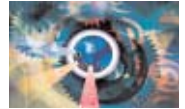# The role of IT in compliance

A report from the Economist Intelligence Unit
sponsored by **VERITAS**

Preface

The role of IT in compliance is an Economist Intelligence Unit white paper, sponsored by VERITAS Software Corp. The Economist Intelligence Unit bears sole responsibility for this report. The Economist Intelligence Unit's editorial team executed the survey, conducted the interviews and wrote the report. The findings and views expressed in this report do not necessarily reflect the views of the sponsor. Paul Kielstra is the author of the report.

Our research drew on two main initiatives: We conducted a global online survey in March 2005 of 133 senior executives on the topic of the changing role of IT in compliance.

To supplement the survey results, we also conducted in-depth interviews with senior executives. Our thanks are due to all survey respondents and interviewees for their time and insights.

April 2005

Executive summary

Companies face a wide array of rules whose number and complexity have grown over the years, dramatically so since the collapse of Enron in 2001. The massive fraud uncovered at the Texan energy company, as well as at MCI, Parmalat and others, has engendered a new wave of regulations in many countries that aim to tighten financial reporting requirements and strengthen executive accountability.

Information technology (IT) has long played a crucial role in supporting companies' compliance efforts. The scale and scope of regulations have prompted companies to invest heavily in labour-saving technology in order to keep up with the amount of official paperwork. Post-Enron regulation has placed an even higher premium on IT to find ways to help corporate executives exercise control over their companies and to comply with the new rules.

In light of these trends, the Economist Intelligence Unit, in co-operation with VERITAS Software Corp., surveyed 133 executives around the world and conducted ten in-depth interviews with senior businesspeople to find out how the role of IT is changing. The responses show that its role has certainly grown as the executive suite places more demands on it. With the increase in IT's importance, it has become more integrated into the compliance process, diffusing responsibility for technology decisions in this area.

In the past, many of the decisions about how much money to spend on IT and how to spend it were left up to the chief information officer (CIO). Now, however, compliance-related IT has become too important to remain within the purview of the CIO alone. The chief executive officer (CEO) is more dependent than ever on IT for knowledge of what is going on in the company. As the downfall of MCI's chairman, Bernie Ebbers, shows, ignorance is no defence.

Here are some examples of recent developments.

● The Sarbanes-Oxley Act (SOX) in the US and similar laws elsewhere have led many companies to scramble to overhaul their financial reporting, internal controls and data storage in order to meet unprecedented requirements for speed, consistency and accuracy. Companies have found Section 404 of the act to be particularly demanding. It requires corporations and their auditors to report on the effectiveness of the former's internal control structures and procedures for financial reporting. In practice, this has meant describing, documenting and demonstrating the robustness of a vast number of processes, most of which use information technology.

● For banks, the Revised International Capital Framework (commonly known as Basel II) will radically change how financial services organisations calculate risk. Rather than using the same measures of risk across all banks, the accord will allow them to use their own performance data to measure risk and therefore capital requirements. Basel II, however, also introduces for the first time the need to measure operational risk arising from internal or external problems.

● A host of data-privacy legislation worldwide has led to a demand for heightened levels of accuracy and network protection. Some laws, such as California's Database Security Breach Notification Act, require companies to tell individuals about improperly leaked data, and Europe's Data Protection Directive prevents data transfer even within firms to departments operating in countries with insufficient legal safeguards.

These and many other new regulations underline the

importance of strong compliance procedures and the ability of IT to support this effort.

The recent wave of new corporate rules is having a strong effect on the manner in which technology is used and the role of IT departments in compliance. This survey revealed the following key findings.

● The use of IT in compliance is growing rapidly in monitoring business activity that is heavily reliant on technology, such as privacy and security. It is expanding elsewhere, but more slowly.

● Expenditure on compliance-related IT appears to be rising rapidly, although many respondents in the survey admit that they don't have a clear picture of how much is being spent. Of those respondents that say they have an accurate idea of their compliance spending, 53% say that annual expenditure in this area of IT is expanding by over 10% a year.

● Even though this form of spending is growing fast, 46% say that it has not had an effect on expenditure on other forms of IT procurement, and 27% believe that it has actually increased this type of spending. Only 9% say it has decreased.

● The role of IT departments in compliance efforts varies widely. A full 62% of respondents say that the IT department focuses on the system requirements of compliance programmes, a traditional role. But 36% say IT is involved at a strategic level with the company's response and almost 25% say IT is permanently represented on the core compliance team (executives could choose more than one type of role).

● The degree to which companies outsource their compliance processes also varies. Fully 44% of respondents do not outsource this IT element , but 29% outsource more than one-tenth of their compliance effort. Executives may have relied heavily on outsourcing to comply with Section 404 of SOX, at least in the initial stages, and may now be trying to reduce the amount of outsourcing. Many IT departments are hiring compliance specialists answerable to the CIO.

● Companies seem fairly satisfied with the results of their IT compliance investment, but their expectations are moderate, at least for 66% of respondents.

● The IT department faces a number of challenges in implementing a compliance strategy. Foremost among them, respondents say, is that their current technology does not address the company's compliance needs. In second place is the response that their current hardware technologies will not scale to meet long-term compliance requirements. Third is a lack of understanding of the needs of other departments, and in fourth place is the opinion that their existing software will not scale to meet long-term needs.

● On the question of whether compliance spending should be focused on automation or employee training, 44% of respondents - the largest portion – say it should be focused on both. This suggests that companies see the major benefits that come from automation, but that such systems cannot remove the human element entirely, or even run smoothly without carefully teaching people how to operate them.

● The use of IT in compliance is leading to a greater centralisation of compliance efforts and this presents challenges, especially for companies operating in multiple jurisdictions.

The use of IT in compliance

In the past three years, the role of IT has increased in many areas of compliance, in particular in the following:

- **privacy and security**—mostly in the protection of computer-based information and networks;
- **document retention**—dealing with a vast number of documents created and stored digitally;
- **financial regulation**—involving many IT-laden processes, as SOX Section 404 compliance efforts have made plain.

