key elements being prioritized to drive programmatic maturity.

Program maturity

- **9%** Fully developed
- **71%** Work in progress
- **IG Program**
- **9%** New Initiative
- **11%** Do not have an IG program

Enterprise-level factors considered to prioritize IG*

- **76%** Compliance risk
- **38%** Impending legislation
- **47%** Quality control/ quality assurance
- **62%** Reputational risk
- **44%** Current legislation
- **35%** Decision-making and information delivery
- **56%** Litigation
- **41%** Cost reduction
- **12%** IG is not a priority for our organization
- **71%** Security threats/ obligations
- **50%** Enhanced productivity

Information governance

IG program maturity overview

As IG programs mature the below elements depict points of focus for organizations across the energy industry. The next pages shows a double click into IG policy infrastructure.

63% — Enterprise Policies have been established to set guidelines and expectations pertaining to IG within the organization

40% — Dedicated resources have been assigned to drive and support the IG compliance program

40% — A dedicated, independent IG organization (or group) is in place (or responsibilities have been formally assigned to an existing group) to drive the execution of IG compliance in accordance with the overarching compliance governance program

34% — Formal processes dedicated to IG are in place to guide decisions and activities

29% — A program charter is in place with a clearly defined mission, and role and responsibilities to guide the IG compliance organization

29% — Executive Sponsorship has been received for an independent compliance governance program for IG

29% — A formal framework that defines and identifies the key roles and responsibilities pertaining to IG is in place to help instill ownership and accountability

26% — A steering committee (or equivalent) is in place to provide governance and oversight over the IG program

23% — Formal controls dedicated to IG are in place to provide assurance on data privacy compliance

20% — Consumer Policies have been established to set guidelines and expectations pertaining to IG within the organization

14% — Other*

11% — Dedicated C-suite responsibilities for IG have been established and clearly communicated to the respective executives

11% — Formal metrics and performance benchmarks for IG have been established

Others include, but not limited to:
- A draft of the Policy created and rest of the activities in progress
- IG is of low maturity
- We are in the process of establishing a governance framework for IG
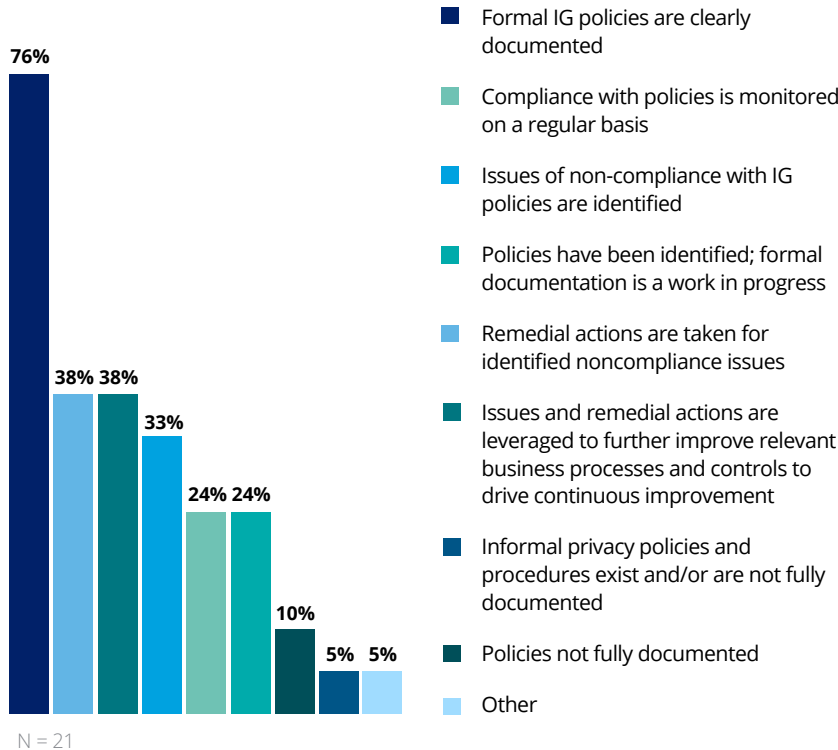- Building awareness and process

N = 35

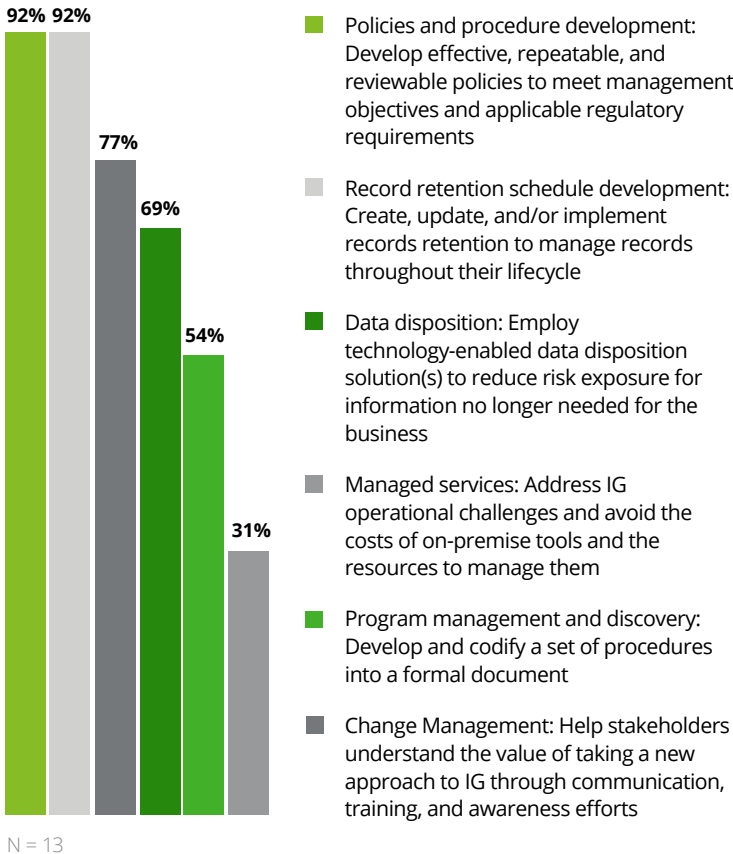Respondents were asked to select all applicable options.

