What Auditors Think about Crypto Technologies

Sponsored by Thales eSecurity

Independently conducted by Ponemon Institute LLC

Publication Date: March 2011

What Auditors Think about Crypto Technologies

Ponemon Institute, March 2011

Part 1. Executive summary

Ponemon Institute is pleased to present the findings of *What Auditors Think about Crypto Technologies,* sponsored by Thales eSecurity. We surveyed 505 auditors of information security systems, information security auditors, qualified security assessors and EDP auditors. The purpose of this research is to examine what auditors think about crypto technologies as applied to data protection and compliance activities in private and public organizations.

Why are auditor opinions important? By virtue of their role, auditors identify areas of greatest risk and influence how organizations achieve their security objectives and mission. We believe there are very few research studies that seek out the opinions of auditors who have a unique perspective on the success or failure of today's security strategies – which includes the use of crypto technologies such as encryption, tokenization and PKI.

The survey focused on the following issues:

- The experience of auditors participating in the study.
- The difficulty and importance of an organization's compliance with specific requirements as defined by internal and external compliance standards such as ISO, NIST, PCI DSS and many others.
- The perceptions of auditors concerning data protection and crypto solutions.

Following are some of the most salient findings of this research.

- A large number of respondents say their organizations are not taking data security seriously, and may not be allocating enough resources to achieve a reasonable state of compliance with laws and regulations, as well as a high security posture.
- In the world of compliance, business units rather than legal, IT or compliance, own the budget and thus determine whether or not to invest in audits.
- Audits may be failing in the areas that pose the greatest threat or risk to organizations.
- The primary purpose of audits appears to be the identification of risks and vulnerabilities rather than to determine compliance with policies, laws or contractual agreements.
- Respondents say that restricting access to confidential data on a on a need-to-know basis is a very difficult compliance requirement to achieve. Other difficult requirements include the need to maintain secure systems and applications and protecting confidential data at rest (in storage).
- Encryption is the hands-down favorite technology for achieving data protection compliance. In fact, the overwhelming majority of respondents believe an organization's information assets cannot be fully protected without encryption or other crypto solutions.
- Encryption rather than tokenization, suppression or masking appears to be viewed by respondents as the best technology for securing databases, data in storage, data in applications and data at point of capture (such as POS systems).
- Respondents admit that despite a favorable response to encryption, key management can be very challenging in terms of meeting compliance requirements.
- Respondents express uncertainty about whether encrypted data in various venues is out-of-scope for most compliance audits.

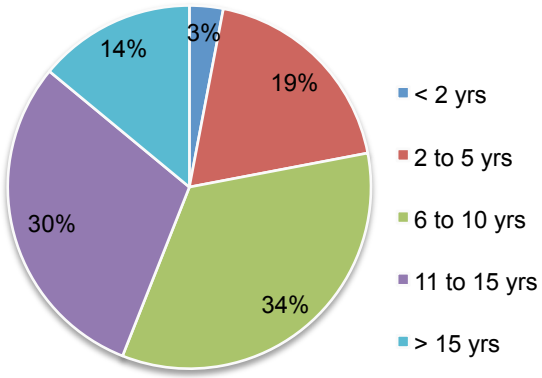
The next section provides more detail to these and other findings from our research study involving information system auditing professionals.

Part 2. Key findings

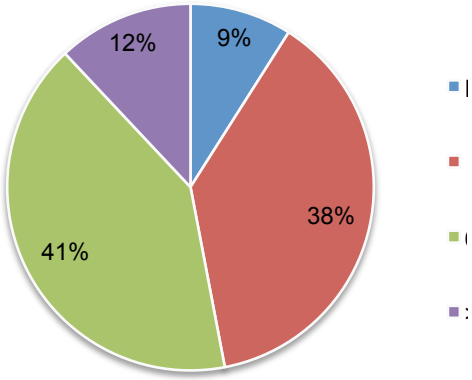
We have organized this paper around the following topics: auditors' experience and knowledge about data security and compliance, auditors' observations about the practices of organizations they work with and the use of crypto technologies to achieve compliance and data security.

Auditors participating in this study have a deep level of knowledge and experience. Sixty-four percent (30+34) of auditors participating in this study have 10 or more years of relevant work experience auditing or assessing data security compliance and related controls or systems (Pie Chart 1). Fifty-three percent (41+12) of respondents have participated in at least six audits or assessments within the past 12 months (Pie Chart 2). The top certifications are CISA and CISSP.

Pie Chart 1
Years of relevant work experience

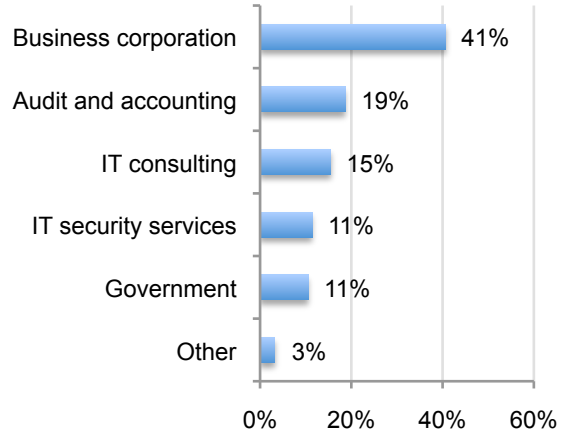


Pie Chart 2
Number of audits conducted over the past year

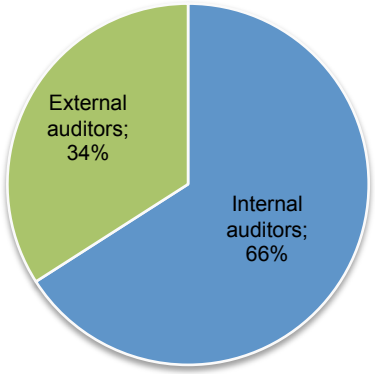


Forty-one percent of respondents work for a corporation and 19 percent work for an audit and accounting firm (Bar Chart 1). Fifteen percent work for IT consulting firms. Pie Chart 3 shows two-thirds are internal auditors and one-third external auditors. Auditors are "external" if they work for a professional services firm (including QSAs).