A full 45% of respondents say IT's role has "increased greatly" in privacy and security, by far the highest response. Document retention came second with 34% and financial regulation third with 33% (Q.2, see appendix).

It is not a coincidence that these are the areas that require the heaviest investment in technology because, even after setting aside compliance, these are IT-intensive processes. Other aspects of regulation, such as product safety and workplace health, have seen some increase in the role of IT but not nearly as much. Indeed, 75% of respondents said that the role of IT has stayed the same in the realm of environmental regulations over the past three years.

At least two factors explain the growth of IT in the areas of privacy, computer security, document retention and financial regulations.

- These areas have seen rapid regulatory growth which only IT can efficiently address. In the US alone, there are 8,500 federal and state regulations on record management, before voluntary codes are even taken into account. Also, SOX, Basel II, various data privacy initiatives and other new regulations make specific demands on IT.
- Three of the four leading impediments that corporate IT departments face in implementing compliance strategies relate to inadequate or too quickly obsolete technology. Technological limitations are less likely to affect the monitoring of already highly IT-based processes.

This does not mean that IT cannot play a significant role elsewhere. However, it often requires some imagination on the part of executives to see the benefits of investment in technology in fields such as human rights compliance (see sidebar). Indeed, IT's role in compliance is growing in most areas. For example, Roger Louis, chief compliance officer of Genzyme, a US biotechnology and pharmaceutical company, believes there is no low-technology way the company can train sales staff in the array of legal requirements involved in selling a range of pharmaceutical products across 80 national compliance regimes. As Jean Holley, CIO of Tellabs, a US-based communications technology company, says: "IT is the *how* part of compliance."

Counting the cost

One reason for the growth in the importance of IT in compliance is that companies are spending more on information technology to help deal with the rising burden of regulation. According to 53% of respondents, annual spending on compliance-related IT grew by more than 10% over the past three years compared with the previous three years (Q.11). (Only respondents who thought they had an accurate idea of this spending category were asked to respond to this question.) Admittedly, only 36% of those surveyed said they had an accurate view, but other evidence supports the opinion that large sums are being spent on compliance-related IT. CIO.com estimates that US businesses will spend US$80bn on compliance in the

IT gives shoemakers more than SOX

Human rights compliance for companies sourcing products from the developing world involves satisfying multiple constituencies. Local employment legislation is only the first and often the easiest hurdle. Many groups, such as local factory employees, workforces in a company's Western operations, human rights organisations and consumers, can criticise a company for even the appearance of inappropriate practices.

The apparel industry—with strong brand emphasis, frequent sourcing from these countries and unpredictable customers—is particularly vulnerable.

Reebok, a maker of sports shoes, regularly audits practices at supplier factories around the world. In the past, the results of these social audits were trapped in Word documents, and users inside the company needed more structured access. At the same time, interested outside parties were pressing the company to reveal what it had found out about working conditions.

A decade ago, Reebok's vice-president for human rights, Doug Cahn, and its CIO, Peter Burrows, began to experiment with software solutions that eventually became a web-based program in which social audit results are recorded in a structured but flexible database. Then, other companies benchmarking themselves against Reebok wanted to buy the program. Not a software producer, the company joined with other firms, as well as the National Retail Federation, the Retail Council of Canada and World Monitors (which brought a State Department grant), to create the Fair Factories Clearinghouse (/www.fairfactories.org). The clearinghouse, a non-profit organisation, will supply the software to member companies and, eventually, allow them to share non-competitive findings about workplace conditions with other members.

According to Reebok, it has gained several benefits from the software:
- it gives the company's own purchasers, who must consult the database before sourcing an order, instant, real-time data on whether a factory's practices are acceptable, thus saving time, costs and site visits;
- it helps the company assist intermediary sources to manage their supply chains;
- it has increased consistency across human rights audit reports;
- it allows some automated data collection, although social audits remain largely manual;
- it permits easy comparison of factories over time and highlights any large geographic areas of non-compliance where auditors should focus; and
- it is flexible enough to monitor compliance with environmental rules and US C-TPAT regulations that deal with security at foreign factories producing goods for the American market.

Mr Cahn also hopes that, as companies expand information sharing, they can increase their joint leverage over factories to improve conditions. This issue is likely to grow. As Mr Burrows notes, other sectors that are now adopting the kind of outsourcing that has been the practice of the apparel industry for years do not yet understand that the human rights bar has been raised higher than ever. Creative use of IT can help meet this challenge, while providing other business benefits.

next five years. (Regulatory Compliance: An $80 Billion Opportunity, February 2005 http://www2.cio.com/analyst/report3316.html)

Given these big sums, it is hardly surprising that companies are cost-conscious. More than one-half of our respondents say their compliance investment strategy has been to build upon existing systems and only 6% say they have started from scratch. Even the 6% figure may overstate the situation, as firms aim to incorporate compliance-related IT investment in a thorough revamp that was already taking place. Ron Blakely, CFO for downstream operations at Shell International, notes, for example, that the company was already overhauling its technology "from stem to gudgeon" for other business reasons anyway, and simply included up-to-date compliance controls as part of the overhaul.

It should be noted that many respondents do not have an accurate estimate of spending on compliance-related IT. Fully 64% admit as much (Q.10). It is hard to separate spending on IT for compliance from other forms of technology investment and some of the spending could be counted under other categories.

The role of IT departments in compliance

IT plays an increasingly important role in compliance, and this has added to the responsibilities of the CIO and the CIO's department. In fact, 69% of respondents say that the department's role and influence in compliance programmes has increased either somewhat or greatly (Q.6). At the same time, it seems that compliance-related IT has become too important to be left solely in the hands of the CIO. Given the fact that a chief executive officer (CEO) in the US and elsewhere can be held personally liable for failing to meet financial reporting requirements, a CEO's career relies on having reliable and accurate IT systems.

