The State of Supply Chain Risk in Healthcare

February 28, 2023

Sponsored by Healthcare Sector Coordinating Council

Ponemon
INSTITUTE

About Ponemon Institute

- Founded in 2002, 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.

The State of Supply Chain Risk in Healthcare

Ponemon Institute in collaboration with the Healthcare Sector Coordinating Council conducted a study on the cybersecurity challenges facing the healthcare sector. More than 400 IT and IT security practitioners were surveyed who are involved in their organizations' supply chain risk management program (SCRM) and familiar with their cybersecurity plans or programs.

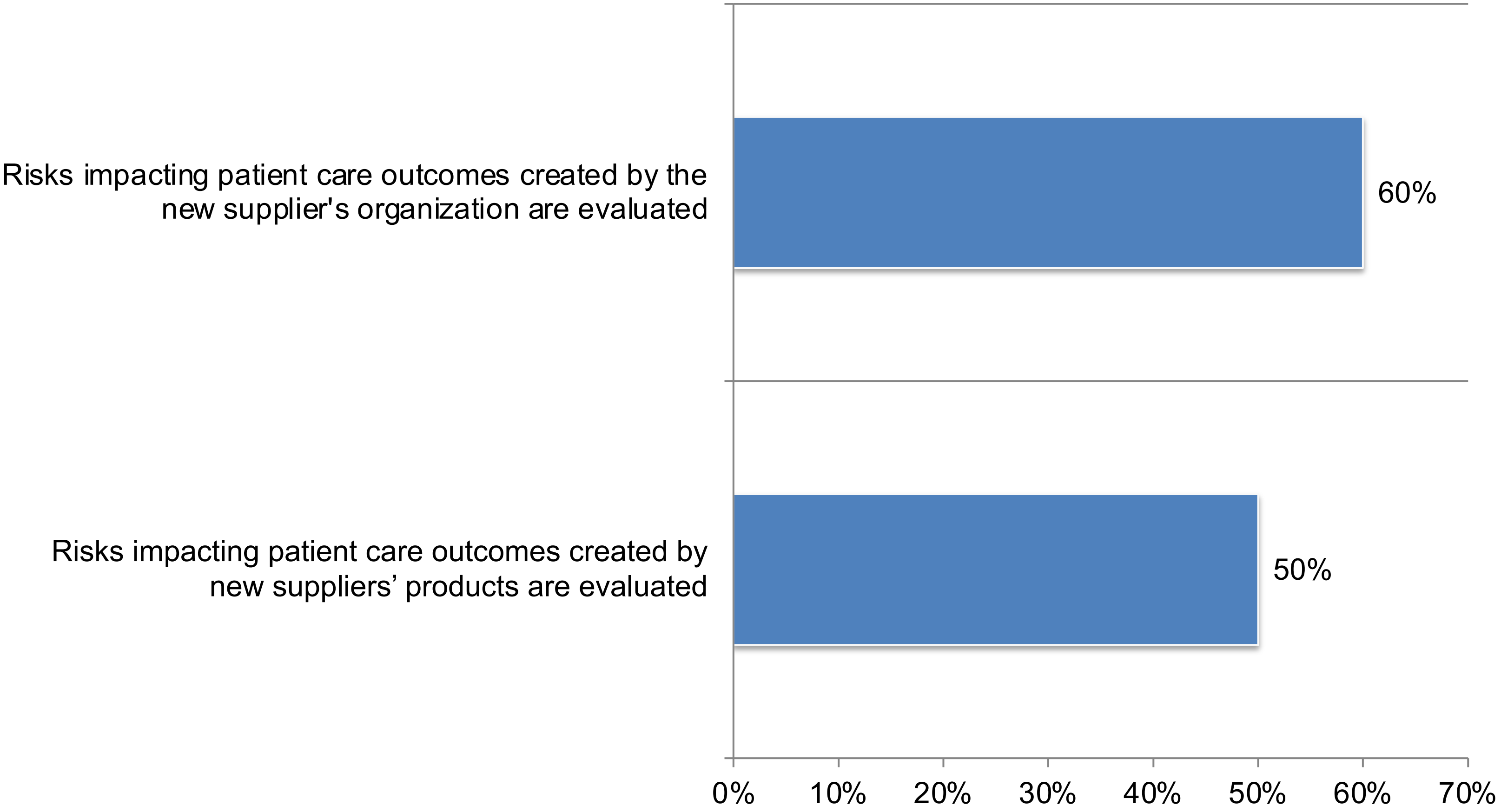
The Healthcare and Public Sector Coordinating Council (HSCC) is a coalition of private-sector, critical healthcare infrastructure entities organized under Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public.

Sample distribution

Sample response	Freq	Pct%
Sampling frame	11,064	100.0%
Total returns	463	4.2%
Rejected or screened surveys	61	0.6%
Final sample	402	3.6%

A key takeaway is that risks to patients caused by new suppliers are not being evaluated by many healthcare organizations.

Does your organization evaluate the risks impacting patient care outcomes created by new suppliers?



The following findings reveal why the supply chain is vulnerable to a cyberattack.