IG policy infrastructure

This question pertains to those who answered that they have enterprise and/or consumer policies to set IG guidelines. Results indicate that the majority of these respondents have clearly documented IG policies.

This question pertains to those who answered that they have a dedicated IG program. A large majority of respondents reported having policies and procedure development, record retention schedule development, and change management.

Chart 1 (N = 21):

Value	Legend
76%	Formal IG policies are clearly documented
38%	Compliance with policies is monitored on a regular basis
38%	Issues of non-compliance with IG policies are identified
33%	Policies have been identified; formal documentation is a work in progress
24%	Remedial actions are taken for identified noncompliance issues
24%	Issues and remedial actions are leveraged to further improve relevant business processes and controls to drive continuous improvement
10%	Informal privacy policies and procedures exist and/or are not fully documented
5%	Policies not fully documented
5%	Other

N = 21

Chart 2 (N = 13):

Value	Legend
92%	Policies and procedure development: Develop effective, repeatable, and reviewable policies to meet management objectives and applicable regulatory requirements
92%	Record retention schedule development: Create, update, and/or implement records retention to manage records throughout their lifecycle
77%	Data disposition: Employ technology-enabled data disposition solution(s) to reduce risk exposure for information no longer needed for the business
69%	Managed services: Address IG operational challenges and avoid the costs of on-premise tools and the resources to manage them
54%	Program management and discovery: Develop and codify a set of procedures into a formal document
31%	Change Management: Help stakeholders understand the value of taking a new approach to IG through communication, training, and awareness efforts

N = 13

Respondents were asked to select all applicable options.

IG governance

Among the 34% of respondents that indicated having a dedicated C-suite level owner of IG responsibilities, a majority of respondents indicated the Chief Ethics and/or Compliance Officer as the owner.

Assignment of dedicated C-suite responsibilities pertaining to IG

67%

33%

■ Chief Ethics and/or Compliance Officer

■ General Counsel
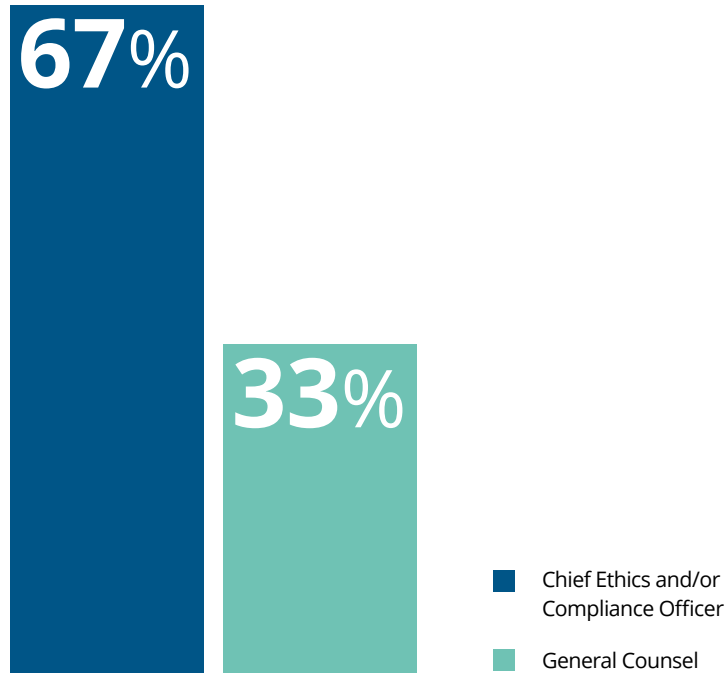
N = 3

Maturity of the formal governance and accountability framework that defines and identifies the key roles and responsibilities pertaining to IG

75%

25%

■ Clear assignment of key roles and responsibilities

■ Limited assignment of roles and responsibilities (e.g., only for high risk areas)
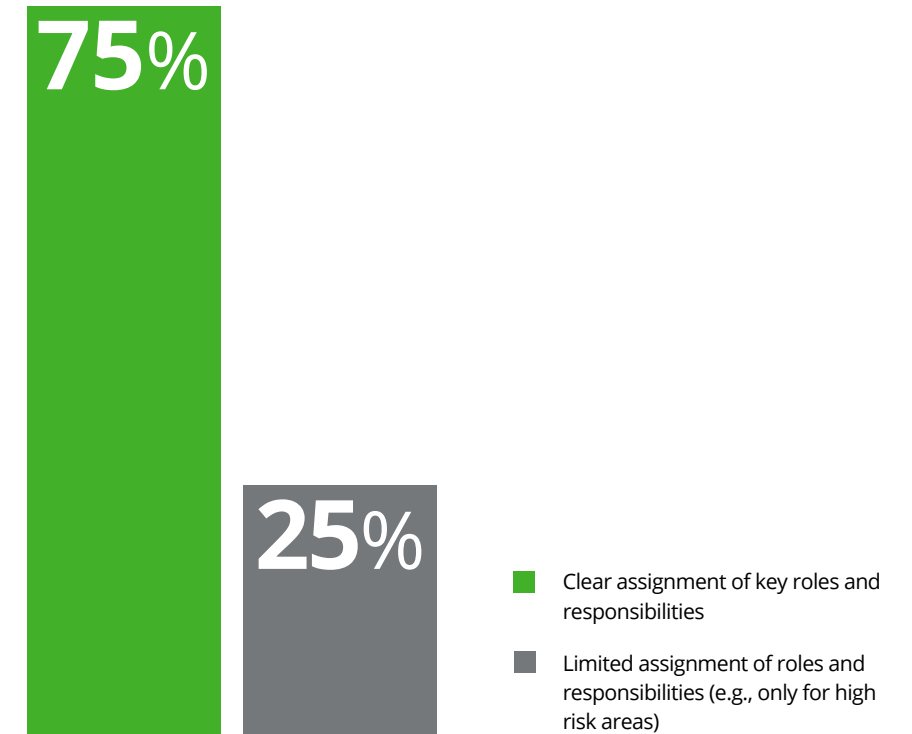
N = 8

IG process maturity

Half of respondents cited having high-level business processes, while only 20% cited having detailed business processes with clear ownership. Of the respondents that indicated having formal IG controls, 86% said these controls are regularly evaluated and updated.