Responses varied widely in answer to the question of what role the IT department plays in a company's compliance programmes. By far the largest number of respondents—62%—say that the department focuses on the systems requirements associated with the compliance programmes (Q.5). In second place, 36% say that IT is involved at a strategic level in planning the company's response to the growing regulatory burden. Perhaps surprisingly, only 23% believe that the IT department is permanently represented on the core compliance team. This implies that, in many instances, IT will set up a compliance system under instructions from others. Such companies may well be failing to maximise on the expertise of the IT department.

Although IT is playing an increased role in compliance, technology challenges create difficulties when implementing a compliance strategy. When asked to rank the main challenges faced by the IT department, the top challenges cited by survey respondents are as follows:

● technology does not adequately address the company's compliance needs;
● hardware will not scale up to meet long-term compliance needs;
● a lack of understanding of the needs of other departments; and
● software will not scale to meet long-term needs.

Respondents were of course being asked for challenges, and these results should be interpreted in the light of general overall satisfaction with compliance technology. In order to obtain scalable technology to address needs more fully, however, companies may have to rethink the reliance on existing systems and instead invest from scratch.

Another challenge lies in the fact that the compliance role of technology departments is not clear. The IT expert at a leading Australian bank points out that the volume and nature of new regulations are blurring the roles of audit, risk, compliance and IT. He believes that the challenge is to establish a crystal-clear demarcation of roles and responsibilities. Who does what is rarely straightforward. Mr Louis, for example, is the chief compliance officer of Genzyme but had only a small role in the company's SOX-compliance preparations and several banks interviewed off the record had separate departments leading their compliance with SOX and Basel II. Moreover, CIOs who improve security are not just protecting networks but are complying with a range of legislative requirements now seen as part of compliance.

Most importantly, this sharing of responsibilities across functions, if correctly managed, can improve interdepartmental co-operation and help further align IT with business needs. Compliance with SOX and similar regulations has increased company-wide knowledge of business processes and controls. This has helped to foster a much broader understanding of the IT department's activities, a better relationship with other departments and a closer alignment between IT and the rest of the company. Ms Holley explains that at her company, Tellabs, decisions about who has password access to which information is now a business decision, rather than one made by the IT department. She calls this change "a great thing",

because it makes business sense.

Spending decisions are also being shared. A full 43% of respondents say that a combination of departments hold the budget for compliance-related IT purchases (Q.13). Only 33% say that IT is solely responsible. In budget terms, the growing number of rules to be complied with has clearly benefited the IT department. As one participant in our survey puts it: "Budgets once queried or refused are now approved or pushed forward, but for non-IT reasons. We have the toys to resolve other people's problems." Furthermore, IT-related compliance spending does not seem to have hurt other forms of IT spending. Over 46% of survey takers say it has had no effect (Q.12), and 27% believe it has actually increased spending compared with 9% who believe it has decreased it.

Division of labour

IT departments deal with the manpower challenge of compliance in a variety of ways. On one end of the scale, 44% of companies do not outsource compliance at all (Q.9). By contrast, 29% contract out more than 10% of their compliance IT work. The large amount of time dedicated to meeting compliance requirements has resulted in more companies deciding to outsource provision of software, expertise and in some cases even the compliance function. However, several of those interviewed noted that although they had hired outside experts for SOX compliance, they are intending to wean themselves from this dependence as this aspect of compliance becomes more routine. Banco Popular of Puerto Rico has taken a more entrepreneurial approach. It transferred its internally developed expertise in SOX compliance to a wholly owned technology subsidiary, Evertec, to sell its services to other banks.

Outsourcing of compliance expertise is nothing new for IT departments; it is an example of the common preference to buy off-the-shelf technology. A bigger change is the introduction of permanent compliance

staff under the CIO. Every company executive interviewed for this report has either recently created such positions or was considering doing so. In the past year, the number of such employees at Genzyme has risen from zero to 5% of IT staff. Even companies that hired temporary extra staff to help set up processes to comply with SOX are now considering taking on permanent employees. Rob Mankiewitz, head of compliance at Aspen Re, a British reinsurance company, points out that this provides CIOs with their own reassurance that they are obeying the law.

Weighing the benefits

According to the survey, most executives—66%—had moderate expectations with regard to their company's investments in compliance systems and 56% had modest expectations that were met or exceeded (Q.14). Technology is therefore playing a helpful role in compliance. But has compliance-related IT helped companies realise any beneficial side effects? According to the survey results, 30% responded "Yes" and 70% responded that they have not realised additional benefits (Q.7). When the former were asked to provide examples of the benefits, a tenth said that compliance systems had made it easier to abide by the regulations. Other respondents pointed out that newer, faster and more accurate technology, controls, information and archive retrieval all bring their own rewards. These gains include better management oversight, greater efficiency, heightened communication security and better product quality, all of which reduce risk.

In our in-depth interviews, executives stated that the benefits of compliance-related IT investments were "stumbled upon" or "incidental and not measured". They say the benefits include more reliable information, enabling managers to make better-informed decisions, as well as a possible reduction in the cost of raising capital for companies with a good reputation. Although some interviewees are convinced

that these indirect gains are the "only way you can make [such spending] pay out", there is no evidence of widespread strategic attempts to enhance business value through an efficient compliance programme. In fact, these interviews seem to suggest that the difference between the 30% and 70% in the larger survey is not between those who had found such benefits and those who had not, but between those who chose to focus on them and those who have not explored these possibilities. After all, companies are investing in compliance technology with the goal of reducing their risk of legal or other penalties for misbehaviour. It is hard to estimate the precise value of avoiding such penalties, but it is easy to appreciate the consequences of failing to comply. Bankruptcy brought down Enron long before anyone was convicted. As Ms Holley notes, it is possible to calculate how operating without insurance might affect a company's bottom line, "but why would you?"