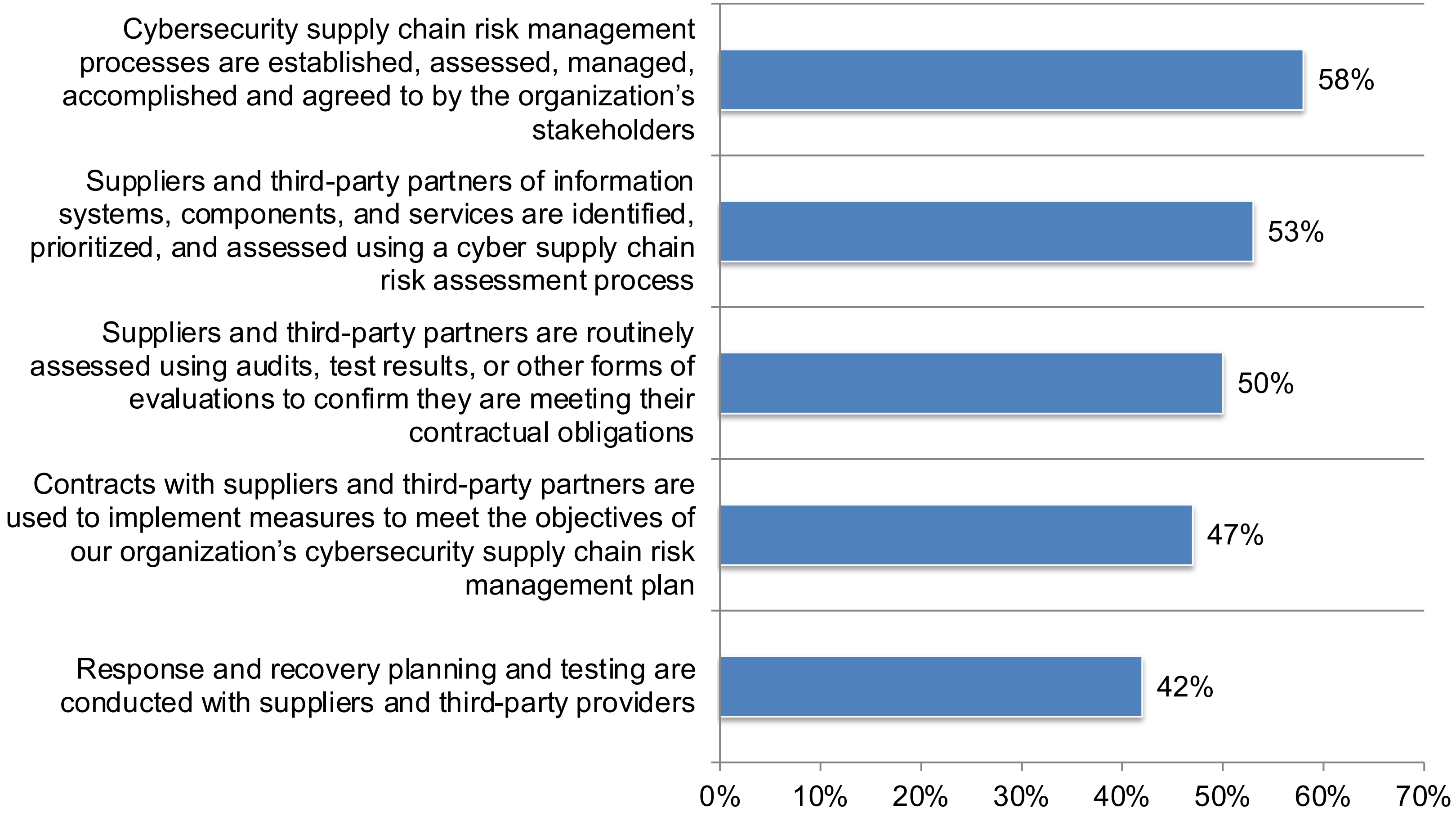
- Most organizations are in the dark about potential risks created by suppliers.
- Business-critical suppliers are not regularly evaluated for their security practices.
- Most organizations are not assessing suppliers' software and technology.
- Pre-existing suppliers and not new suppliers are more likely to be included in the scope of an organization's SCRM.
- Rarely are suppliers categorized based on their connectivity or network access to the healthcare organization.
- There is a lack of integration between procurement and/or contracting departments and the SCRM process that could affect the ability of contracts to ensure the security of the supply chain.
- The lack of standardized language in security contracts and supply chain issues is a deterrent to an effective SCRM program.
- Healthcare organizations face the challenge of having the in-house expertise and senior leadership support needed to have a successful SCRM program.
- A lack of cooperation from suppliers and employees is the primary people-related impediment to a successful SCRM program.
- Controlling the sprawl of software usage is the number one technology-related impediment to achieving an effective SCRM program.

To address the supply chain risks discussed above, healthcare organizations are making the following activities a priority.

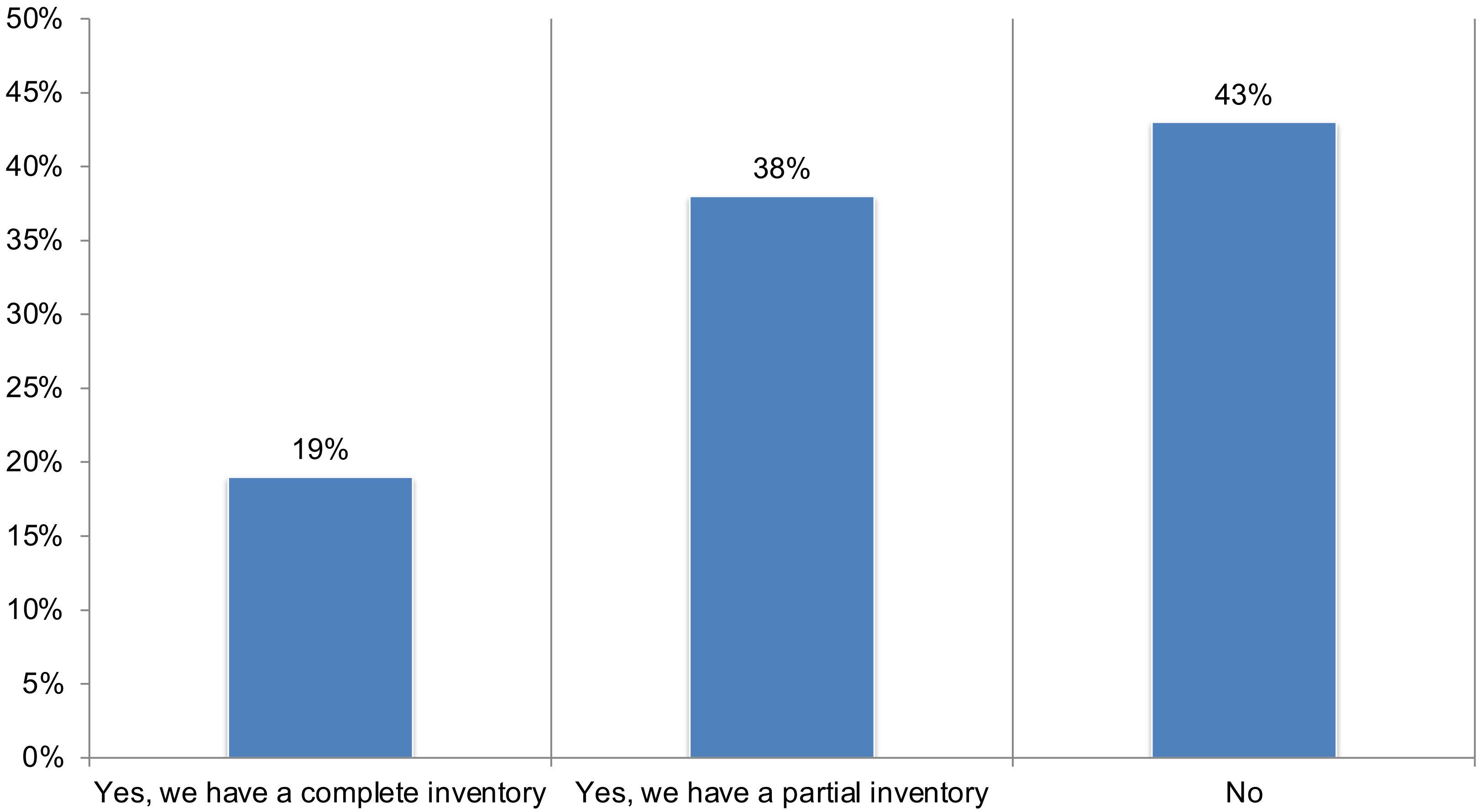
- Improvement of supply chain management is a priority.
- Business goals for SCRM are the cost, product quality and the supply chain.
- Organizations are focused on tracking direct suppliers and products/services electronically (43 percent of respondents).