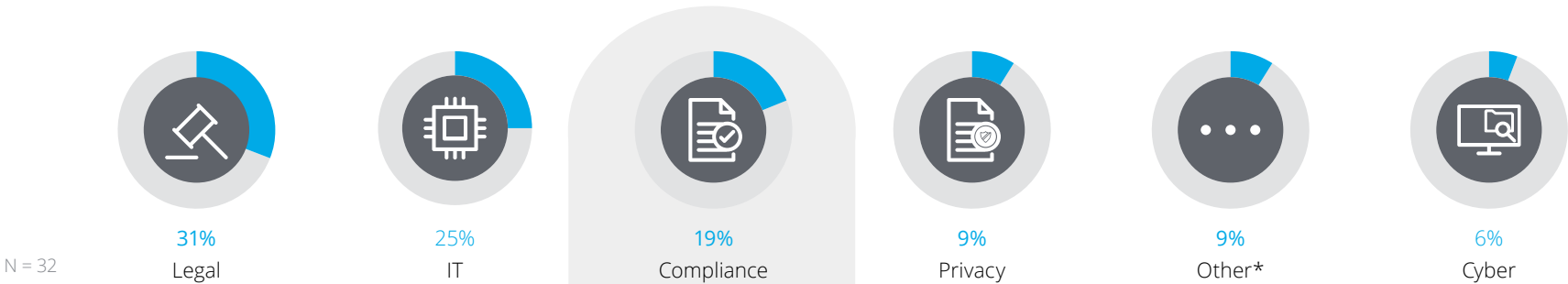## Maturity of formal business processes pertaining to IG

50% High-level business processes are in place

40% Business processes have been effectively operationalized

30% Business processes are clearly documented

30% Business processes have been inventoried either within each business unit or in a central repository

20% Detailed business processes with clear ownership and decisions are in place

20% Other*

N = 10

Legend:
- ■ Detailed business processes with clear ownership and decisions are in place
- ■ Business processes have been effectively operationalized
- ■ Business processes are clearly documented
- ■ High-level business processes are in place
- ■ Business processes have been inventoried either within each business unit or in a central repository
- ■ Other*

86% IG controls are in place

86% IG controls are regularly evaluated and updated as needed

29% IG controls have been automated

29% IG controls are regularly monitored through established mechanisms

N = 7

Legend:
- ■ IG controls are in place
- ■ IG controls are regularly evaluated and updated as needed
- ■ IG controls have been automated
- ■ IG controls are regularly monitored through established mechanisms

*Others include, but not limited to:
- Not consistently in place
- Implementation of documented processes is not done across enterprise

Respondents were asked to select all applicable options.

Information governance

37

IG program functional ownership and roles

Ownership of IG responsibilities appears to reside primarily in IT and Legal with Compliance being slightly less common. Compliance plays a prominent role in consulting the business on matters of privacy, regulatory reporting, program setup, and data loss prevention as it relates to IG.

Business functions serving as the primary lead of the IG program

N = 32

31% Legal	25% IT	19% Compliance	9% Privacy	9% Other*	6% Cyber

Role of the compliance function as it relates to IG*

59% Privacy compliance	50% Data loss protection	47% IG program setup and operationalization	41% Big data initiatives	34% Regulatory reporting	19% De-commissioning	13% The enterprise compliance function does not consult on IG projects	13% Other*

N = 32

*Others include, but not limited to:
- Not consistently in place
- Implementation of documented processes is not done across enterprise

**Respondents were asked to select all applicable options.

Regulatory compliance focus

Acknowledging the nascency and foundational focus on IG across the industry, it is natural that IG programs across a majority of respondents currently operate in a 'reactive' mode where IG leadership and stakeholders rely on available infrastructure to solve issues identified.

Resilience of the IG program

REACTIVE — **61%** — IG leadership and stakeholders tend to rely on available infrastructure to solve issues identified

ACTIVE — **36%** — IG leadership and stakeholders anticipate emerging issues and leverage available infrastructure to navigate through these issues

PROACTIVE — **3%** — IG leadership and stakeholders predict and plan for potential IG risk scenarios and continually focus on enhancing the IG infrastructure within the organization

N = 32

Enablement of the regulatory compliance priorities*

59%
Supports on-going record management obligations

56%
Supports responding to regulatory requests or regulatory audits

25%
Provides a central repository for retrieving records in a timely fashion

28%
The IG program does not support the organization's regulatory compliance priorities

N = 33

*Respondents were asked to select all applicable options.

39
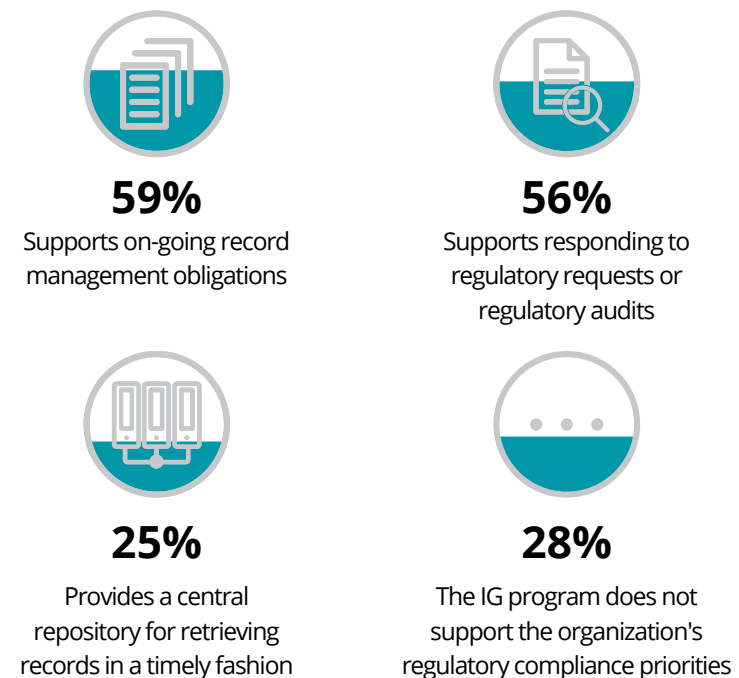
Ranking of IG principles from a regulatory compliance lens

Respondents were asked to rank the various IG principles—on a scale of high, medium and low—through a regulatory compliance lens. Given the newfound focus on IG across the industry, accountability, protection, completeness, and retention were ranked as "high importance" by a majority of respondents.