Moreover, regulations are not written to increase business profitability, even though they can still yield business benefits. Free marketeers would say that if the required actions increased profits, then companies would have adopted them long ago without being forced to. With that said, making it mandatory to wear seat belts saves lives. Similarly, SOX increases corporate accountability and integrity by requiring that companies be definite about the quality and accuracy of their financial information.

IT-related compliance spending can bring significant business benefits to a company. When Netherlands-based Royal Ahold, an international supermarket operator, had to clear up an accounting scandal in 2003 at one American subsidiary, the wholesaler US Foodservice (USF), Ahold ordered an overhaul of USF's IT systems. Although driven by pressing compliance needs, the various programs also allowed it to:

● provide more consistent and accurate treatment of retailer rebates;

● replace the company's nine stand-alone IT systems with an enterprise-wide model;
● provide a single interface for customers to make their ordering easier; and
● integrate supply chain management to improve the efficiency of purchasing and logistics.

It is often difficult to separate the benefits of compliance investment from other IT benefits, but it seems clear that compliance-driven changes can benefit the rest of the company's operations significantly.

Tools need hands

One objective of IT is to improve automation. By reducing human error and the opportunity for malfeasance, compliance is improved. More broadly, regulators increasingly rely on companies to invest in IT in order to adapt to changing standards. One example is the Basel II capital requirements for certain global banks, which would be impossible to comply with if these institutions did not invest in the necessary information technology tools to calculate operational risk. What holds for large banks is also true of small stockbrokers. In January 2005, when the US Municipal Securities Rulemaking Board required notification of every trade of such securities within 15 minutes of the transaction, it had to presume that dealers, most with under 150 employees, had automated systems for reporting.

Many respondents to the survey see no contradiction between investing in compliance-related automation and investing in the training of employees. In fact, employee training is an essential complement to any IT system. Even the most heavily automated systems require people to run them and companies embracing automation are not looking to eliminate humans from compliance but to redeploy people intelligently. Our survey asked executives to choose between the following statements: that compliance should be focused on automation, that

compliance should emphasise training, or both. Just under 44% of respondents, by far the highest percentage, chose both statements (Q.15). Mr Blakely of Shell International pointed out that although IT can provide good controls and eliminate human error, "the more you rely on technology the more you need human experts who understand it". The IT expert at the Australian bank also stressed the need to inculcate a sense of personal ownership of, and accountability for, compliance systems. As Mr Louis said, IT compliance systems are "tools not ends".

E pluribus unum

IT compliance systems, as well as procurement and implementation decisions, are highly centralised. In companies that need to deal with multiple jurisdictions, 67% of respondents have focused on building a company-wide compliance system rather than one based on individual jurisdictions (Q.19). In addition, 65% of all respondents manage compliance procurement and implementation of compliance IT from the centre (Q.20), whereas only 14% seek to decentralise. The most common arrangement is to try to create a universal compliance regime with national or local modifications added on only where absolutely necessary. The attractions of this approach are considerable: a single company-wide system is easier and less expensive to implement, maintain and protect, and has simpler processes to understand. All

these factors increase its usefulness along with its ability to pass regulatory muster. Adjusting global compliance systems for national or local needs, however, is not easy. Tellabs finds this the most difficult part of IT-related compliance.

Centralisation also compounds the widespread concern of executives about the difficulty in meeting regulations arising in jurisdictions outside the company's home country. Most major companies, and 76% of those surveyed, with operations or share listings in several countries, face multiple sets of regulation. Washington's—or even the New York District Attorney's—writ runs in offices in Johannesburg and Singapore, just as Brussels' does in Seattle. "Global" compliance systems, however, are almost inevitably based on a company's home country legislation and then adapted to comply with other countries' regulations. The next generation of compliance technology may need greater flexibility to deal with differences in regulations between countries.

Another danger is the increased risk of any single failure resulting in severe consequences. Mr Blakely points out that when Shell had approximately 150 country-based business platforms, a failure on one was merely a headache. Now that the company is shifting to a centralised and unified platform, a failure would entail far more dramatic problems. This illustrates the need for appropriate IT investments to lessen the potential risks arising from centralisation and standardisation.

Conclusion

The application of IT is growing across most fields of compliance, and is increasing rapidly in highly IT-reliant business areas. IT-related compliance costs are rising quickly, even if it is difficult to determine figures with precision.
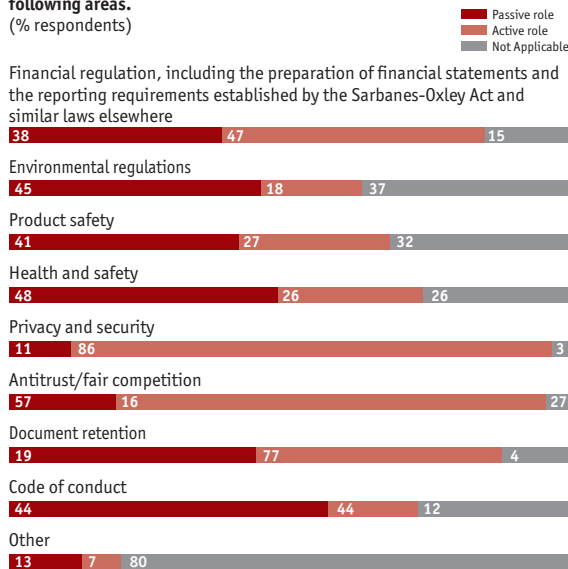
The increased use of IT in compliance is placing heavier responsibilities on the IT department itself, as well as blurring the demarcation between functions. Increased use also seems to be improving IT's general business alignment. Recent regulatory demands have driven some IT departments to hire outside experts. At the same time, however, the employment of a full-time, dedicated compliance staff looks increasingly permanent and the numbers of people working in-house on compliance is likely to grow. The volume and types of new regulations are leading companies to adopt automated systems, but automation is not obviating the need for human controls in the field of compliance. Rather, IT is complementing the role of humans.