Bar Chart 1
Respondents' organizations

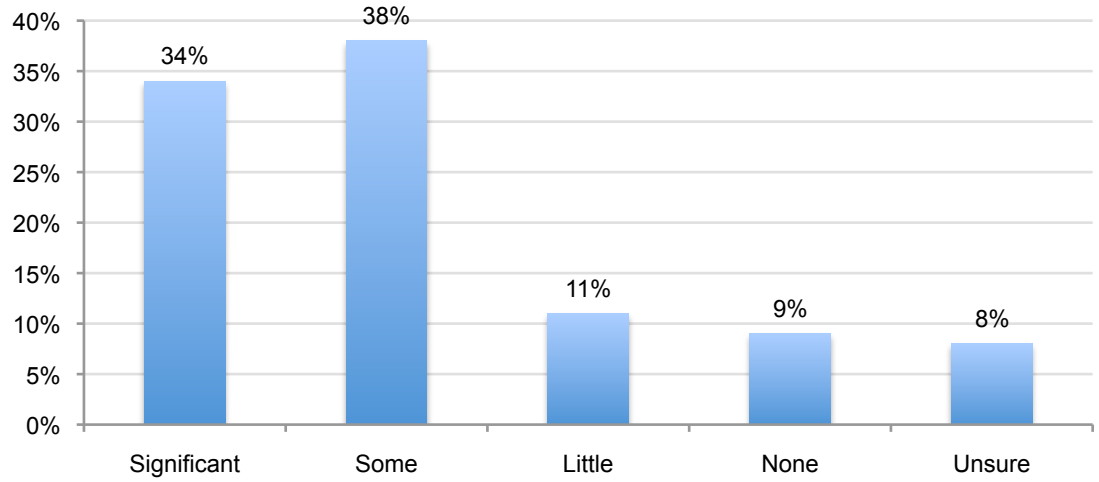


Pie Chart 3
External vs. internal auditors



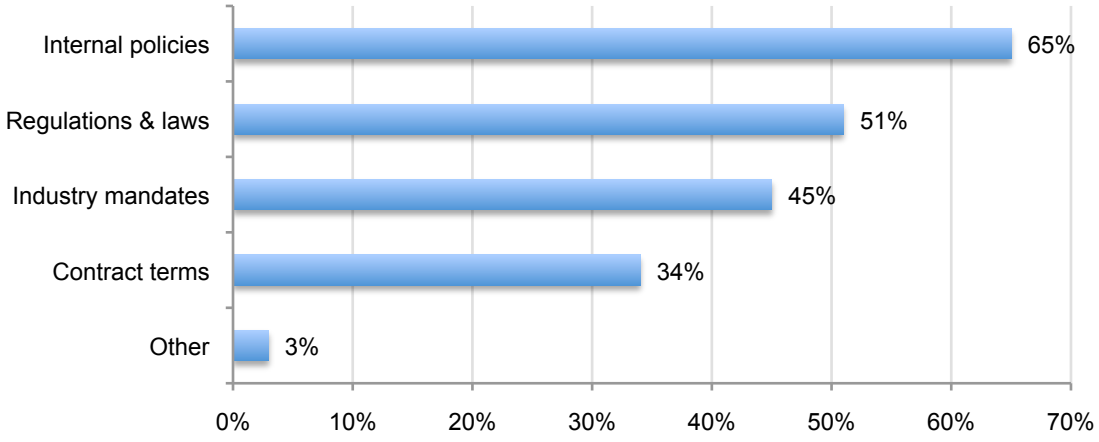
Auditors are favorably influenced by the use of crypto technologies, as shown in Bar Chart 2. The use of such technologies such as encryption or PKI seems to support the adequacy of an organization's security strategy.

Bar Chart 2
How the use of crypto solutions favorably influences auditor perceptions



Internal policies are most often used by auditors to determine data security compliance (Bar Chart 3). These are followed by government rules such as HIPAA, GLBA, FISMA, FTC rules and industry mandates such as PCI DSS.

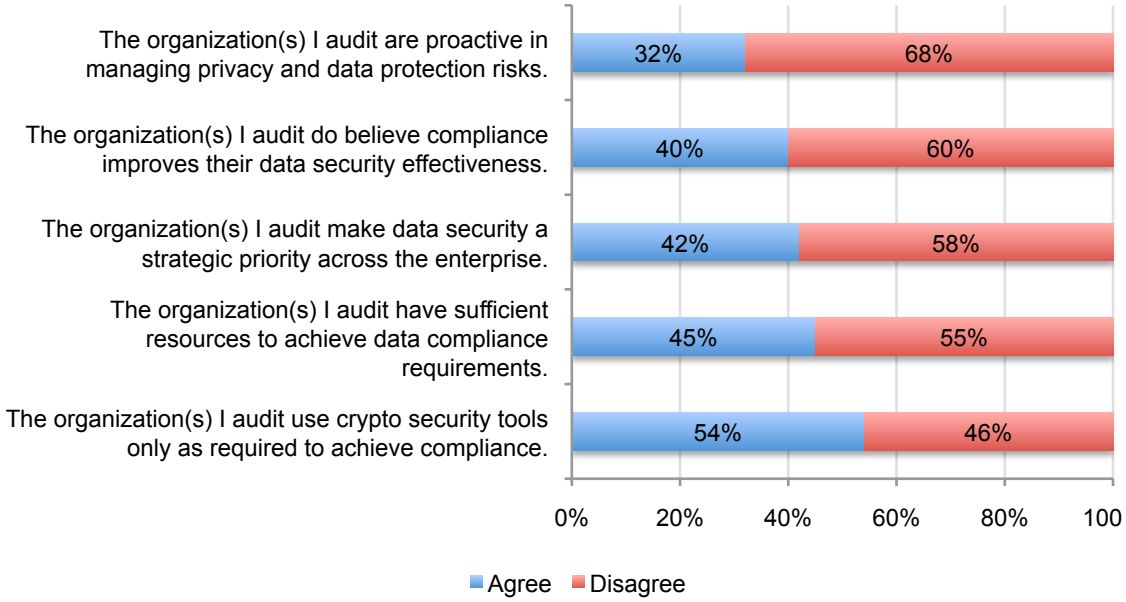
Bar Chart 3
Standards used by auditors to assess data security compliance



Organizations' data security strategies seem to be focused mostly on compliance. Based on their experience auditing organizations, the majority of auditors agree that data security is not a priority and resources are insufficient to achieve data compliance requirements. As noted in Bar Chart 4, only 32 percent say the organizations they audit are proactive in managing privacy and data protection risks.

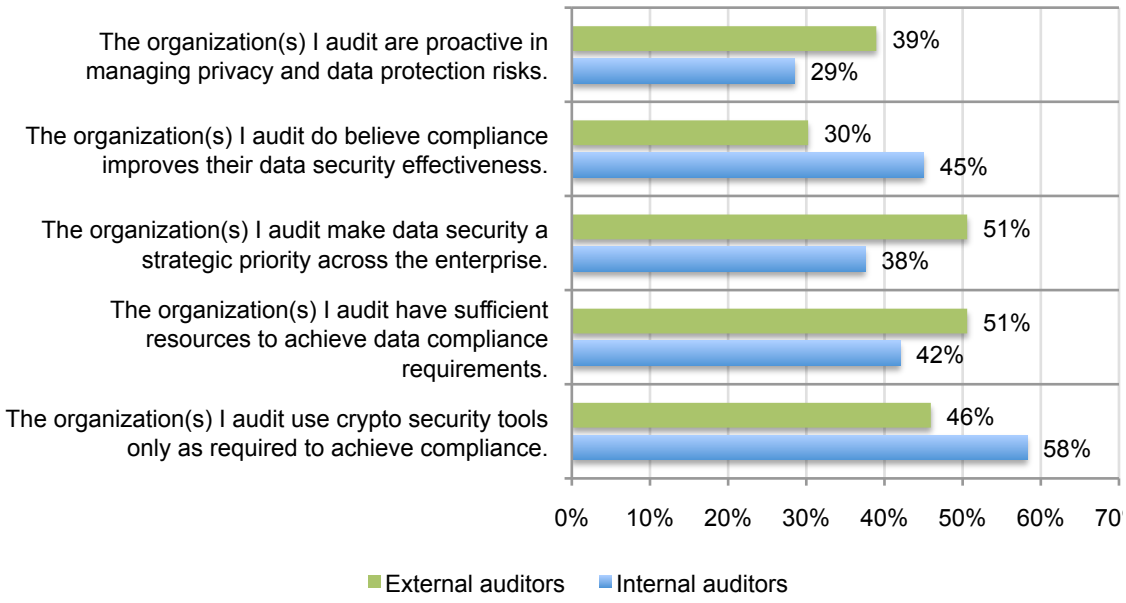
Despite the agreement among auditors that organizations are mostly focused on compliance, 60 percent of auditors surveyed agree that the organizations they audit do not believe compliance improves their data security effectiveness. Moreover, 54 percent agree the organizations they audit use crypto security tools only as required to achieve compliance.

Bar Chart 4
Respondents' perceptions about the state of compliance of organizations they audit



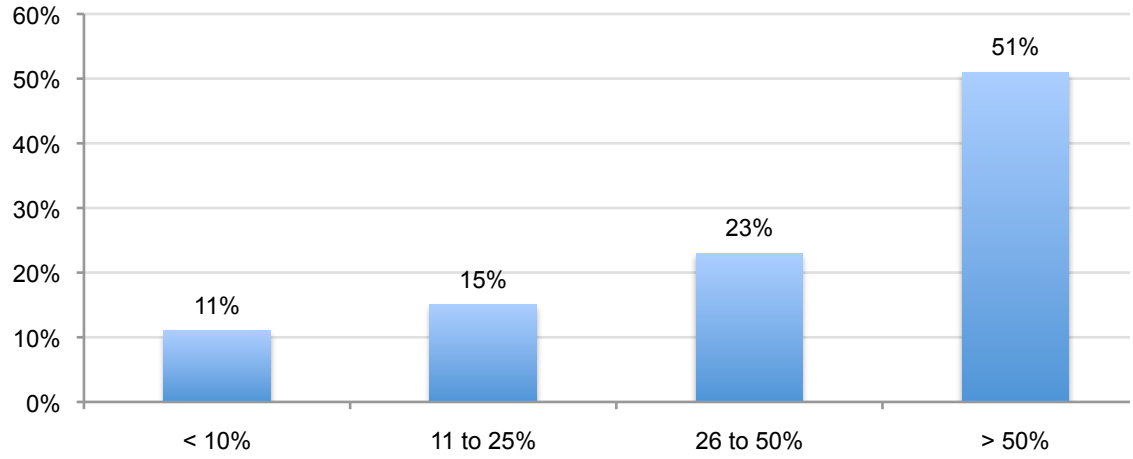
Bar Chart 5 reports internal and external auditors' agreement with five attributions about the state of privacy and data security compliance. With the exception of one attribution dealing with the belief that compliance improves security effectiveness, internal auditors tend to have a more negative or jaundiced view than external auditors.