Regulatory Compliance Focus

	Accountability	Transparency	Integrity	Protection	Completeness	Retention	Disposition	Accessibility
High	13	10	11	14	13	13	7	9
Medium	8	4	5	5	6	4	6	6
Low		7	4	2	4	2	6	4

N = 33   N = 32   N = 32

■ High   ■ Medium   ■ Low
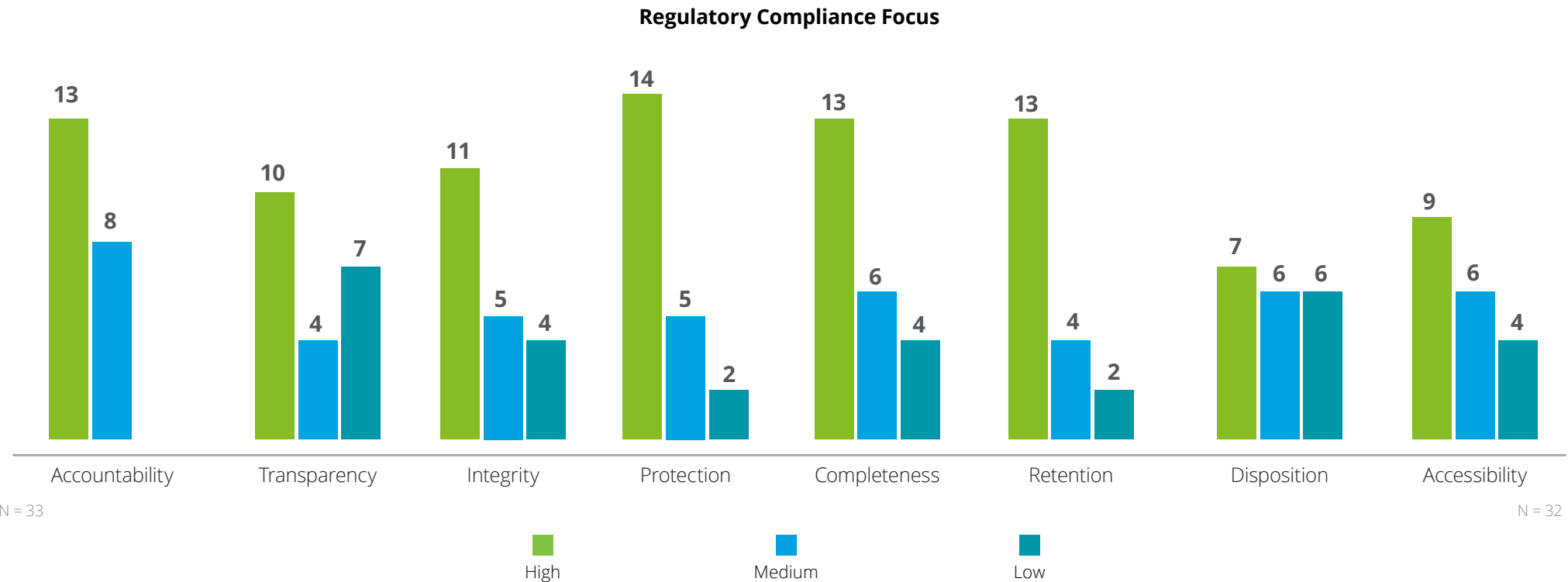
*Others include, but not limited to:
- Primary sponsorship by IT with collaboration from Data Privacy, RIM, and Cyber
- Currently not being lead by any function.
- Not assigned

Respondents were asked to select all applicable options.

40

Maintaining compliance with IG policies

Focus of training and communication to support compliance with IG policies

36%
EMBEDDED
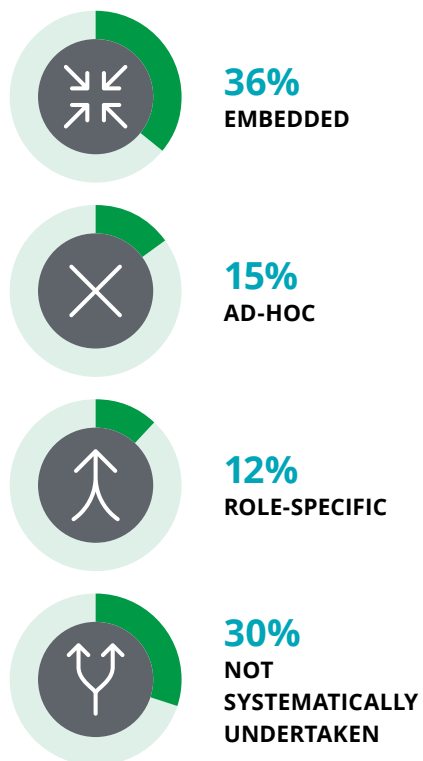
IG training and communication are embedded in on-boarding and routine training, and developed with the assistance of appropriate compliance resources from across the enterprise

15%
AD-HOC

Sometimes, IG training and communications take place on an ad-hoc basis or when there is a policy change or compliance issue

12%
ROLE-SPECIFIC

Role-specific, IG training is provided only to those roles that manage information directly or are impacted by IG compliance matters

30%
NOT SYSTEMATICALLY UNDERTAKEN

IG training and communication are not systematically undertaken across the organization

N = 33

Compliance with record retention timelines to avoid retention past the retained period