Companies generally are satisfied with what they are receiving in return for their investment. The benefits of IT in compliance include time and labour saved, greater transparency, greater control over processes, and heightened accuracy and reliability of information. All of these benefits can help a company's reputation, brand equity, investor and shareholder confidence, and customer/partner/supplier relationships. However, often these are unplanned or additional benefits realised, as the primary goal of IT in compliance is to help companies abide by the rules. Even those who see additional benefits do not appear to be seeking them intentionally. If compliance-related IT investments had directly helped companies increase the bottom line before new regulations were introduced, companies would have invested in this technology years ago. Nevertheless, quantitative and qualitative benefits exist, planned or unplanned, positioning technology as a means of enhancing corporate value.
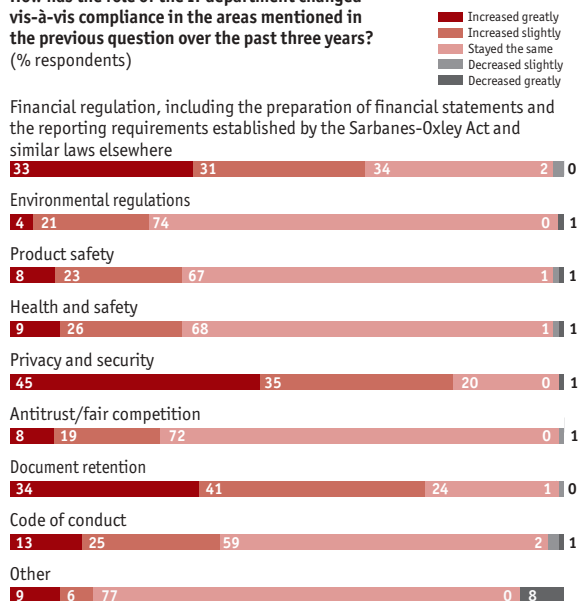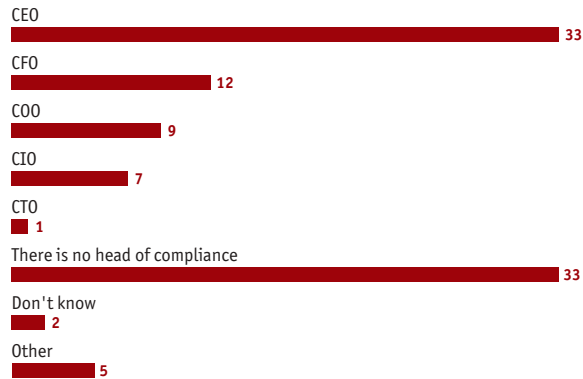
Number of respondents: 132

Q1
Describe the role the IT department plays in monitoring compliance in the following areas.
(% respondents)

- Passive role
- Active role
- Not Applicable

Financial regulation, including the preparation of financial statements and the reporting requirements established by the Sarbanes-Oxley Act and similar laws elsewhere
38 | 47 | 15

Environmental regulations
45 | 18 | 37

Product safety
41 | 27 | 32

Health and safety
48 | 26 | 26

Privacy and security
11 | 86 | 3

Antitrust/fair competition
57 | 16 | 27

Document retention
19 | 77 | 4

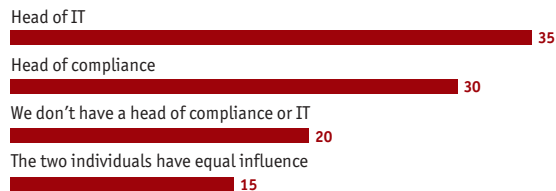Code of conduct
44 | 44 | 12

Other
13 | 7 | 80

Q2
How has the role of the IT department changed vis-à-vis compliance in the areas mentioned in the previous question over the past three years?
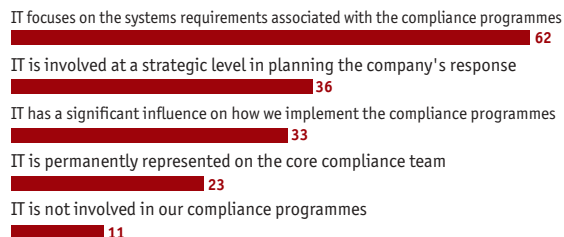(% respondents)

- Increased greatly
- Increased slightly
- Stayed the same
- Decreased slightly
- Decreased greatly

Financial regulation, including the preparation of financial statements and the reporting requirements established by the Sarbanes-Oxley Act and similar laws elsewhere
33 | 31 | 34 | 2 | 0

Environmental regulations
4 | 21 | 74 | 0 | 1

Product safety
8 | 23 | 67 | 1 | 1

Health and safety
9 | 26 | 68 | 1 | 1

Privacy and security
45 | 35 | 20 | 0 | 1

Antitrust/fair competition
8 | 19 | 72 | 0 | 1

Document retention
34 | 41 | 24 | 1 | 0

Code of conduct
13 | 25 | 59 | 2 | 1

Other
9 | 6 | 77 | 0 | 8

Q3
Whom does the head of compliance report to?
(% respondents)

CEO — 33
CFO — 12
COO — 9
CIO — 7
CTO — 1
There is no head of compliance — 33
Don't know — 2
Other — 5

Q4
Which individual has more influence in the decision-making process for compliance-related purchases?
(% respondents)

Head of IT — 35
Head of compliance — 30
We don't have a head of compliance or IT — 20
The two individuals have equal influence — 15

Q5
What role does the IT department play in your company's compliance programmes?
(% respondents)

IT focuses on the systems requirements associated with the compliance programmes — 62
IT is involved at a strategic level in planning the company's response — 36
IT has a significant influence on how we implement the compliance programmes — 33
IT is permanently represented on the core compliance team — 23
IT is not involved in our compliance programmes — 11

Appendix: Survey results for the role of IT in compliance

Q6
How has the IT department's role and influence in the company's compliance programmes changed in the past three years?
(% respondents)