The management of supplier risk

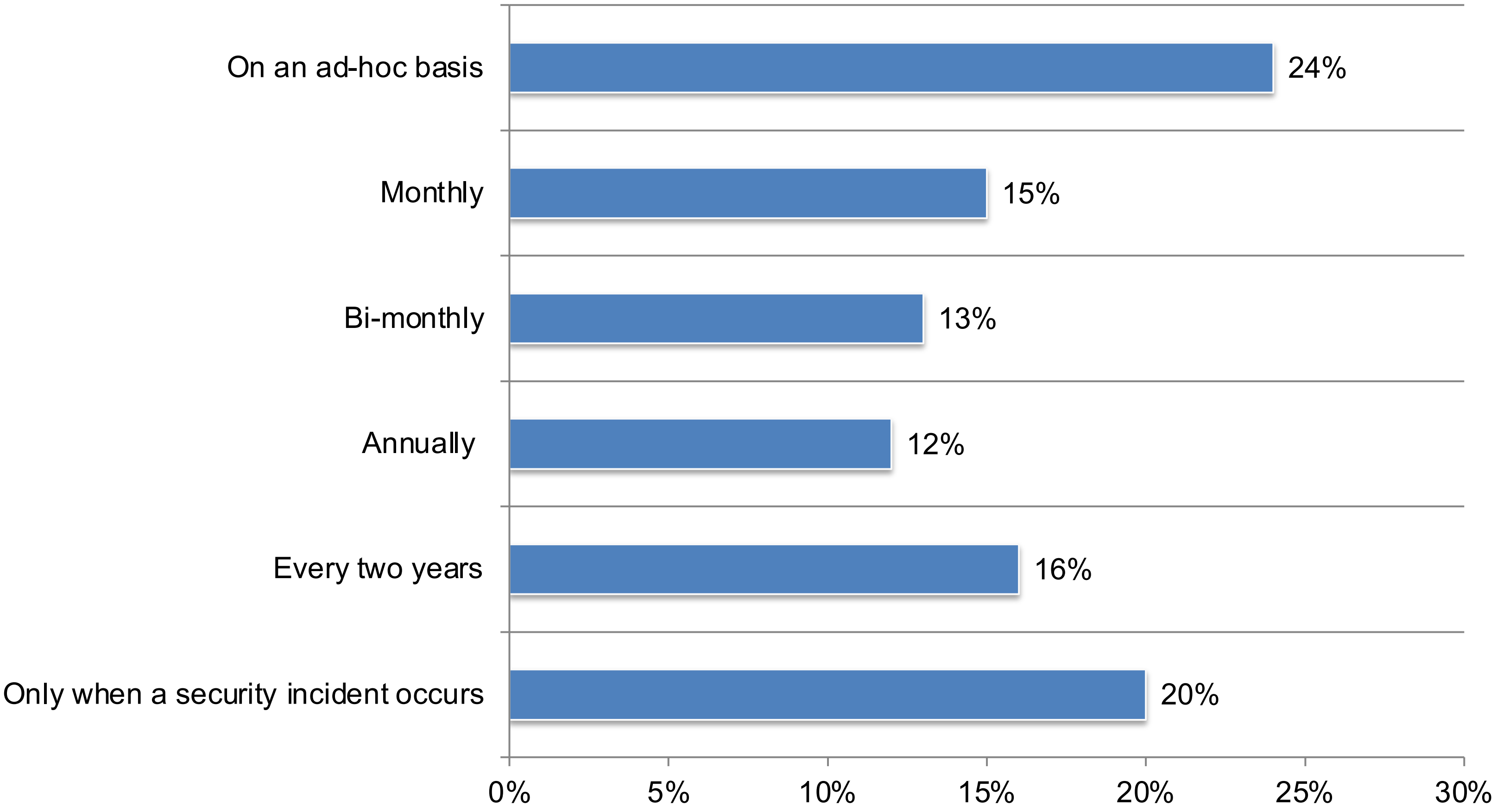
Perceptions about the management of healthcare supplier risk



Does your organization maintain an updated, digital & centralized inventory of suppliers of physical goods, business-critical services and/or third-party information technology?