Bar Chart 5
Comparison of internal and external auditor perceptions about the state of compliance



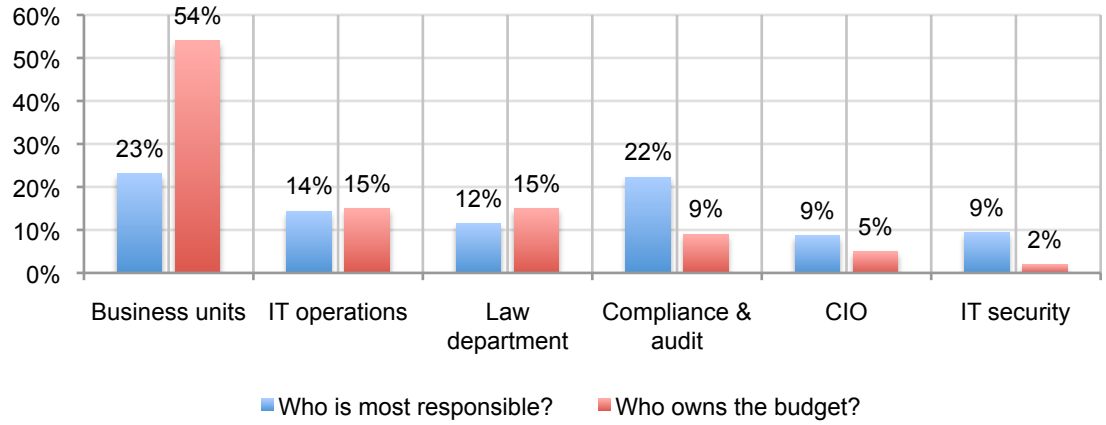
As a consequence of not making data security more of a priority, 51 percent of the auditors surveyed say that on average more than 50 percent of audits they have conducted have had serious deficiencies or failed data security compliance requirements. Bar Chart 6 summarizes the audit failure rates experienced by respondents.

Bar Chart 6
Percentage of audits that had serious deficiencies or failed compliance requirements



Business units continue to own compliance audit or assessment budgets. Consistent with an earlier study (sponsored by Thales)[1] 54 percent of auditors say business unit leaders own the compliance budget (including audits). This is followed by 15 percent who say legal or IT operations own the compliance budget.

Bar Chart 7
Responsibility for the data protection compliance budget

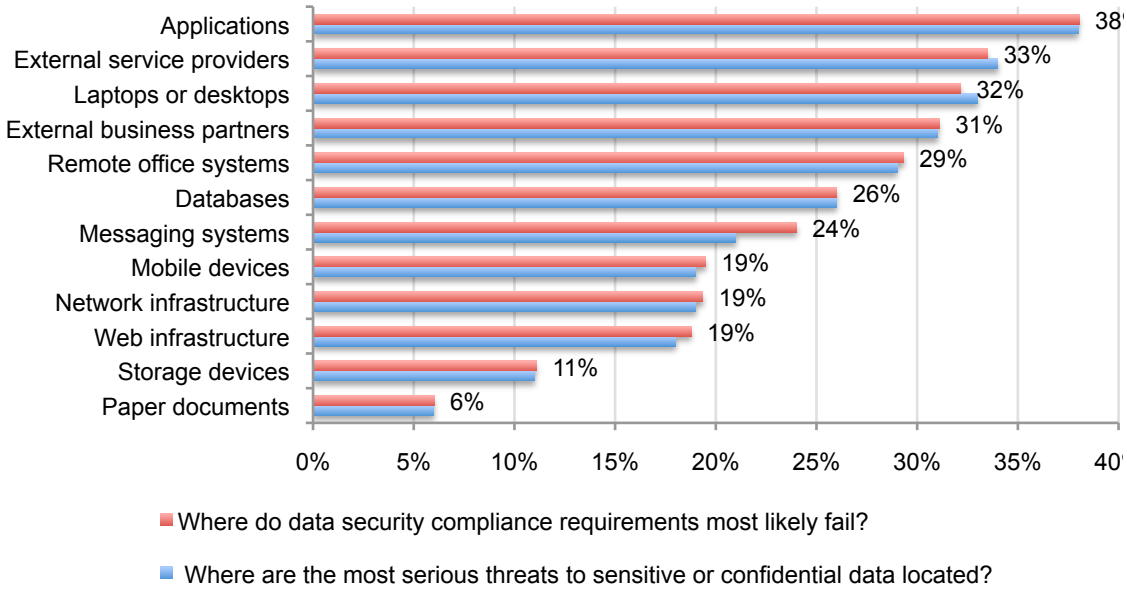


Twenty-three percent of auditors say the business unit leader is most responsible for ensuring compliance, followed by 22 percent who say it is the compliance/audit function and 14 percent who say IT operations. Only 9 percent say the CIO or IT security are most responsible.[2]

As noted in Bar Chart 8, audits are most likely to fail in the areas that pose that greatest threat to organizations' data security.

[1]See 2010 PCI DSS Trends Study Ponemon Institute, February 2010.
[2]In the above study (ibid 1), 30 percent of auditors surveyed said it was the IT security organization.

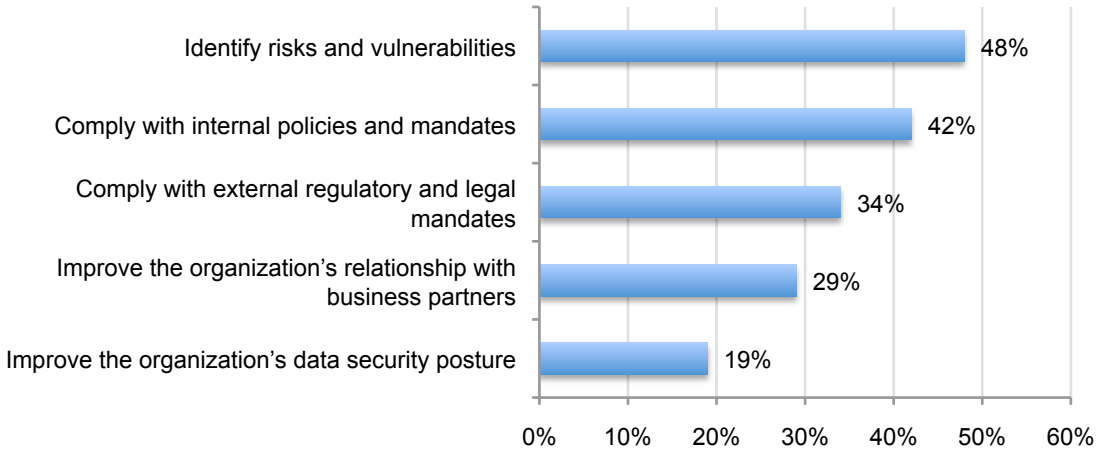
Bar Chart 8
Where compliance requirements fail and where the most serious threats are located



Data security is most at risk in the following areas: applications, external service providers, laptops or desktops and external business partners. These are the areas where data security compliance requirements are most likely to fail. External service providers of greatest risk or threat to the organizations are cloud-computing providers of software as a service, according to 65 percent of auditors. This is followed by outsourcing services and cloud-computing providers of platform services.