15%
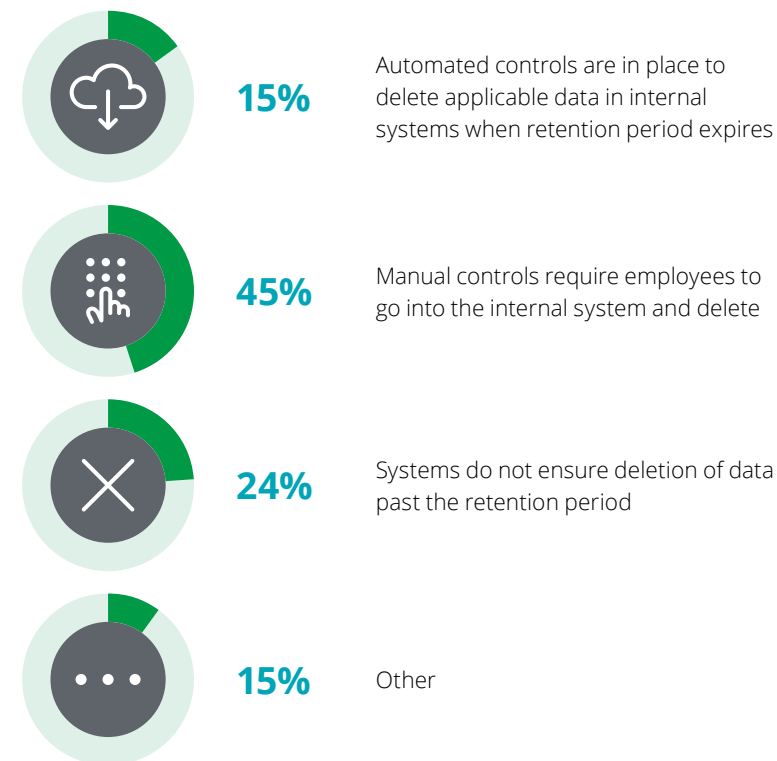
Automated controls are in place to delete applicable data in internal systems when retention period expires

45%

Manual controls require employees to go into the internal system and delete

24%

Systems do not ensure deletion of data past the retention period

15%

Other

N = 33

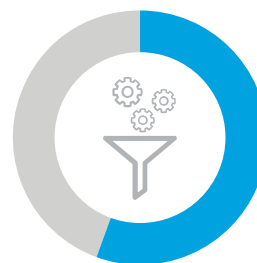# Greatest IG challenges for the organization or IG program

Programs face an array of obstacles in executing information governance efforts.
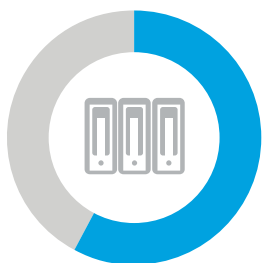
58%
Technology
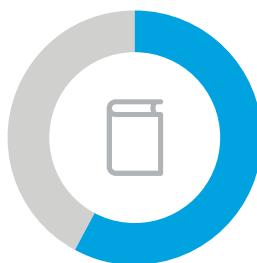
58%
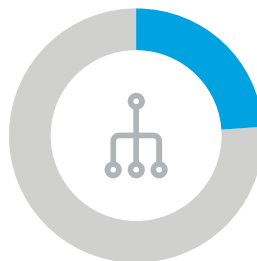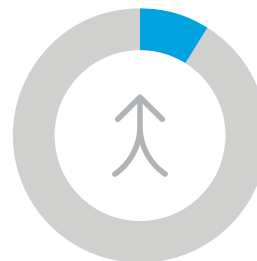Lack of necessary skillsets and/or timely availability of resources

55%
Volume

33%
Insufficiency of funding

33%
Executive

24%
Program

9%
Impact of mergers

3%
Other

N = 33

Respondents were asked to select all applicable options.

Risk, controls, and assurance

This section of the survey covers compliance risk appetite, risk controls, and classification/tracking of these risk controls. This section is meant to paint a broader picture of what role the compliance function plays in organizations' larger assurance and risk landscapes. Questions focused on specific tools or systems used to track risks are also included.

Key takeaways:

Approximately 50% of surveyed respondents **track their compliance controls** (across both regulatory and enterprise compliance functions) with **integrated tools or systems**, while most of the remaining organizations either use excel spreadsheets or track controls ad hoc.

Three quarters of responding organizations report subscribing to the **COSO Framework Three Lines model**, which provides a framework for enterprise risk management.

The **top attributes of successful assurance programs** as identified by surveyed organizations are **enhancing risk prevention, having clear roles and responsibilities, and strong identification of risks.**
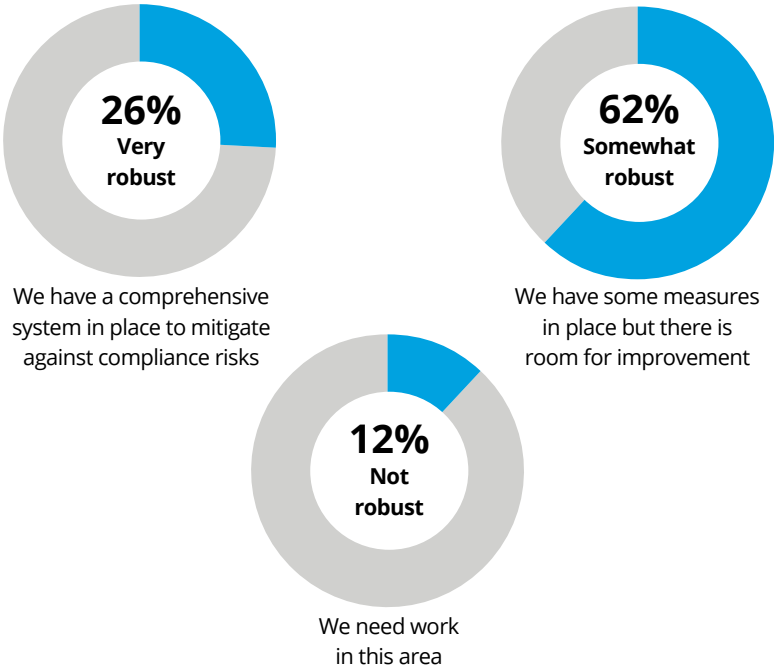
Compliance risk controls