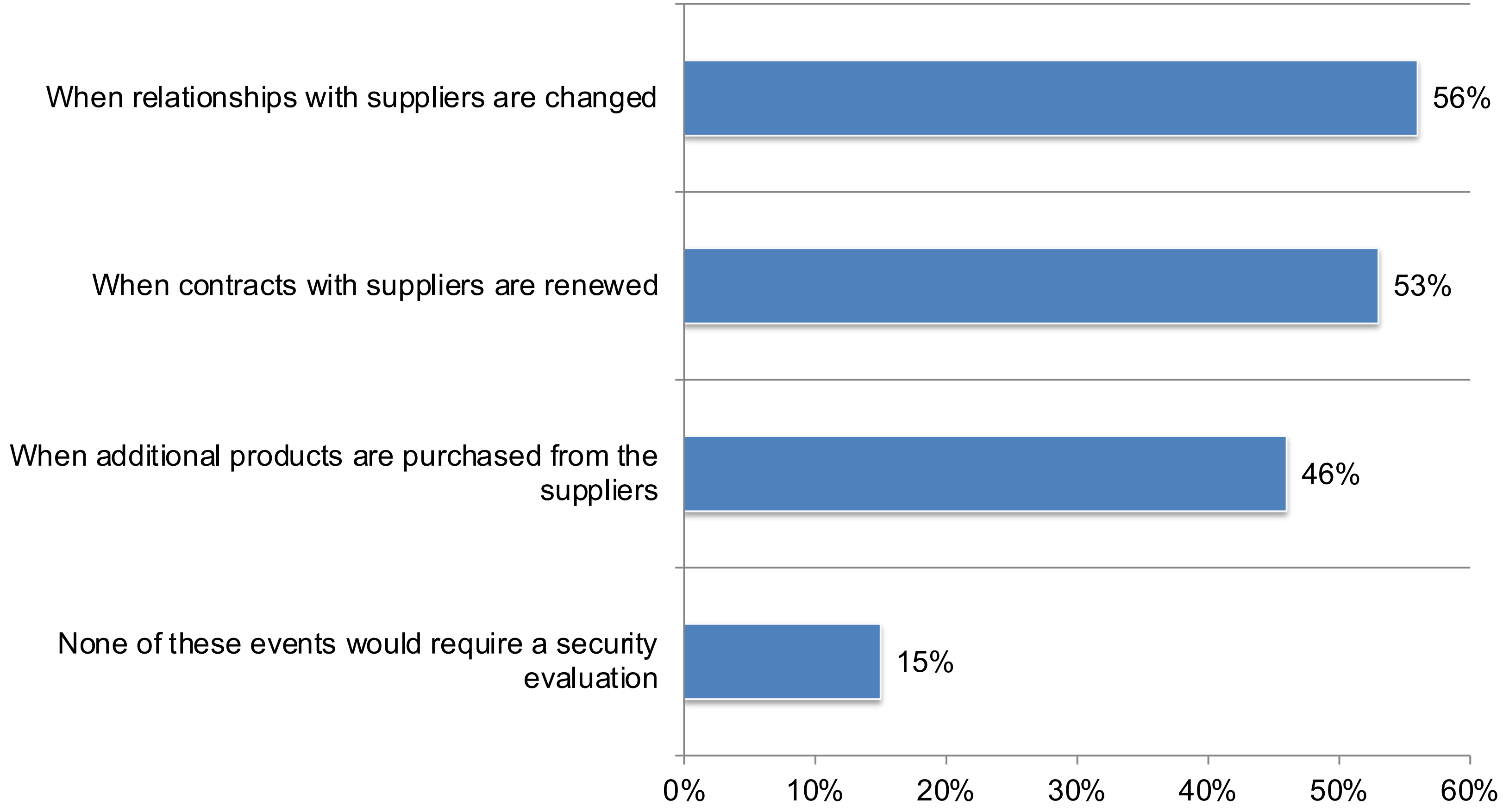


How often does your organization require a security evaluation of its business-critical suppliers?



What events trigger a security evaluation of business-critical suppliers?