Increased somewhat
51
Stayed the same
27
Increased greatly
17
Decreased slightly
4
Decreased greatly
0
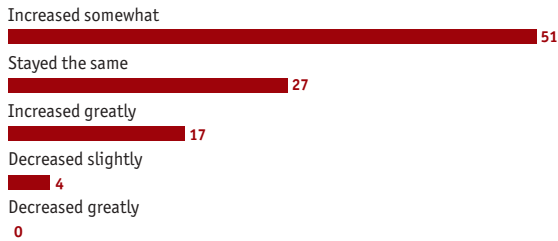
Q7
Have recent IT investments taken as compliance measures produced beneficial side effects?
(% respondents)

Yes **30**
No **70**
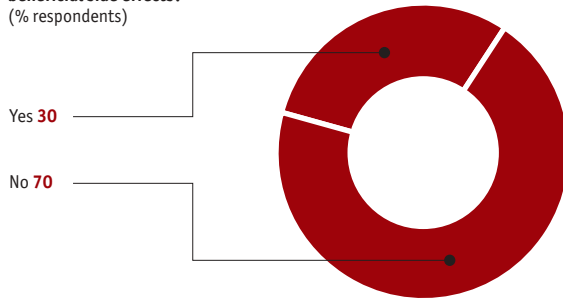
Q8
This is a write-in question.

Q9
How much of the IT element of your company's compliance efforts is outsourced?
(% respondents)

1-5%
5
6-10%
8
11-15%
7
16-20%)
7
More than 20%
16
We do not outsource this IT element
44
Don't know
14
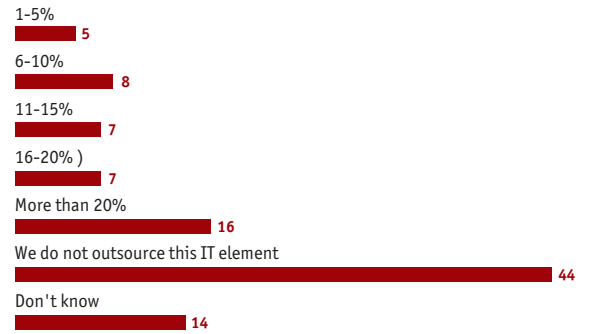
Q10
Does your company have an accurate idea of compliance-related spending, both in the IT department and company-wide?
(% respondents)

Very accurate
7
Fairly accurate
29
Some idea
37
Not very accurate
17
No idea
11
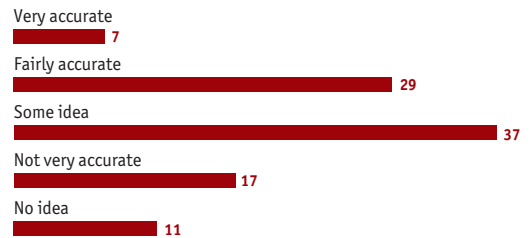
Q11
Please answer this question only if you selected Very accurate or Fairly accurate in Question 10. What was the percentage change in annual spending on compliance-related IT in the past three years compared with the previous three years?
(% respondents)

Increased by 50% or more
11

Increased by 20-50%
18

Increased by 10-20%
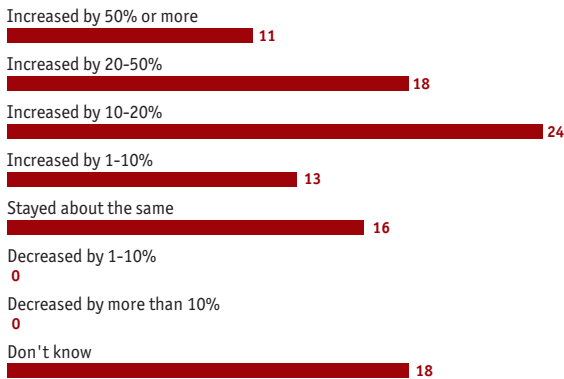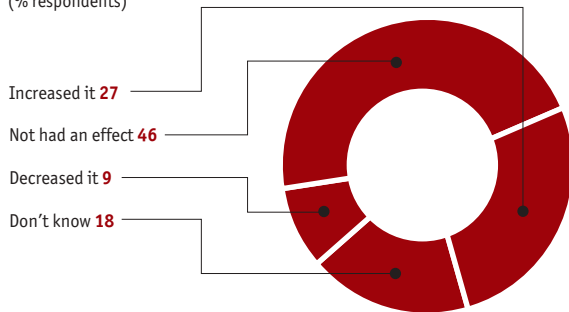**24**

Increased by 1-10%
13

Stayed about the same
16

Decreased by 1-10%
0

Decreased by more than 10%
0

Don't know
18

Q12
How has spending on compliance solutions affected spending on other forms of IT procurement?
(% respondents)

Increased it **27**
Not had an effect **46**
Decreased it **9**
Don't know **18**

Q13
Which department holds the budget for compliance-related IT purchases?
(% respondents)

A combination of departments
43

IT
33

Compliance
12

Legal
6

Other
5
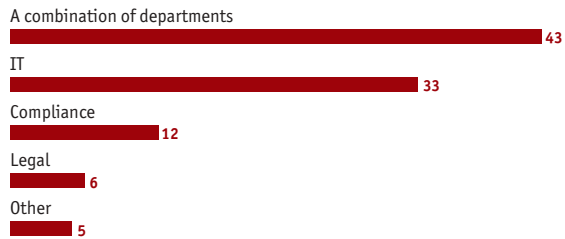
Q14
What were your expectations with regard to your company's investments in compliance systems and have those expectations been met?
(% respondents)

My expectations were moderate and expectations were met
44

My expectations were low and expectations were met
13

My expectations were moderate and expectations were not met
11

My expectations were moderate and expectations were exceeded
11

My expectations were high and expectations were met
6

My expectations were low and the outcome was even worse than I expected
5

My expectations were high and expectations were not met
5

My expectations were low and expectations were exceeded
3

My expectations were high and expectations were exceeded
1

Q15
Which of the following statements best reflects your company's views on compliance spending?
(% respondents)