Several responding companies' compliance programs stated that their compliance controls, while somewhat robust and anticipatory, have room for improvement.
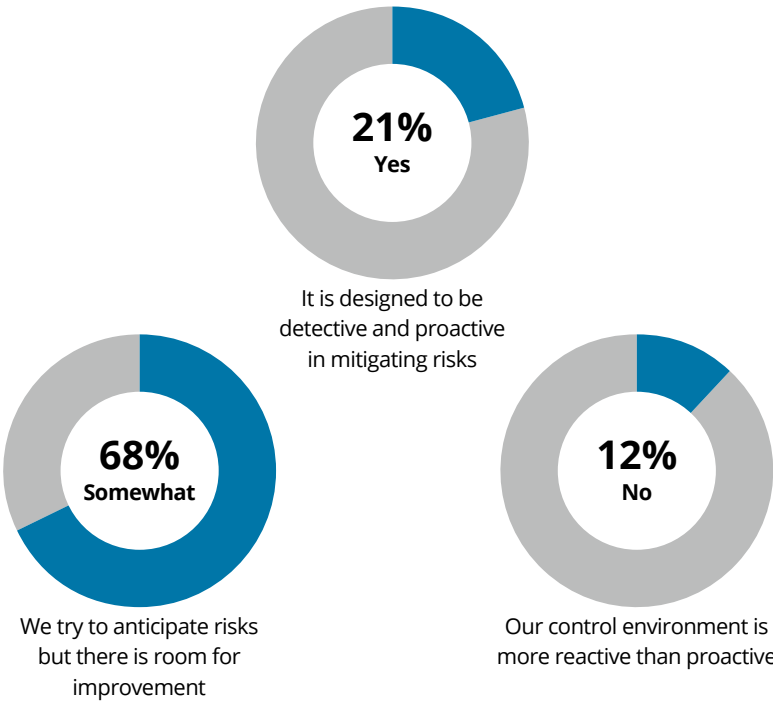
Compliance Risk Controls Robustness

26%
Very robust

We have a comprehensive system in place to mitigate against compliance risks

62%
Somewhat robust

We have some measures in place but there is room for improvement

12%
Not robust

We need work in this area

Compliance Risk Control Environment

21%
Yes

It is designed to be detective and proactive in mitigating risks

68%
Somewhat

We try to anticipate risks but there is room for improvement

12%
No

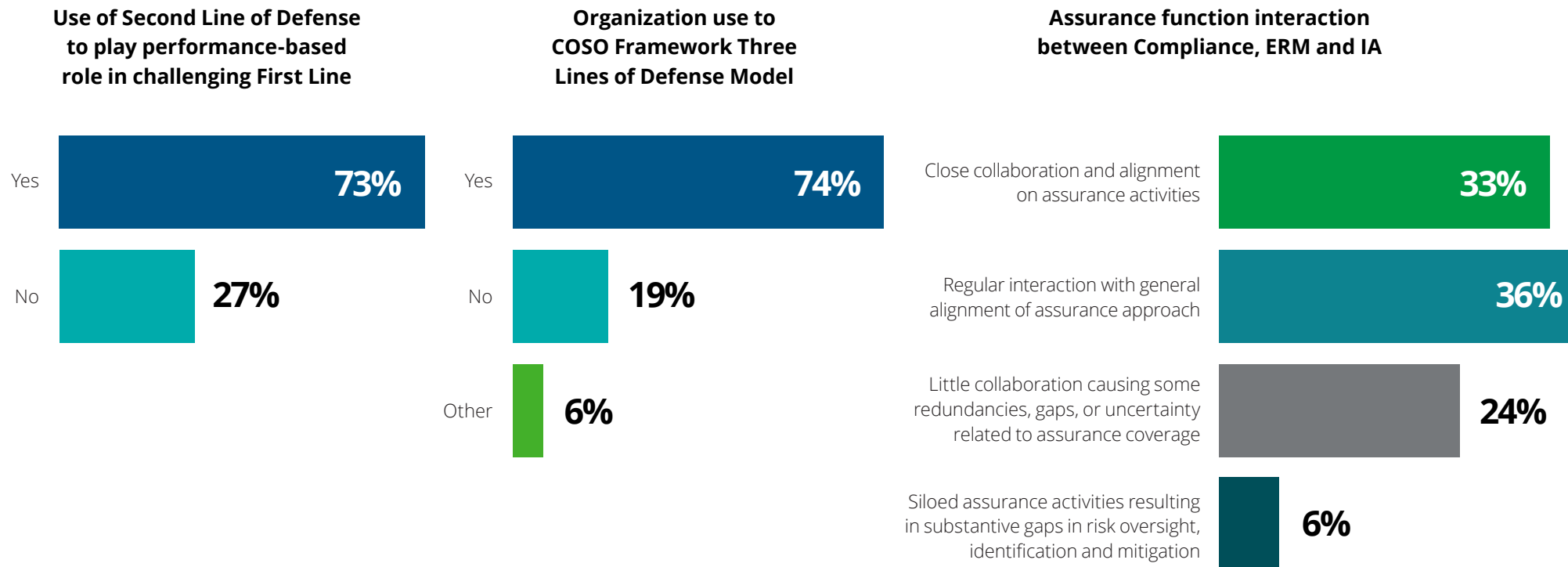Our control environment is more reactive than proactive