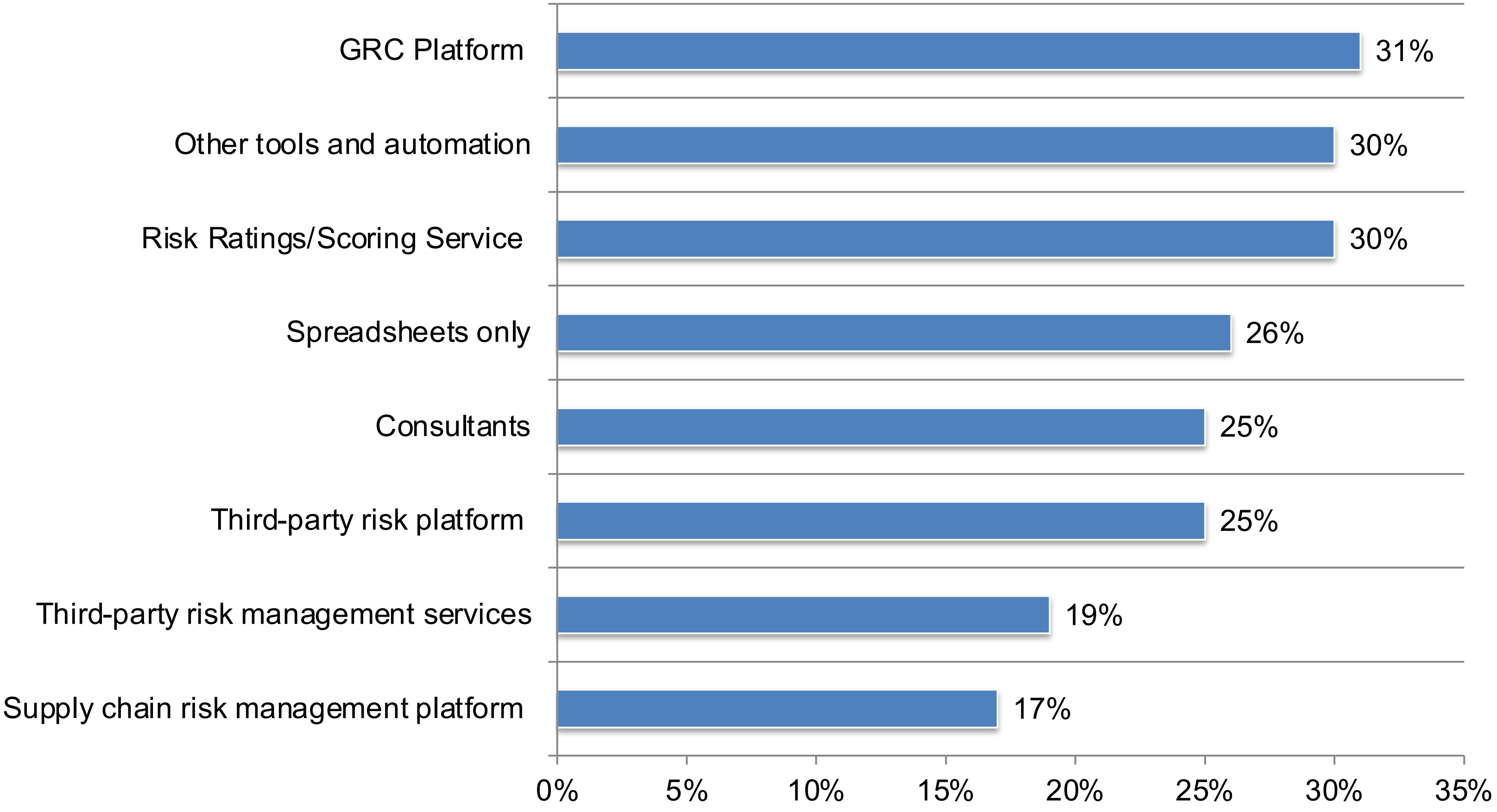
More than one response permitted



Ponemon INSTITUTE

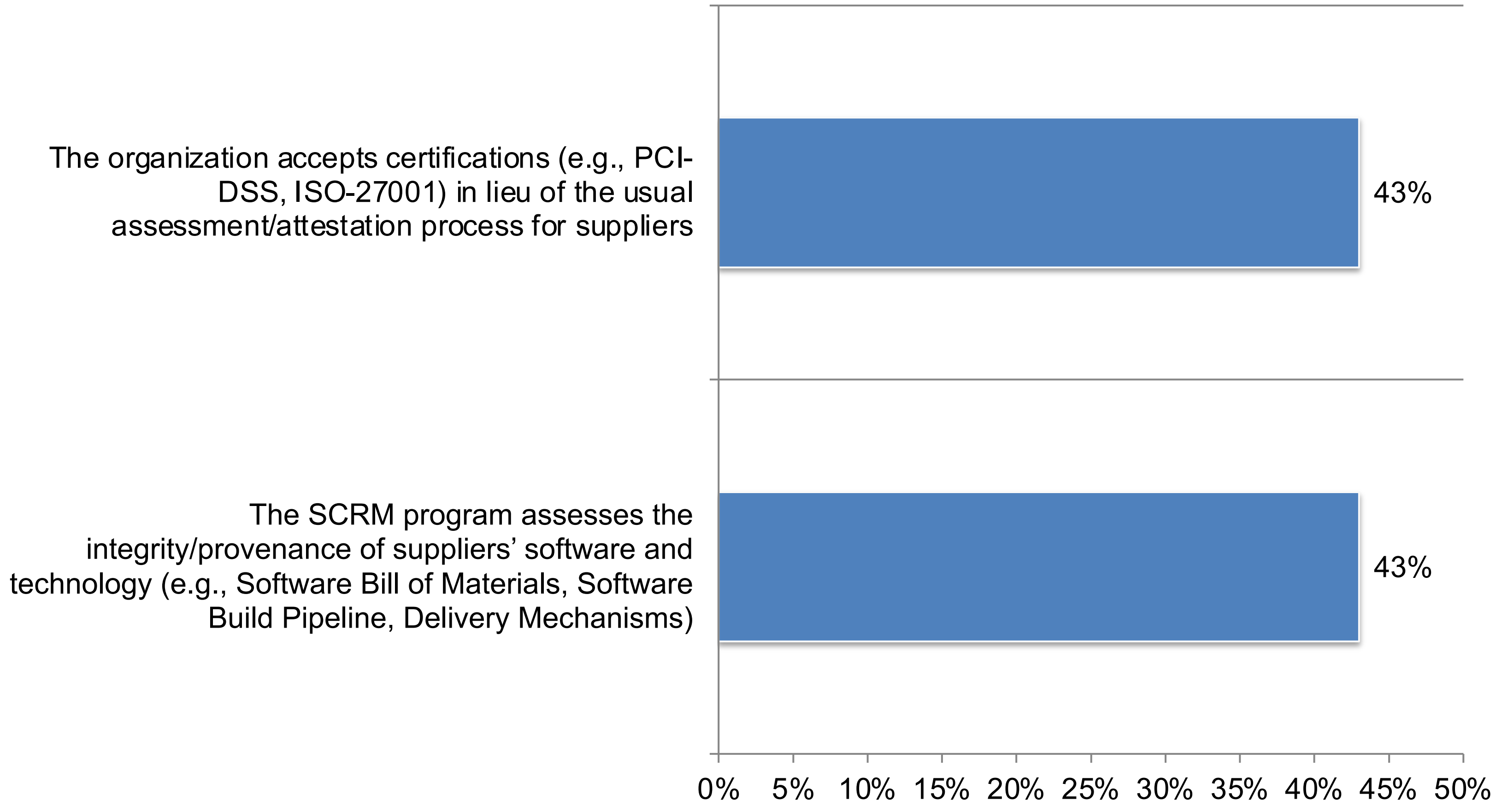
What tools, technologies and services are used as part of your organization's supplier evaluation?

More than one response permitted



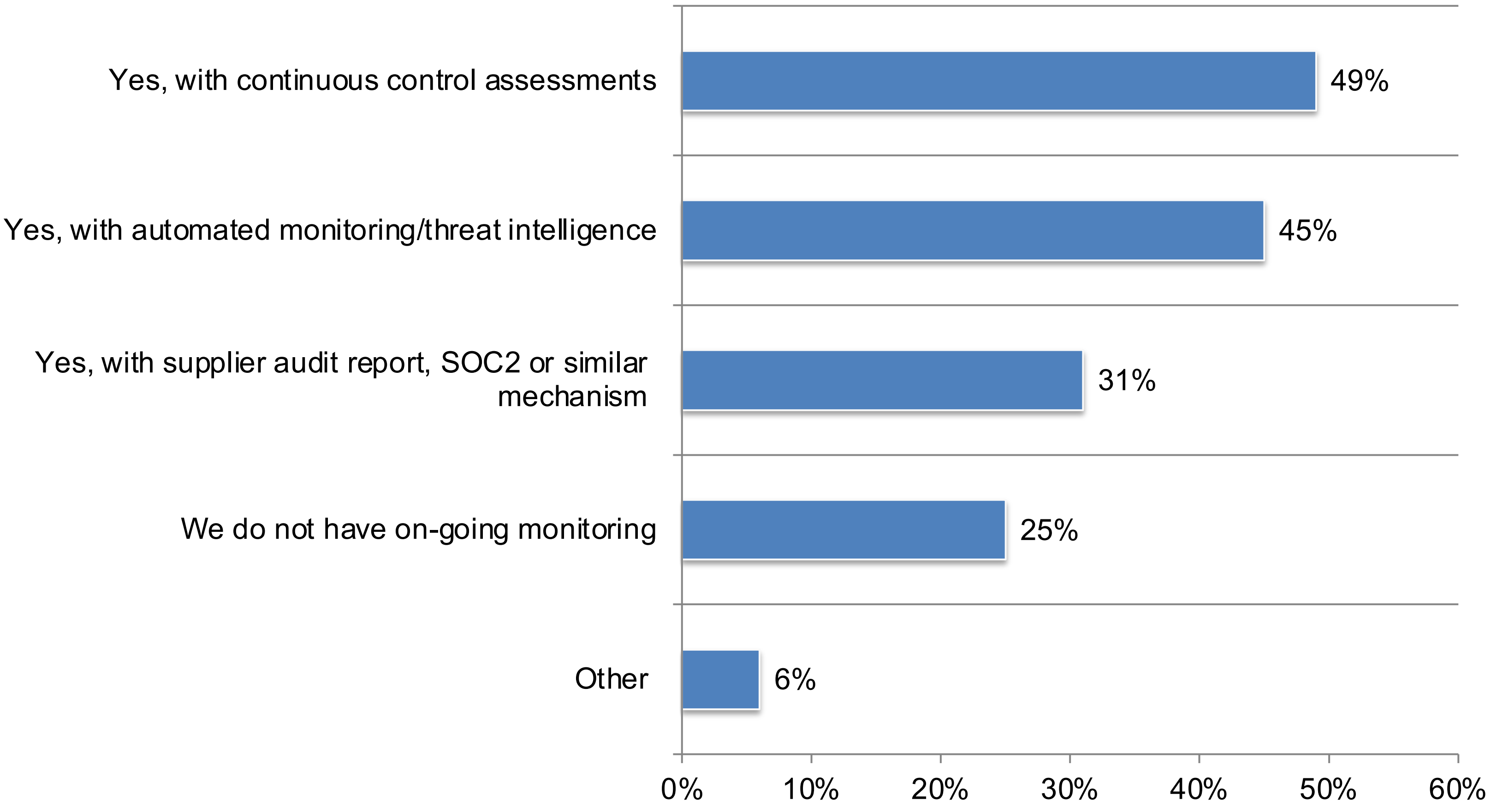
Does the SCRM assess the suppliers' software and technology and/or accept certifications in lieu of the usual supplier assessment process?