Compliance spending should be focused on automated systems that remove the human element from monitoring the company's adherence to the rules. **14**

Compliance spending should be focused on training employees and building reporting systems that require the active participation of the workforce. **33**

Both statements represent the company's views. **44**

Neither statement respresents the company's views. **9**

Q17
Is it your compliance investment strategy to build on existing investments and infrastructure or to start from scratch?
(% respondents)

Building on existing IT systems **56**

Build new IT systems **6**

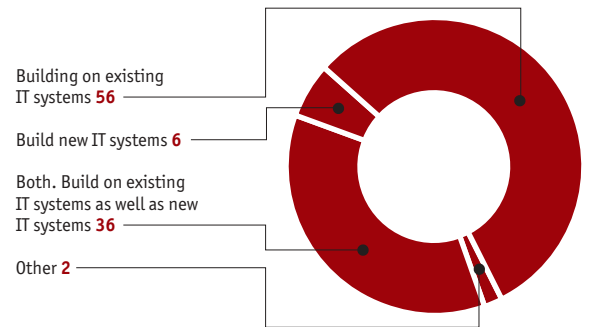Both. Build on existing IT systems as well as new IT systems **36**

Other **2**

Q16
In which of the following areas has your company increased or made new investments in compliance projects over the past three years?
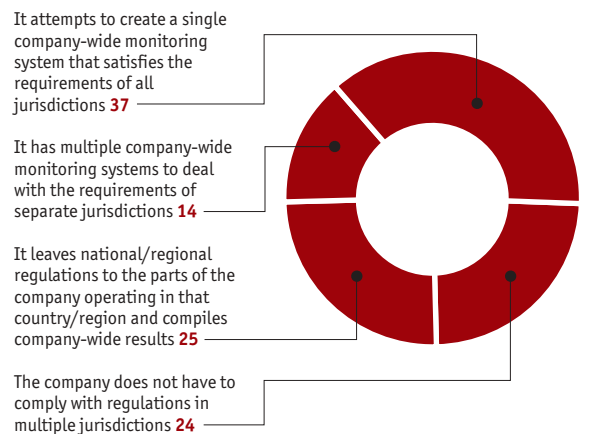(% respondents)

Employee training
67

Adapting existing IT systems
61

New IT systems
42

Revising products and services to meet new regulatory requirements
36

Starting or expanding the compliance department
29

Employing specialists in risk analysis
27

Other
2

Q19
How does your company comply with regulations in multiple jurisdictions?
(% respondents)

It attempts to create a single company-wide monitoring system that satisfies the requirements of all jurisdictions **37**

It has multiple company-wide monitoring systems to deal with the requirements of separate jurisdictions **14**

It leaves national/regional regulations to the parts of the company operating in that country/region and compiles company-wide results **25**

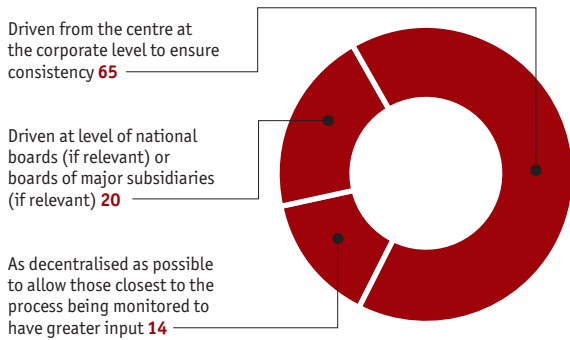The company does not have to comply with regulations in multiple jurisdictions **24**

Please rank the top three challenges for your company's IT department in implementing a compliance strategy.

	1	2	3	4	5	6	7	8	9	10	Rank
The technology does not adequately address my company's compliance needs	35	15	9	62	9	2	0	1	0	0	1
Hardware will not scale to meet long-term compliance needs, which means hardware will have to be regularly replaced	6	27	8	24	60	8	0	0	0	0	2
Software will not scale to meet long-term compliance needs, which means software will have to be regularly replaced	11	8	36	11	12	51	4	0	0	0	3
Lack of understanding of the needs of other departments	13	17	20	25	20	13	24	1	0	0	4
Lack of understanding of the regulatory requirements	21	16	12	4	26	19	25	10	0	0	5
Lack of resources to address all compliance needs	26	17	11	1	6	35	19	14	3	1	6
Poor communication	10	12	10	1	0	4	57	32	7	0	7
Lack of corporate integration	8	17	16	5	0	1	3	72	9	2	8
Turf battles	2	2	11	0	0	0	1	3	112	2	9
Other	1	2	0	0	0	0	0	0	2	128	10

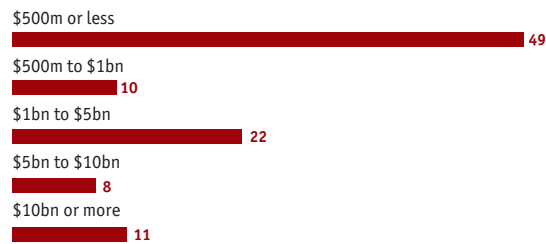**How centralised is the procurement and implementation of compliance IT systems**
(% respondents)