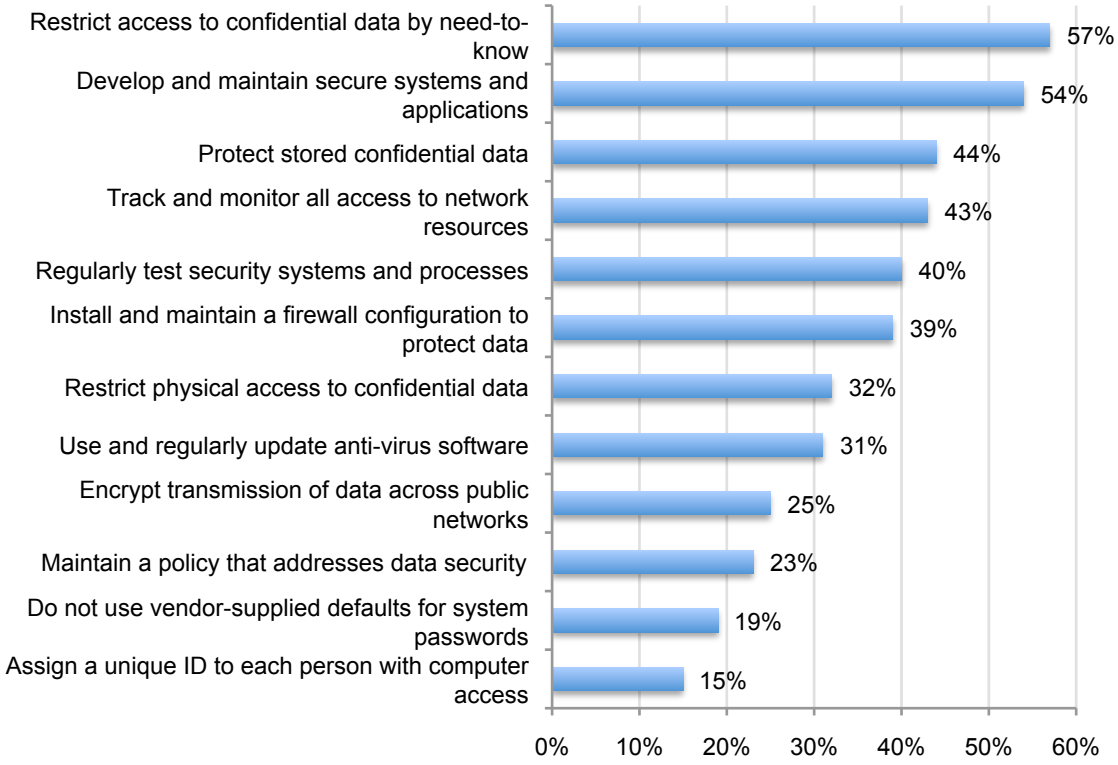
The primary reason for conducting a data compliance audit or assessment is to identify risks and vulnerabilities. Almost half of the respondents (48 percent) say the identification of risks and vulnerabilities is the primary purpose or objective of a data compliance audit. This is followed by 42 percent who say the primary purpose is to determine compliance with policies and mandates. Third-four percent of respondents say it is compliance with external regulatory and legal mandates.

Bar Chart 9
The main reasons for conducting data compliance audits



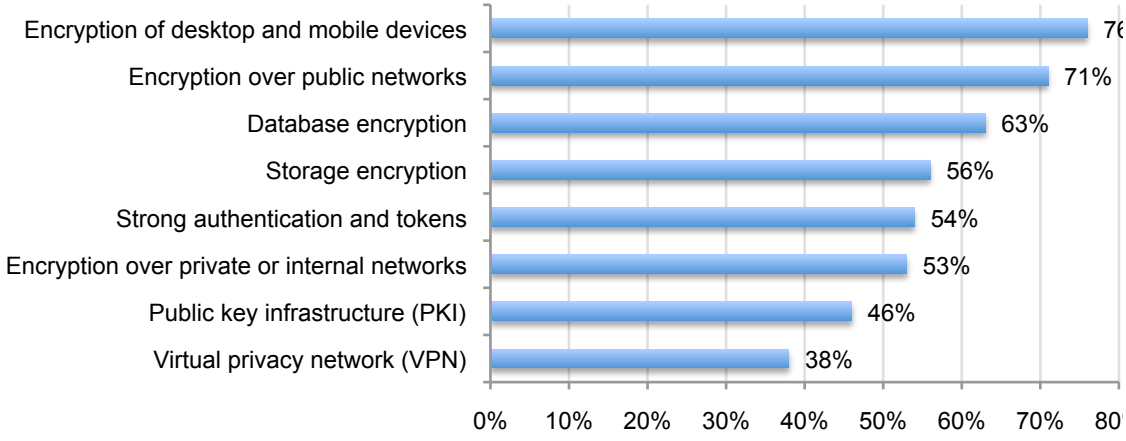
Certain compliance requirements are more difficult to satisfy than others. Specifically, restricting access to confidential data on a need-to-know basis, developing and maintaining secure systems and applications (considered important to an organization's overall security objectives), and protecting confidential data at rest (Bar Chart 10).

Bar Chart 10
The most difficult compliance requirements in descending order
Each bar reflects the very difficult and difficult response combined



Crypto technologies are considered essential and encryption is believed to be the best tool to protect an organization's information assets.

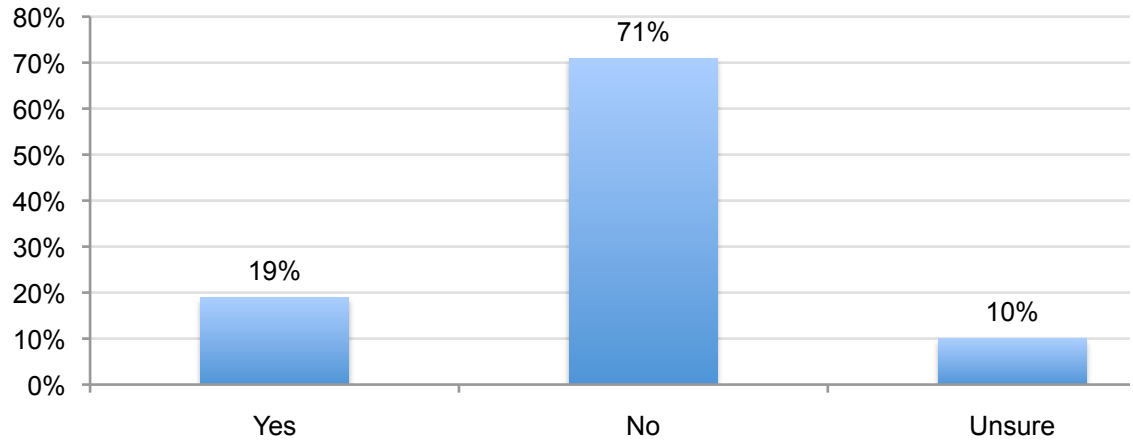
Bar Chart 11
The best crypto technologies for protecting information assets
Each bar defines the high impact response with respect to achieving compliance goals



As shown above, respondents say encryption of desktop and mobile devices (76 percent), encryption over public networks (71 percent) and database encryption (63 percent) are most effective in fostering compliance with an organization's privacy and data protection requirements

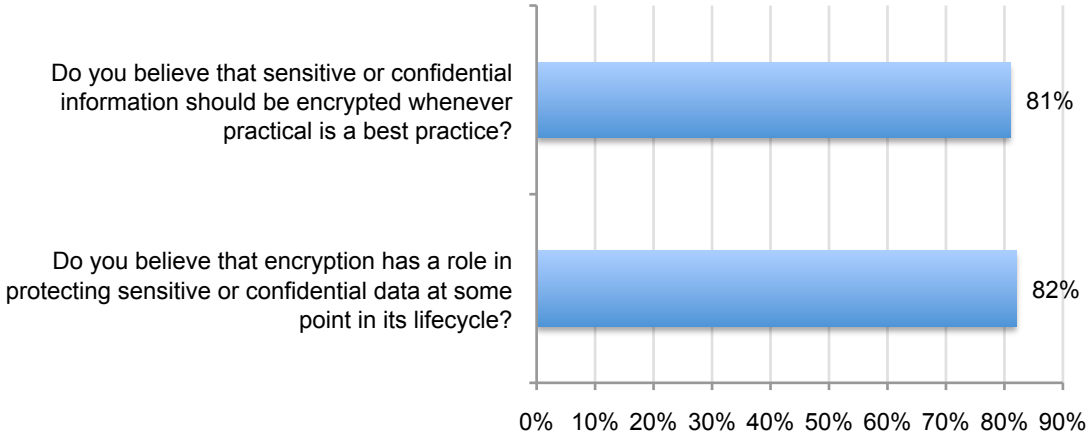
Crypto solutions are considered essential to fully protecting information assets within the corporate boundary (i.e., in-house applications, devices, storage and private networks). Seventy-one percent believe that an organization's information assets cannot be fully protected without the use of crypto solutions (Bar Chart 12).