Yes responses presented



Does your organization have on-going monitoring as part of your SCRM process?

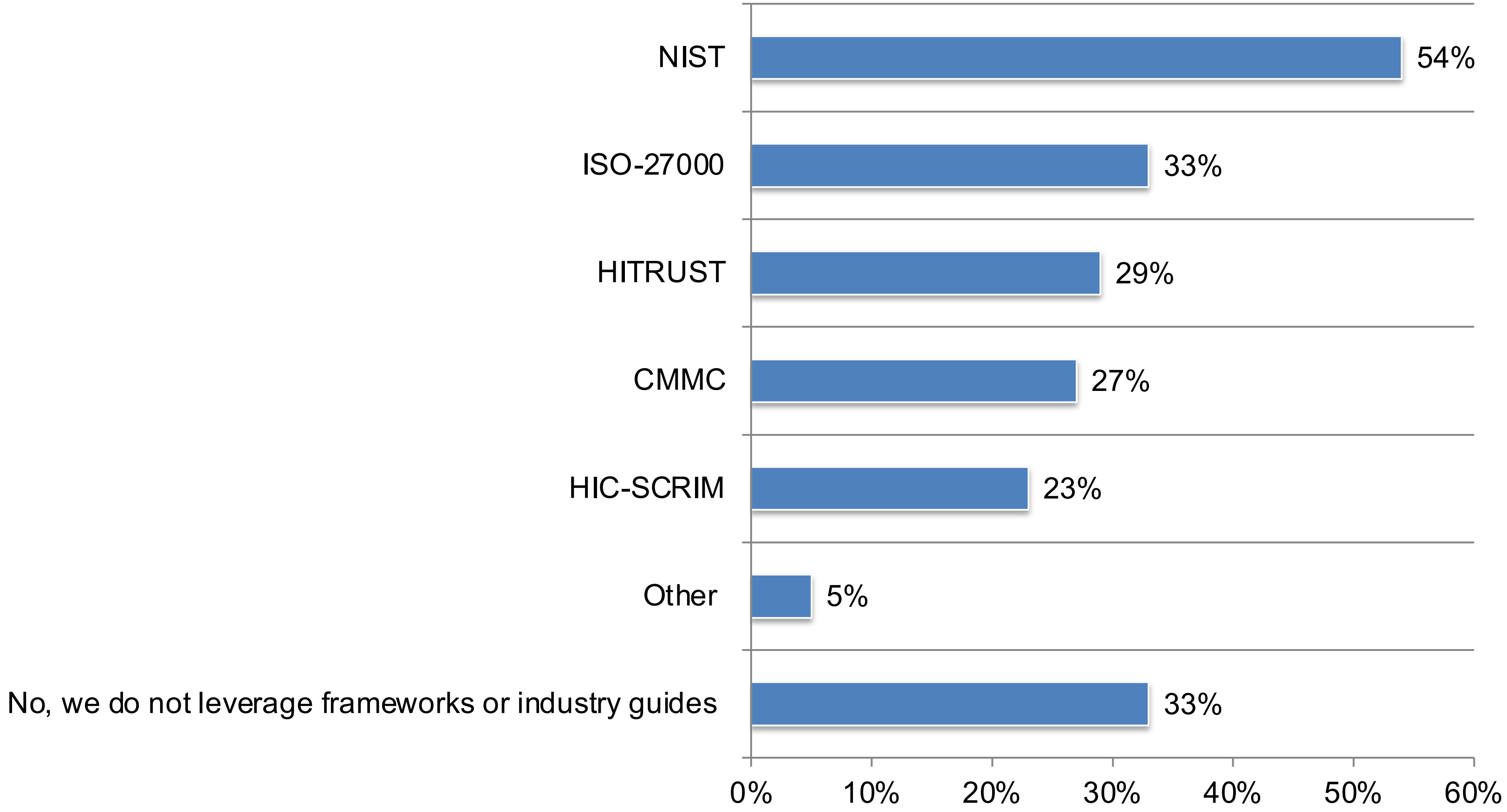
More than one response permitted



Supplier risk governance practices

Which frameworks or industry guides does your organization leverage in its SCRM?