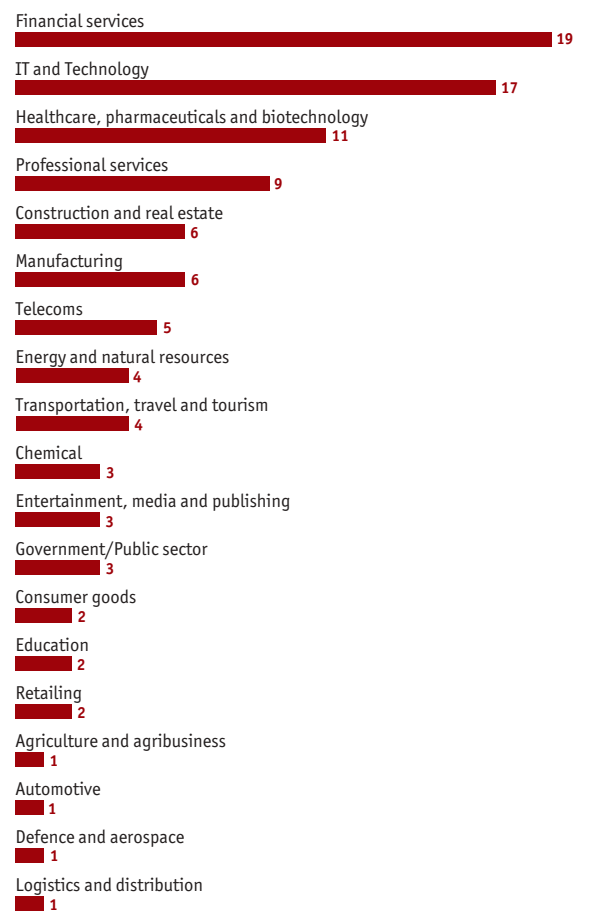Driven from the centre at the corporate level to ensure consistency **65**

Driven at level of national boards (if relevant) or boards of major subsidiaries (if relevant) **20**

As decentralised as possible to allow those closest to the process being monitored to have greater input **14**

Demographics

In which region are you based?
(% respondents)

Asia-Pacific
34

North America
32

Western Europe
23

Eastern Europe
7

Latin America
2

CIS (Commonwealth of Independent States)
1

Middle East and North Africa
1

Sub-Saharan Africa
0
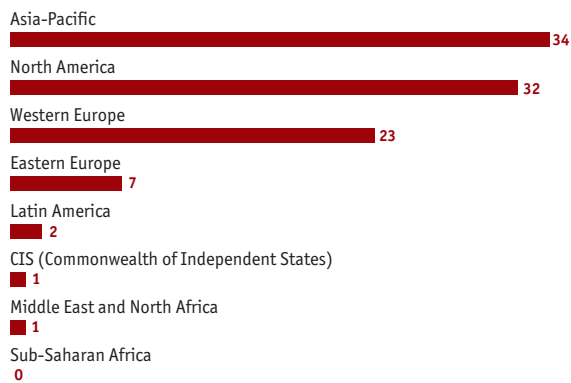
What are your organisation's global annual revenues in US dollars?
(% respondents)

$500m or less
49

$500m to $1bn
10

$1bn to $5bn
22

$5bn to $10bn
8

$10bn or more
11

What is your primary industry?
(% respondents)

Financial services
19

IT and Technology
17

Healthcare, pharmaceuticals and biotechnology
11

Professional services
9

Construction and real estate
6

Manufacturing
6

Telecoms
5

Energy and natural resources
4

Transportation, travel and tourism
4

Chemical
3

Entertainment, media and publishing
3

Government/Public sector
3

Consumer goods
2

Education
2

Retailing
2

Agriculture and agribusiness
1

Automotive
1

Defence and aerospace
1

Logistics and distribution
1

What are your main functional roles? Please choose no more than three functions.
(% respondents)

General management
40

Strategy and business development
39

Marketing and sales
27

Finance
23

IT
21

Risk
13

Information and research
11

Operations and production
10

Customer service
8

R&D
8

Procurement
5

Supply-chain management
5

Human resources
2

Legal
2

Other
8
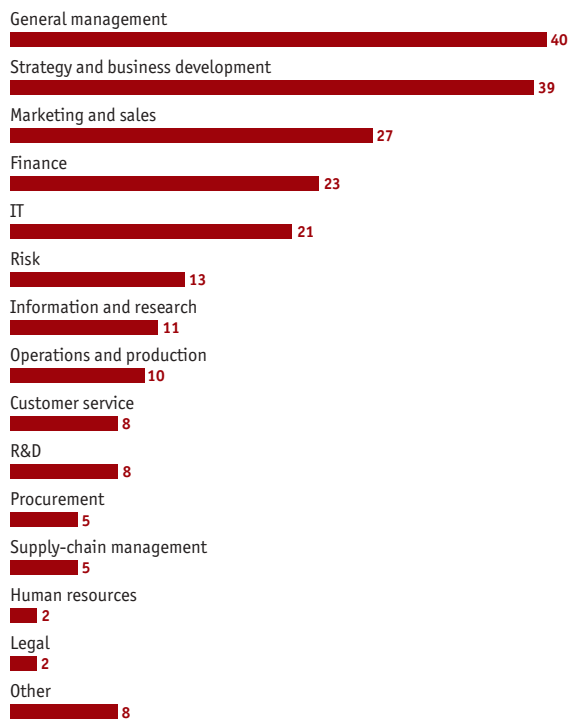
Which of the following best describes your title?
(% respondents)

Board member
6

\CEO/President/Managing director
17

CFO/Treasurer/Comptroller
12

CIO/Technology director
7

Other C-level executive
8

SVP/VP/Director
15

Head of Business Unit
11

Head of Department
5

Manager
14

Other
6
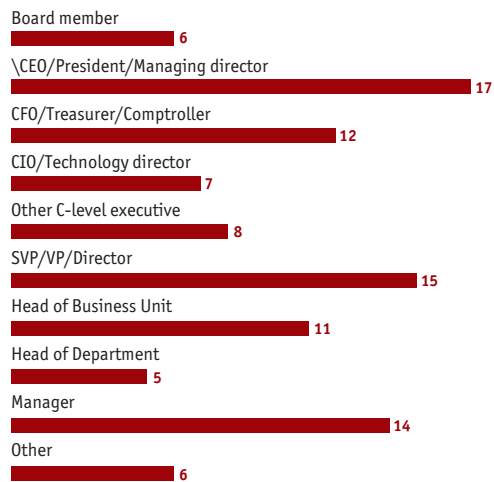
In which country are you personally based?
(% respondents)

United States of America
25

Australia
9

India
8

Canada
7

United Kingdom
7

China
4

Hong Kong
4

Singapore
3

Finland
2

Other
31