Bar Chart 12
Can information assets be fully protected without crypto solutions?



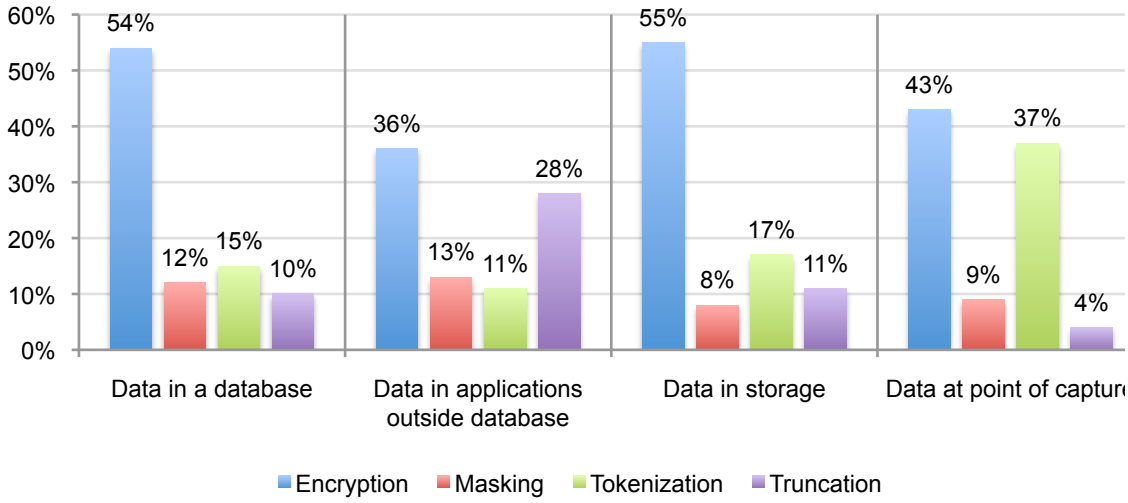
As noted in Bar Chart 13, 82 percent believe encryption has a role in protecting sensitive or confidential data at some point in its lifecycle and 81 percent say this information should be encrypted whenever practical. Business confidential information, health information and financial or accounting information and payment transactions (including credit cards) are the most important types of information to encrypt. More than half (53 percent) do not believe that the convenience of the end-user should be considered when deciding what to encrypt.

Bar Chart 13
Two questions about the role of encryption
Each bar summarizes the percentage Yes response



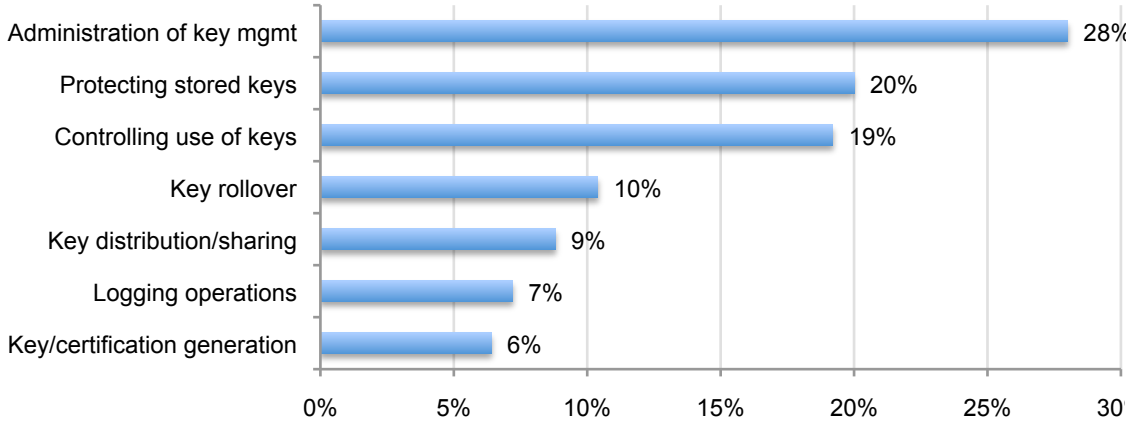
Encryption is considered the best technology to use when securing confidential data in databases, applications, storage, and at the point of capture. To secure confidential data in a database, 54 percent of respondents recommend encryption followed by tokenization at 15 percent. To secure confidential data outside of a database, 36 percent of auditors favor masking followed by 28 percent who favor truncation. When it comes to securing confidential data in storage, 55 percent recommend encryption followed by 17 percent who favor tokenization. Forty-three percent of auditors select encryption for protecting data at the point of capture such as point-of-sale (POS), website, email gateway and call center. The second highest rated in these circumstances is tokenization.

Bar Chart 14
Four data protection technologies in four environments
Each bar shows the technologies considered most effective at protecting data



Encryption and key management for achieving compliance is challenging. As summarized in Bar Chart 15, the most challenging aspect of encryption key management for achieving compliance with privacy and data protection requirements is the administration of key management system (28 percent) followed by protecting stored keys (20 percent) and controlling use of keys (19 percent).

Bar Chart 15
Most challenging aspect of encryption key management



Pie Chart 4 shows 68 percent of the auditors say the use of hardware security modules for encryption and key management reduces the time spent on demonstrating compliance with privacy and data protection requirements. Table 1 reports 46 percent recommend a hardware security module instead of software. Thirty-three percent recommend a hardware security module, but allow software-based encryption and key management.

Pie Chart 4
Does the use of hardware security modules for encryption and key management reduce the time spent on demonstrating compliance?

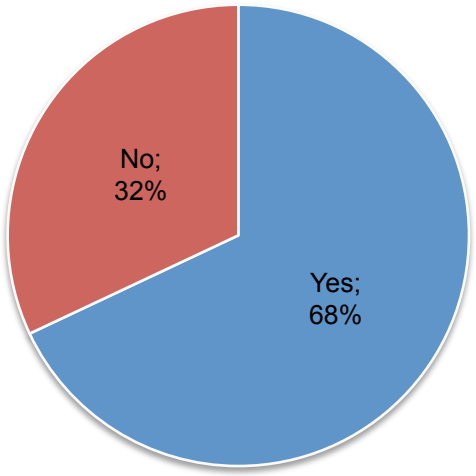
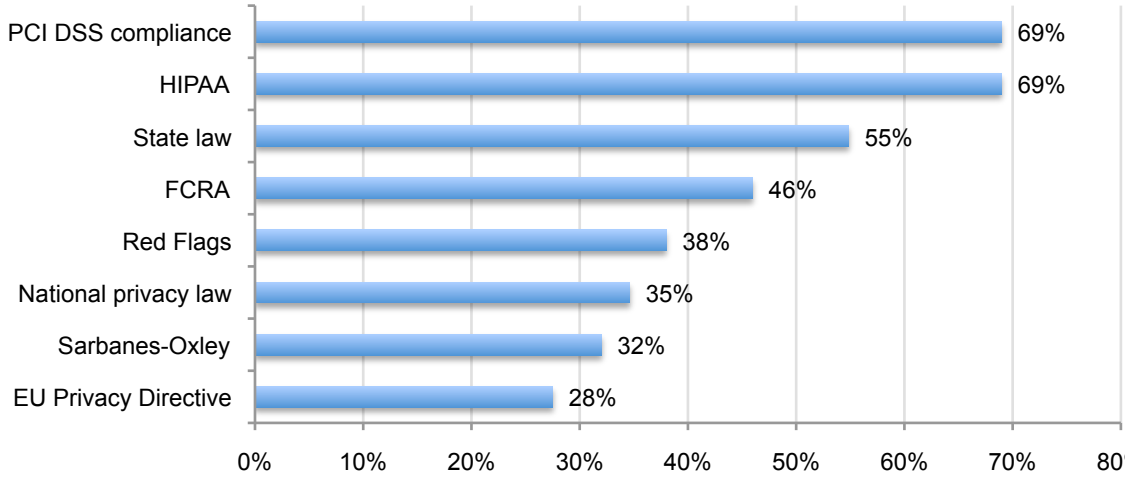


Table 1:
What do you most frequently recommend to your organization or clients for encryption and key management?