N = 34

N = 34

Three Lines of Defense

Responding organizations are largely aware of and leverage the three lines of defense model for addressing risks and in most the second line plays a large role in assuring the performance of the business.
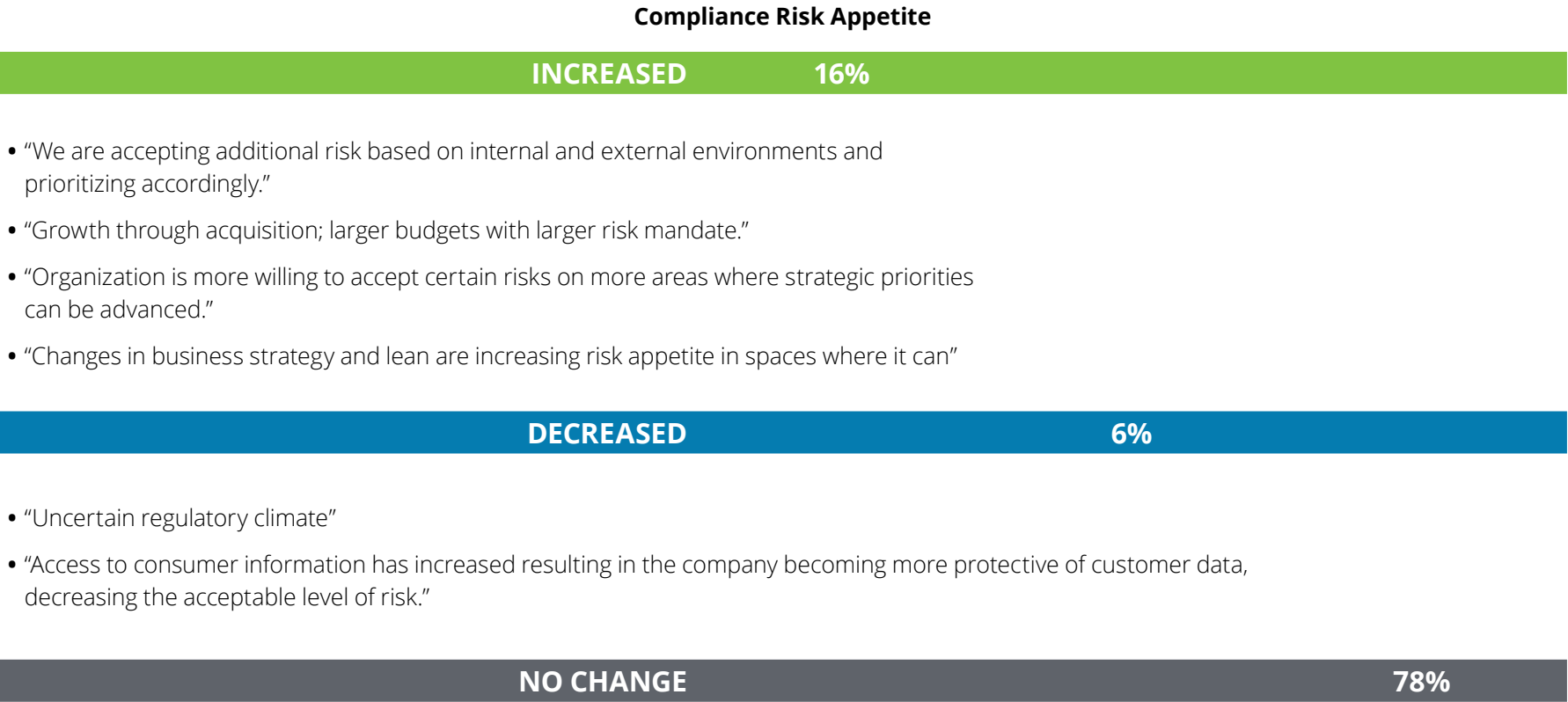
Use of Second Line of Defense to play performance-based role in challenging First Line

Yes	**73%**
No	**27%**

Organization use to COSO Framework Three Lines of Defense Model

Yes	**74%**
No	**19%**
Other	**6%**

Assurance function interaction between Compliance, ERM and IA

Close collaboration and alignment on assurance activities	**33%**
Regular interaction with general alignment of assurance approach	**36%**
Little collaboration causing some redundancies, gaps, or uncertainty related to assurance coverage	**24%**
Siloed assurance activities resulting in substantive gaps in risk oversight, identification and mitigation	**6%**

N = 33

Compliance risk appetite

Most companies' risk appetites have not changed in the last year. 22% of responding organizations' do have new risk postures now for a variety of reasons as depicted below.

Compliance Risk Appetite

| INCREASED | 16% |

- "We are accepting additional risk based on internal and external environments and prioritizing accordingly."

- "Growth through acquisition; larger budgets with larger risk mandate."

- "Organization is more willing to accept certain risks on more areas where strategic priorities can be advanced."

- "Changes in business strategy and lean are increasing risk appetite in spaces where it can"

| DECREASED | 6% |

- "Uncertain regulatory climate"

- "Access to consumer information has increased resulting in the company becoming more protective of customer data, decreasing the acceptable level of risk."
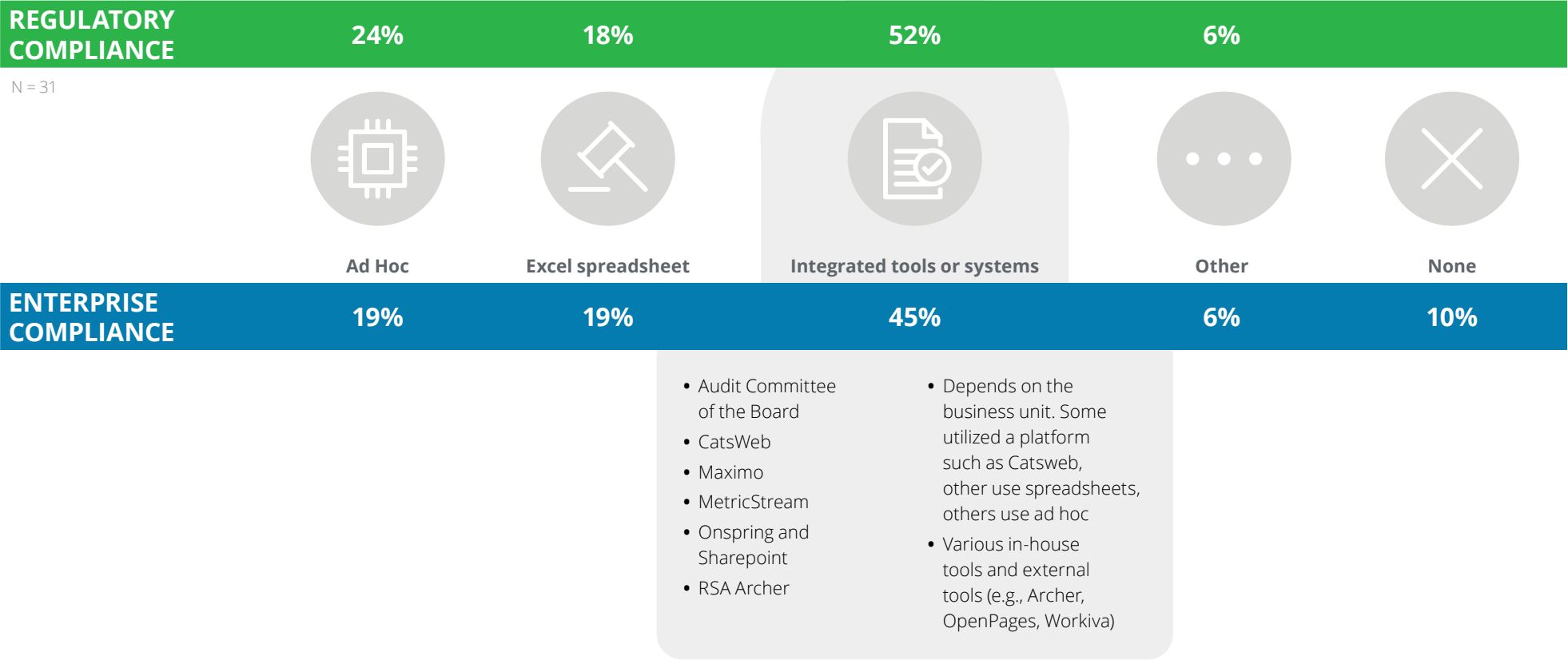
| NO CHANGE | 78% |