More than one response permitted

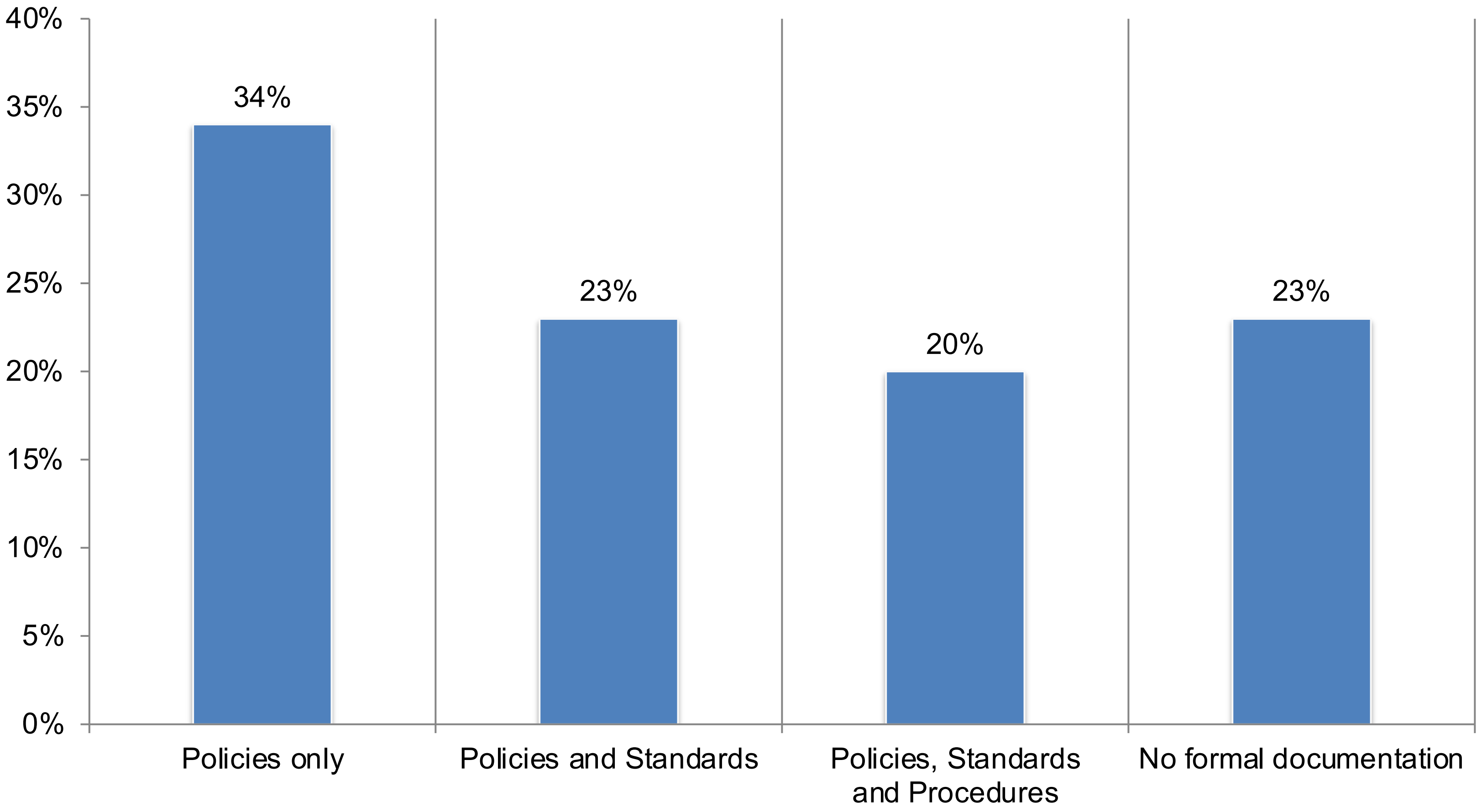


Ponemon INSTITUTE

www.ponemon.org

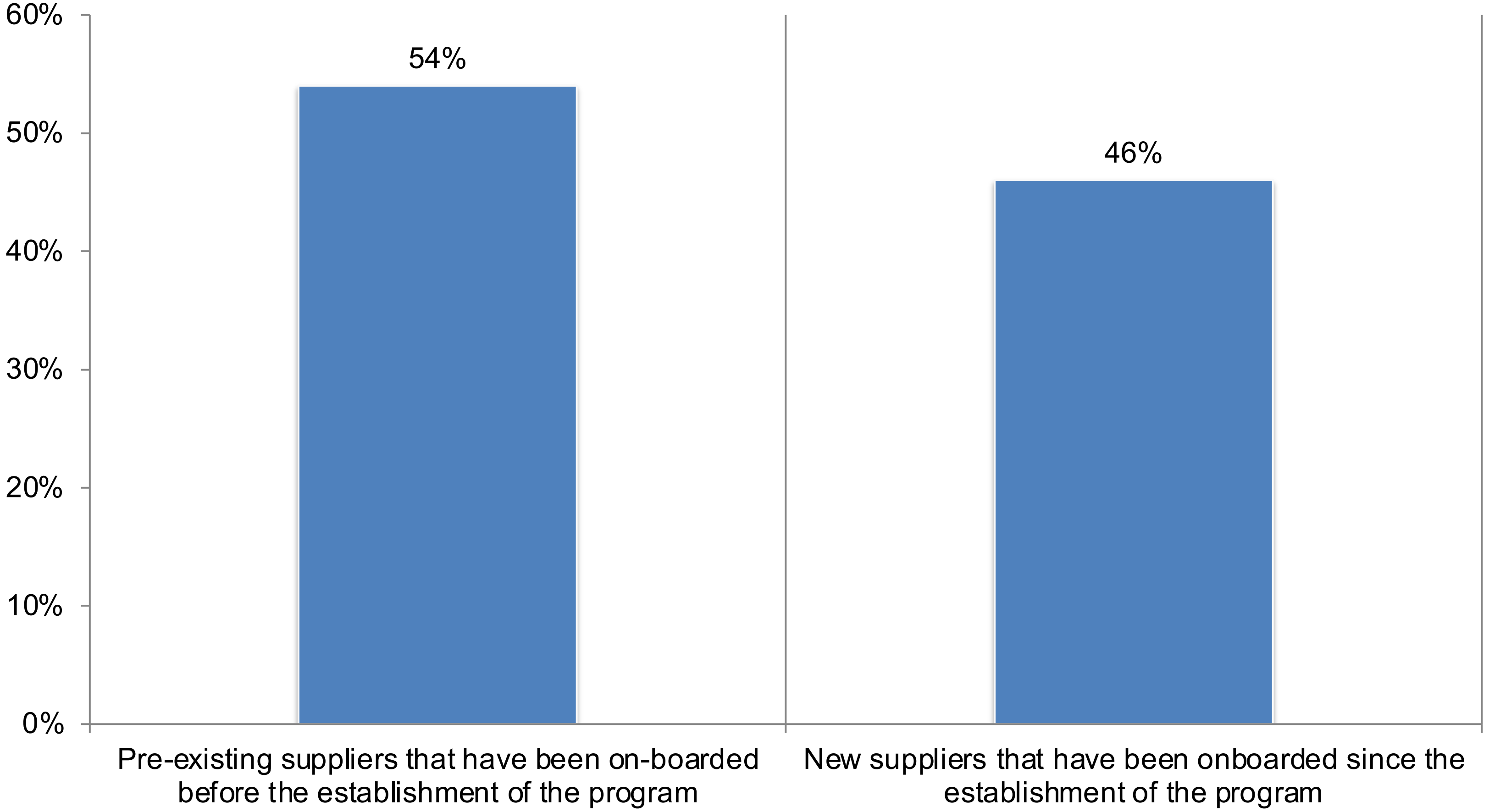
What level of formal document does the SCRM program have?