Hardware security module used instead of software.	46%
Hardware security module, but allow software-based encryption and key management.	33%
Only software-based encryption and key management.	21%
Total	100%

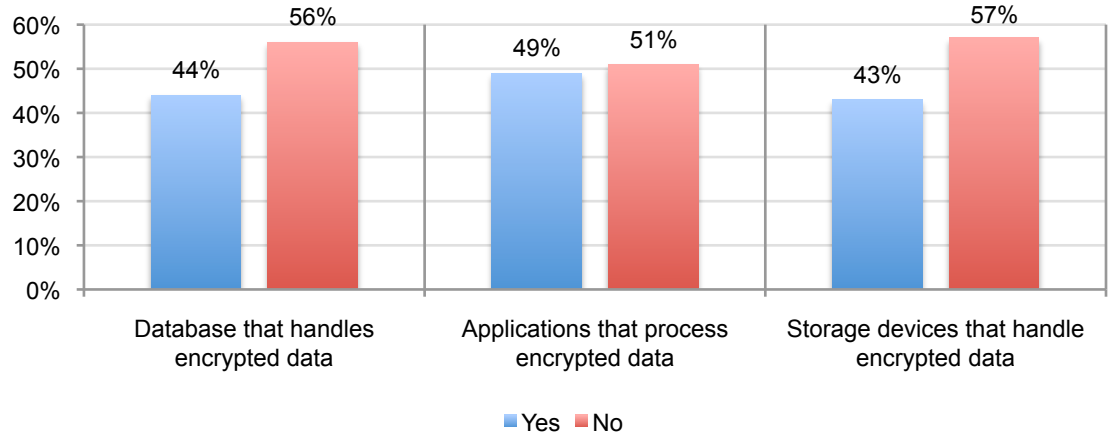
Bar Chart 16 lists data security compliance requirements that motivate the use of crypto security solutions such as encryption, tokenization and PKI. According to respondents, meeting PCI DSS compliance, HIPAA (including HITECH), and various state privacy and data security laws (such as Massachusetts, Nevada, California and others) are the most significant for defining demand for crypto solutions.

Bar Chart 16
Significance of crypto security solutions in meeting compliance requirements
Each bar defines the very significant and significant response combined



There is uncertainty about whether databases, applications and storage devices that handle encrypted data are out-of-scope for purposes of compliance audits. Bar Chart 17 shows 56 percent of auditors surveyed do not consider the database that handles encrypted data to be out-of-scope with audit requirements. Similarly, 57 percent of auditors surveyed do not believe the storage devices that handle encrypted data to be out-of-scope with audit requirements and 51 percent do not consider the applications that process encrypted data to be out-of-scope with audit requirements.

Bar Chart 17
What do respondents consider out-of-scope for purposes of audit requirements?



As a result, it seems clear that there is still confusion in the market regarding the impact that encryption can have in reducing the scope of audits. However, a significant number of organizations are already taking advantage of the opportunity to reduce the overall costs of an audit.

Part 3: Methods

Table 2 summarizes the sample response for this study. As a starting point, we built a sampling frame of nearly 10,000 individuals who had bona fide credentials as an information systems auditor. From this sampling frame, we invited 9,1810 individuals to participate. This resulted in 556 individuals completing the survey of which were rejected for reliability issues. After screening another 15 individuals, our final sample totaled 505 respondents.

Table 2 **Response statistics**	**Freq.**	**Pct%**
Total sample frame	9,956	100.0%
Invitations sent	9,810	98.5%
Total response	556	5.6%
Rejected surveys	36	0.4%
Final sample before screening	520	5.2%
Final sample	505	5.1%

Most respondents (61 percent) held one or more professional credentials or certifications relating to information systems, security and auditing. Forty-six percent of respondents self-report holding the CISA, and 31 percent say they hold the CISSP.

Bar Chart 18
Respondents' professional credentials

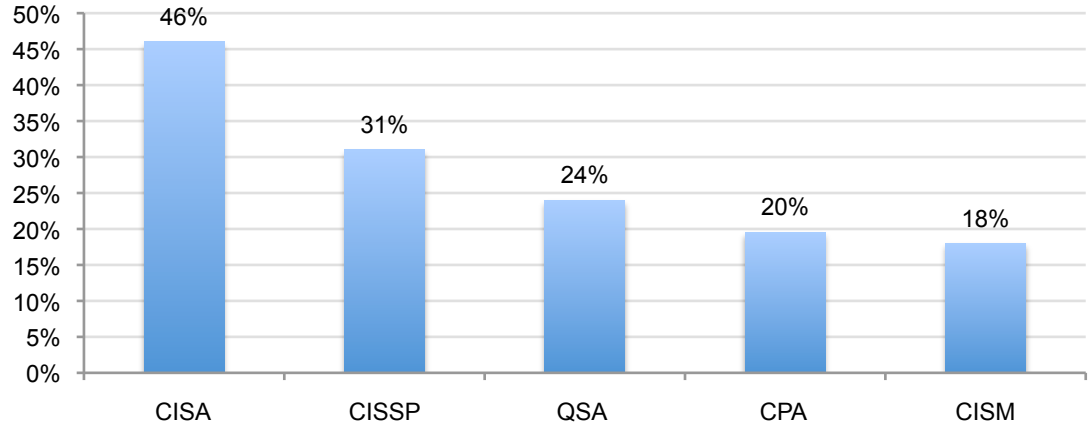


Table 3 shows the headcount (size) of respondents' business companies or government entities. As can be seen, 65 percent of respondents state they work for organizations with more than 5,000 individuals.

Table 3 **The total headcount of respondents' organizations?**	**Pct%**
Less than 100	3%
101 to 1,000	11%
1,001 to 5,000	21%
5001 to 10,000	29%
10,001 to 25,000	16%
25,001 to 75,000	8%
More than 75,000	12%
Total	100%

Pie Chart 5 shows the industry distribution for those respondents who are employed by business organizations (not including governments or professional service firms). As can be seen, the largest sectors

include financial services (including banking, insurance, credit cards, investment management), industrial (including manufacturing and conglomerates), and healthcare.

Pie Chart 5
Distribution of industries for respondents who are employed by business organizations

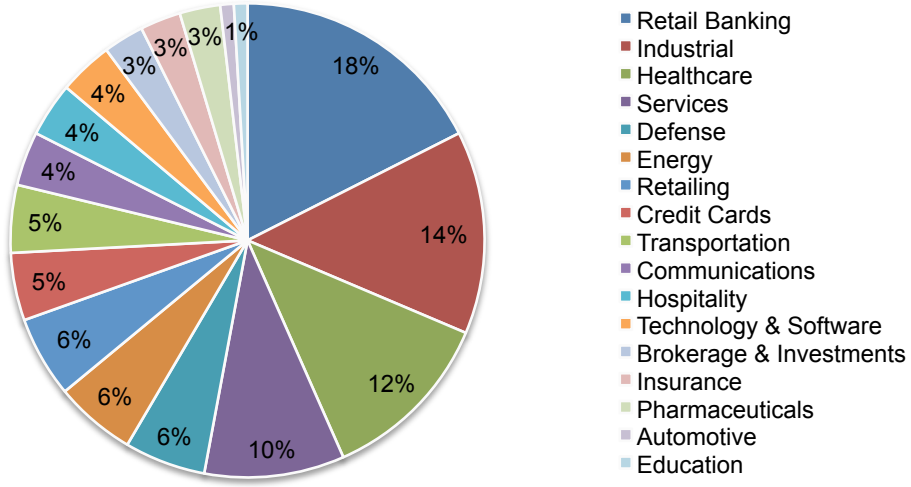


Table 4 reports the geographic footprint of respondents' organizations. In total, 88 percent of organizations have operations (headcount) in two or more countries. In addition, 56 percent have operations in more than one European nation. Finally, a total of 20 percent have operations in all major regions of the globe.

Table 4 **Geographic footprint of respondents' organizations**	Pct%
United States	100%
Canada	63%
Northern Europe	53%
Central Europe	46%
Southern Europe	29%
Middle East and Africa	21%
Asia-Pacific	44%
Latin America (including Mexico)	42%

Part 4. Implications & limitations

The purpose of this study was to find out what auditors think about crypto technologies. Based on the results of this survey research, the following are what we believe are the most important findings.