N = 31   N = 33

Respondents were asked to select all applicable options.

Tracking compliance controls

About half of responding organizations recognize that in today's environment it's essential to leverage an integrated tool or system to track and map compliance controls to relevant risks.
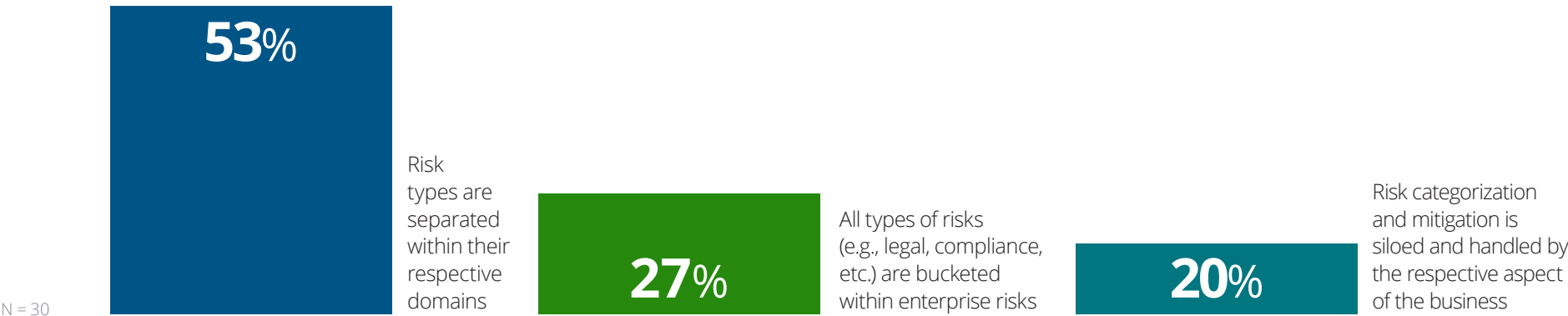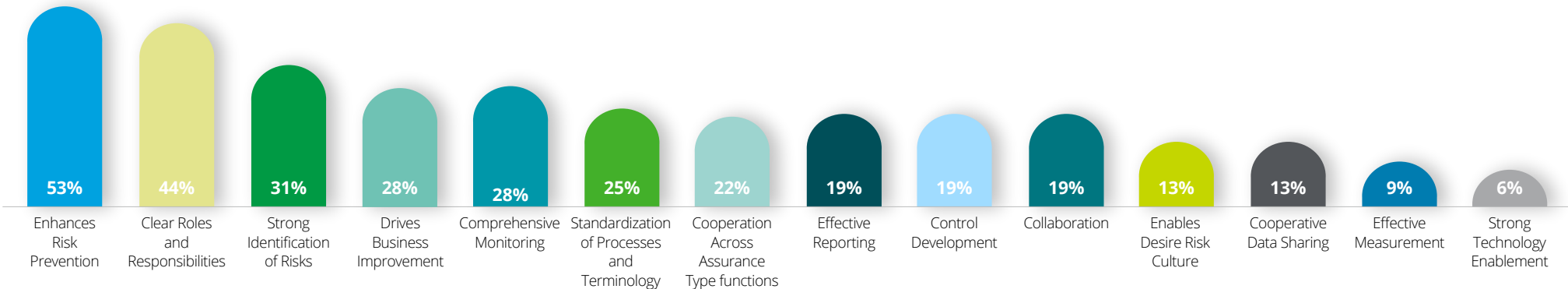
REGULATORY COMPLIANCE	24%	18%	52%	6%	
	Ad Hoc	Excel spreadsheet	Integrated tools or systems	Other	None
ENTERPRISE COMPLIANCE	19%	19%	45%	6%	10%

N = 31

N = 33

- Audit Committee of the Board
- CatsWeb
- Maximo
- MetricStream
- Onspring and Sharepoint
- RSA Archer

- Depends on the business unit. Some utilized a platform such as Catsweb, other use spreadsheets, others use ad hoc
- Various in-house tools and external tools (e.g., Archer, OpenPages, Workiva)

47

Compliance and legal risk classification

Given the broad scope of compliance and legal risks impacting companies in the energy industry, many appear to favor specialized and targeted approaches to organizing and classifying risks as opposed to siloed or broad overarching approaches.

N = 30

53% Risk types are separated within their respective domains

27% All types of risks (e.g., legal, compliance, etc.) are bucketed within enterprise risks

20% Risk categorization and mitigation is siloed and handled by the respective aspect of the business

Successful aligned assurance program attributes*

Below depicts respondents' most common successful attributes for having aligned assurance programs where all lines of defense are working harmoniously to mitigate against risk.

Attribute	%
Enhances Risk Prevention	53%
Clear Roles and Responsibilities	44%
Strong Identification of Risks	31%
Drives Business Improvement	28%
Comprehensive Monitoring	28%
Standardization of Processes and Terminology	25%
Cooperation Across Assurance Type functions	22%
Effective Reporting	19%
Control Development	19%
Collaboration	19%
Enables Desire Risk Culture	13%
Cooperative Data Sharing	13%
Effective Measurement	9%
Strong Technology Enablement	6%

N = 32

*Respondents were asked to select all applicable options.

Deloitte.

This presentation contains general information only, and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.