- Auditors believe that the main objective of their organization's data security strategy is compliance with regulations, policies and contractual obligations.
- Perhaps this linear focus on compliance is keeping organizations from allocating sufficient resources to achieving a higher security posture. In fact the majority of auditors surveyed agree that compliance does not necessarily lead to data security effectiveness.
- The majority of auditors say business units control the purse strings for compliance and data security audits. Perhaps if the IT or security function controlled the budget there might be more of a focus on achieving an effective security posture. Currently, 51 percent of auditors say that more than half of the their audits reveal significant deficiencies or fail data security compliance requirements.
- Auditors also point out a serious vulnerability in organizations. That is, where compliance requirements fail is where the most serious threats are located. These include applications, external service providers, mobile devices and others.
- Crypto technologies get high marks for their ability to protect an organization's information assets. In the domain of crypto, encryption is considered the best technology to use when securing confidential data in databases, storage, applications, and at the point of capture.
- Auditors are uncertain about whether databases, applications and storage devices that handle encrypted data are out-of-scope for purpose of compliance audits. This means that many organizations may not be taking advantage of the opportunity to reduce the overall cost of an audit within organizations that deploy crypto technologies throughout the enterprise.

We believe these findings are useful for organizations in developing their strategies for compliance and the protection of sensitive or confidential information assets. We also hope that information system auditors find these results useful in guiding them in future audits.

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of auditing professionals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that auditors who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are information system auditors. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

Appendix: Detailed Survey Responses

Following are the survey results for a final sample of 505 information systems auditing professionals. Fieldwork concluded in February 2011.

Response statistics	Freq.	Pct%
Total sample frame	9,956	100.0%
Invitations sent	9,810	98.5%
Total response	556	5.6%
Rejected surveys	36	0.4%
Final sample before screening	520	5.2%
Final sample	505	5.1%

Part 1. Screen		
Q1a. Are you presently an auditor of information security systems?	Freq.	Pct%
Yes	438	84%
No	82	16%
Total	520	100%

Q1b. If no, were you employed as an information security systems auditor, information security auditor, qualified security assessor or EDP auditor sometime during the past five years?	Freq.	Pct%
Yes	67	82%
No (STOP)	15	18%
Total	82	100%

Part 2. Background	
Q2. Please select all the certifications you presently hold.	Pct%
QSA	24%
CISSP	31%
CISA	46%
CISM	18%
CPA	20%
CMA	2%
CFE	4%
CA	3%
CIPP	1%
Total	151%

Q3. How many years of relevant work experience do you have auditing or assessing data security compliance and related controls or systems?	Pct%
Less than 2 years	3%
Between 2 and 5 years	19%
Between 6 and 10 years	34%
Between 11 and 15 years	30%
More than 15 years	14%
Total	100%

Q4. How many audits or assessments have you conducted or participated in within the past 12 months?	Pct%
None	9%
1 to 5	38%
6 to 10	41%
More than 10	12%
Total	100%

Q5. What standards do you use in determining data security compliance?	Pct%
Industry mandates such as PCI DSS	45%
Government laws such as HIPAA, GLBA, FISMA, FTC rules and others	51%
Organization's policies	65%
External policies or contracts (such as third party or business partner agreements)	34%
Other (please specify)	3%
Total	198%

Q6. How many of the above audits or assessments were supervised or led by you?	Pct%
Less than 25%	12%
25 to 50%	22%
51 to 75%	26%
More than 75%	40%
Total	100%

Q7a. What best describes the type of organization you work for?	Pct%
Audit and accounting firm	19%
Business corporation	41%
Government organization	11%
IT consulting firm	15%
IT security services firm	11%
Other (please specify)	3%
Total	100%

Q7b. If you work for a business corporation, please check its primary industry classification.	Pct%	n=205
Retail Banking	18%	
Industrial	14%	
Healthcare	12%	
Services	10%	
Defense	6%	
Energy	6%	
Retailing	6%	
Credit Cards	5%	
Transportation	5%	
Communications	4%	
Hospitality	4%	
Technology & Software	4%	
Brokerage & Investments	3%	
Insurance	3%	
Pharmaceuticals	3%	
Automotive	1%	
Education	1%	
Total	100%	

Q7c. If you work for a business corporation or government entity, how significant is your company's use of crypto security tools such as encryption, tokenization or PKI within your organization?	Pct%
Very significant	37%
Significant	38%
Insignificant	23%
We don't use	2%
Total	100%

Q8. What is the total headcount of your business or governmental organization?	Pct%
Less than 100 people	3%
101 to 1,000 people	11%
1,001 to 5,000 people	21%
5001 to 10,000 people	29%
10,001 to 25,000 people	16%
25,001 to 75,000 people	8%
More than 75,000 people	12%
Total	100%

Q9. In what geographies have you or your organization conducted audits or assessments? Please check all that apply.	Pct%
United States	100%
Canada	63%
Northern Europe	53%
Central Europe	46%
Southern Europe	29%
Middle East and Africa	21%
Asia-Pacific	44%
Latin America (including Mexico)	42%

Part 3. Attributions			
Q10. Please rate each one of the following five statements using the scale provided below each item.	Strongly agree	Agree	Combined
Q10a. The organization(s) I audit have sufficient resources to achieve data compliance requirements.	19%	26%	45%
Q10b. The organization(s) I audit make data security a strategic priority across the enterprise.	18%	24%	42%
Q10c. The organization(s) I audit are proactive in managing privacy and data protection risks.	13%	19%	32%
Q10d. The organization(s) I audit do believe compliance improves their data security effectiveness.	18%	22%	40%
Q10e. The organization(s) I audit use crypto security tools only as required to achieve compliance.	23%	31%	54%

Part 4. Audit experience	
Q11a. Typically, who is **most responsible** for ensuring compliance with privacy and data protection requirements within your organization or the clients you serve? Please select one best response.	Pct%
CIO	9%
CTO	4%
IT security leader (CISO)	9%
Privacy officer or leader (CPO)	4%
Quality assurance	2%
IT operations	14%
Compliance/audit	22%
Legal	12%
Business unit leaders	23%
Other (please specify)	1%
Total	100%

Q11b. Typically, who **owns the budget** for audits and assessments with your organization or the clients you serve? Please select one best response.	Pct%
CIO	5%
IT security leader (CISO)	2%
IT operations	15%
Compliance/audit	9%
Legal	15%
Business unit leaders	54%
Total	100%

Q12. On average, what percent of audits conducted by you have had serious deficiencies or failed data security compliance requirements?	Pct%
Less than 10 percent	11%
11 to 25 percent	15%
26 to 50 percent	23%
More than 50 percent	51%
Total	100%

Q13a. Where are the most serious threats to sensitive or confidential data located? Please select only the top three choices.	Pct%
Applications	38%
Databases	26%
Storage devices	11%
Messaging systems	21%
Network infrastructure	19%
Laptops or desktops	33%
Mainframes	5%
Web infrastructure	18%
Remote office systems	29%
Mobile devices	19%
External service providers	34%
External business partners	31%
Personal storage devices	3%
Backup media	4%
Paper documents	6%
Total	298%

Q13b. Where do data security compliance requirements most likely fail? Please select only the top three choices.	Pct%
Applications	38%
Databases	26%
Storage devices	11%
Messaging systems	24%
Network infrastructure	19%
Laptops or desktops	32%
Mainframes	4%
Web infrastructure	19%
Remote office systems	29%
Mobile devices	19%
External service providers	33%
External business partners	31%
Personal storage devices	3%
Backup media	4%
Paper documents	6%
Other (please specify)	0%
Total	299%

Q13c. [complete If you selected "External service providers in either 13a or 13b] What types of external service providers are of greatest threats or risk to your organization. Please select only the top two choices.	Pct%	n=171
Cloud computing, software as a service	65%	
Cloud computing, infrastructure services	21%	
Cloud computing, platform services	32%	
Outsourcing services	48%	
Co-sourcing services	12%	
Other (please specify)	3%	
Total	181%	

Q14. In your opinion, what are the main reasons for conducting data compliance audits or assessments? Check only the two top choices.	Pct%
Identify risks and vulnerabilities	48%
Comply with internal policies and mandates	42%
Comply with external regulatory and legal mandates	34%
Improve the organization's data security posture	19%
Improve the organization's reputation	2%
Improve the organization's relationship with business partners	29%
Heighten awareness among C-levels within the organization	11%
Help secure more funding for the organization's IT security	6%
None of the above	0%
Total	191%

Part 6. Data compliance requirements			
Following are 12 well-known data compliance requirements as defined by standards such as ISO, NIST, PCI DSS and others. For each requirement, please rate relative difficulty companies have in achieving compliance; the importance of the requirement in achieving the company's overall security objectives; degree to which a requirement is absolute or can be met with other controls	Difficulty	Importance	Compensating controls
Q15a. Install and maintain a firewall configuration to protect confidential data	39%	68%	33%
Q15b. Do not use vendor-supplied defaults for system passwords and other security parameters	19%	34%	21%
Q15c. Protect stored confidential data	44%	48%	76%
Q15d. Encrypt transmission of confidential data across open, public networks	25%	69%	60%
Q15e. Use and regularly update anti-virus software	31%	59%	47%
Q15f. Develop and maintain secure systems and applications	54%	59%	58%
Q15g. Restrict access to confidential data by need-to-know only	57%	71%	57%
Q15h. Assign a unique ID to each person with computer access	15%	28%	76%
Q15i. Restrict physical access to confidential data	32%	33%	21%
Q15j. Track and monitor all access to network resources and confidential data	43%	57%	45%
Q15k. Regularly test security systems and processes	40%	59%	78%
Q15l. Maintain a policy that addresses data security	23%	38%	46%

Part 7. Data Protection & Crypto Solutions			
Q16. Following are crypto technologies that foster compliance with an organization's privacy and data protection requirements. For each item, indicate the **effectiveness** of each technology with respect to achieving data compliance goals by using one of three choices: high, moderate or low effectiveness, respectively.			
Crypto technologies used to achieve compliance	High	Moderate	Low
Database encryption	63%	21%	16%
Storage encryption	56%	28%	16%
Encryption over public networks	71%	19%	10%
Encryption over private or internal networks	53%	25%	22%
Encryption of desktop and mobile devices	76%	15%	9%
Strong authentication and tokens	54%	20%	26%
Public key infrastructure (PKI)	46%	23%	31%
Virtual privacy network (VPN)	38%	29%	33%
Average	57%	23%	20%

Q17. To secure confidential data in a database, what technology do you recommend most often to your organization or the clients you serve? Please select one.	Pct%
Encryption	54%
Masking	12%
Tokenization	15%
Truncation	10%
Other (please specify)	3%
None	6%
Total	100%

Q18. To secure confidential data in applications outside of a database, what technology do you recommend most often to your organization or the clients you serve? Please select one.	Pct%
Encryption	36%
Masking	13%
Tokenization	11%
Truncation	28%
Other (please specify)	5%
None	7%
Total	100%

Q19. To secure confidential data in storage, what technology do you recommend most often to your organization or the clients you serve? Please select one.	Pct%
Encryption	55%
Masking	8%
Tokenization	17%
Truncation	11%
Other (please specify)	3%
None	6%
Total	100%

Q20. What do you believe is the most effective technology for your organization or clients to protect data at the point of capture such as point-of-sale (POS), website, email gateway and call center? Please select one.	Pct%
Encryption	43%
Masking	9%
Tokenization	37%
Other (please specify)	4%
None	3%
Total	4%
	100%

Q21. What is the most challenging aspect of encryption key management for achieving compliance with privacy and data protection requirements? Please select one.	Pct%
Key rollover	10%
Protecting stored keys	20%
Controlling use of keys	19%
Administration of key management system	28%
Logging operations	7%
Key distribution/sharing	9%
Key/certification generation	6%
Other (please specify)	0%
None	0%
Total	100%

Q22. Does the use of hardware security modules for encryption and key management reduce the time spent on demonstrating compliance with privacy and data protection requirements?	Pct%
Yes	68%
No	32%
Total	100%

Q23. What do you most frequently recommend to your organization or clients for encryption and key management?	Pct%
I recommend a hardware security module be used instead of software.	46%
I recommend a hardware security module, but allow software-based encryption and key management.	33%
I recommend only software-based encryption and key management.	21%
Total	100%

Q24a. Do you consider the database that handles encrypted data (properly managed and controlled to your requirements in Q19) to be out-of-scope with audit requirements?	Pct%
Yes	44%
No	56%
Total	100%

Q24b. Do you consider the applications that process encrypted data (properly managed and controlled to your requirements in Q20) to be out-of-scope with audit requirements?	Pct%
Yes	49%
No	51%
Total	100%

Q24c. Do you consider the storage devices that handle encrypted data (properly managed and controlled to your requirements in Q21) to be out-of-scope with audit requirements?	Pct%
Yes	43%
No	57%
Total	100%

Q24d. How does an organization's use of crypto solutions such as encryption or PKI to protect information assets, favorably influence your perception about its security posture?	Pct%
Significant influence	34%
Some influence	38%
Little influence	11%
No influence	9%
Unsure	8%
Total	100%

Q25a. Do you believe an organization's information assets can be fully protected **within the corporate boundary** (i.e., in-house applications, devices, storage and private networks) without the use of crypto solutions?	Pct%
Yes	19%
No	71%
Unsure	10%
Total	100%

Q25b. If yes, what are these alternative security technologies and controls? Please check only the top two choices.	Pct%
Manual control procedures such as segregation of duties	31%
Access controls including identity and access management	20%
Perimeter controls including firewalls, IDS, and others	17%
Endpoint security systems including AV	19%
Network intelligence tools	13%
Other (please specify)	0%
Total	100%

Q26. Do you believe that encryption has a role in protecting sensitive or confidential data at some point in its lifecycle?	Pct%
Yes	82%
No	18%
Total	100%

Q27. Do you believe that sensitive or confidential information should be encrypted whenever practical is a best practice?	Pct%
Yes	81%
No	19%
Total	100%

Q28. In your opinion, where is the encryption of information most needed?	Pct%
As soon as it is captured or enters business systems	9%
Whenever it is stored	9%
Whenever it passes over a network	38%
As soon as it is practical	20%
Whenever it is shared with an external party	23%
Total	100%

Q29. In your opinion, what types of information are most likely to require encryption?	Pct%
Customer information	54%
Employee information	51%
Payment transactions (including credit cards)	70%
Health information	76%
Business confidential information	77%
Financial or accounting information	64%
Intellectual properties	48%
Other (please specify)	3%
Total	443%

Q30. Should end-user convenience be considered when deciding if confidential or sensitive information needs to be encrypted (or other crypto solution)?	Pct%
Yes	34%
No	53%
Unsure	13%
Total	100%

Part 7. Regulations			
Q33a. Please check all the privacy and data security regulations that (to the best of your knowledge) your organization (or your clients) is required to comply with today.			
Q33b. For each privacy and data security regulation checked above (in Q33a), please rate the level of difficulty that compliance creates for your organization using the following four-point scale:	Q33a	Q33b	Q33c
Q33c. For each privacy and data security regulation checked above (in Q33a), please rate the significance that crypto security solutions play in meeting the selected compliance requirements.	Required to comply	Difficulty	Significance of crypto
State privacy and data security laws	94%	61%	55%
Health Insurance Portability & Accountability Act (HIPAA)	15%	54%	69%
HIPAA provisions of the HITECH Act.	36%	49%	61%
Children's Online Privacy Protection Act (COPPA)	12%	16%	10%
Gramm-Leach-Bliley Act	20%	18%	8%
Fair & Accurate Credit Transactions Act (FACTA)	17%	26%	23%
The Red Flags Rule	19%	19%	38%
Fair Credit Reporting Act (FCRA)	23%	39%	46%
Federal Privacy Act	18%	15%	15%
Various national privacy laws (different countries around the world)	65%	69%	35%
EU Privacy Directive (including Safe Harbor compliance)	48%	33%	28%
PCI DSS compliance	59%	62%	69%
Sarbanes-Oxley compliance	58%	56%	32%
CANSPAM Act	60%	23%	9%
FTC's Do Not Call Registry	61%	19%	6%
FCC requirements	9%	29%	13%
Other (please specify)	8%	37%	5%
Total	622%	625%	521%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.