Only one choice permitted



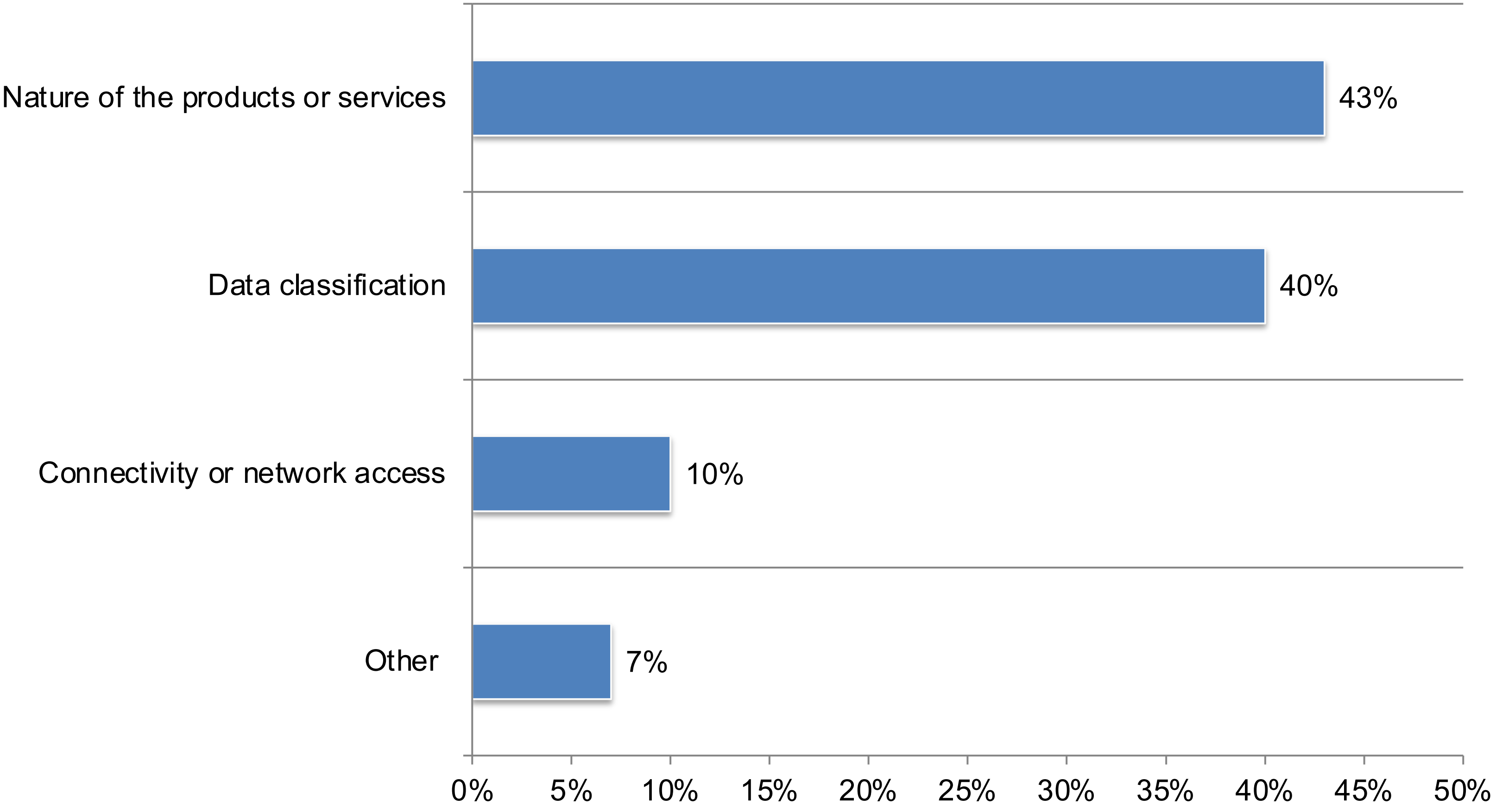
Which of the following is included in the scope of your organization's SCRM program?

Only one response permitted

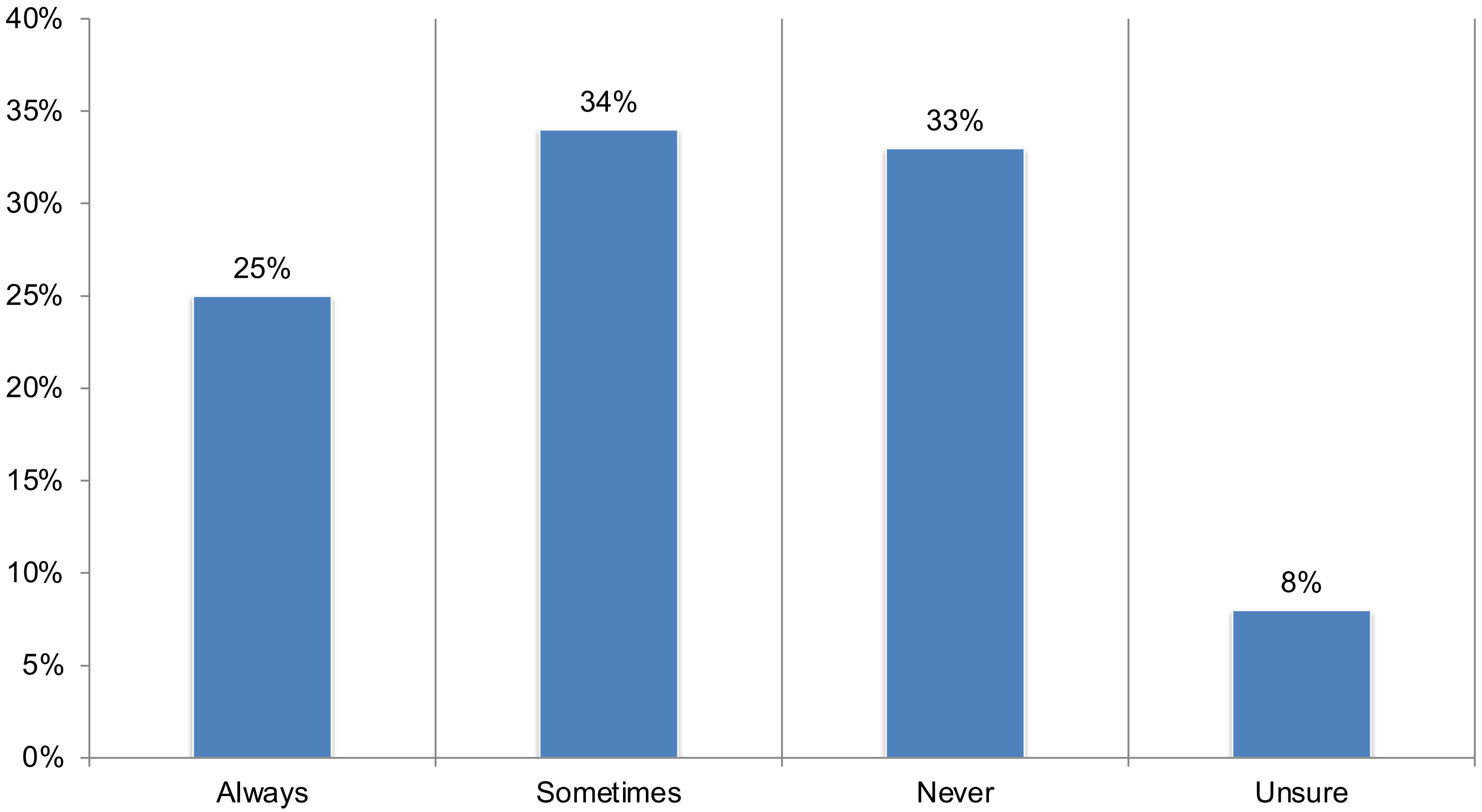


How does your organization categorize suppliers?

Only one choice permitted



Do you add supplier remediations into your contracts if needed?



Ponemon INSTITUTE

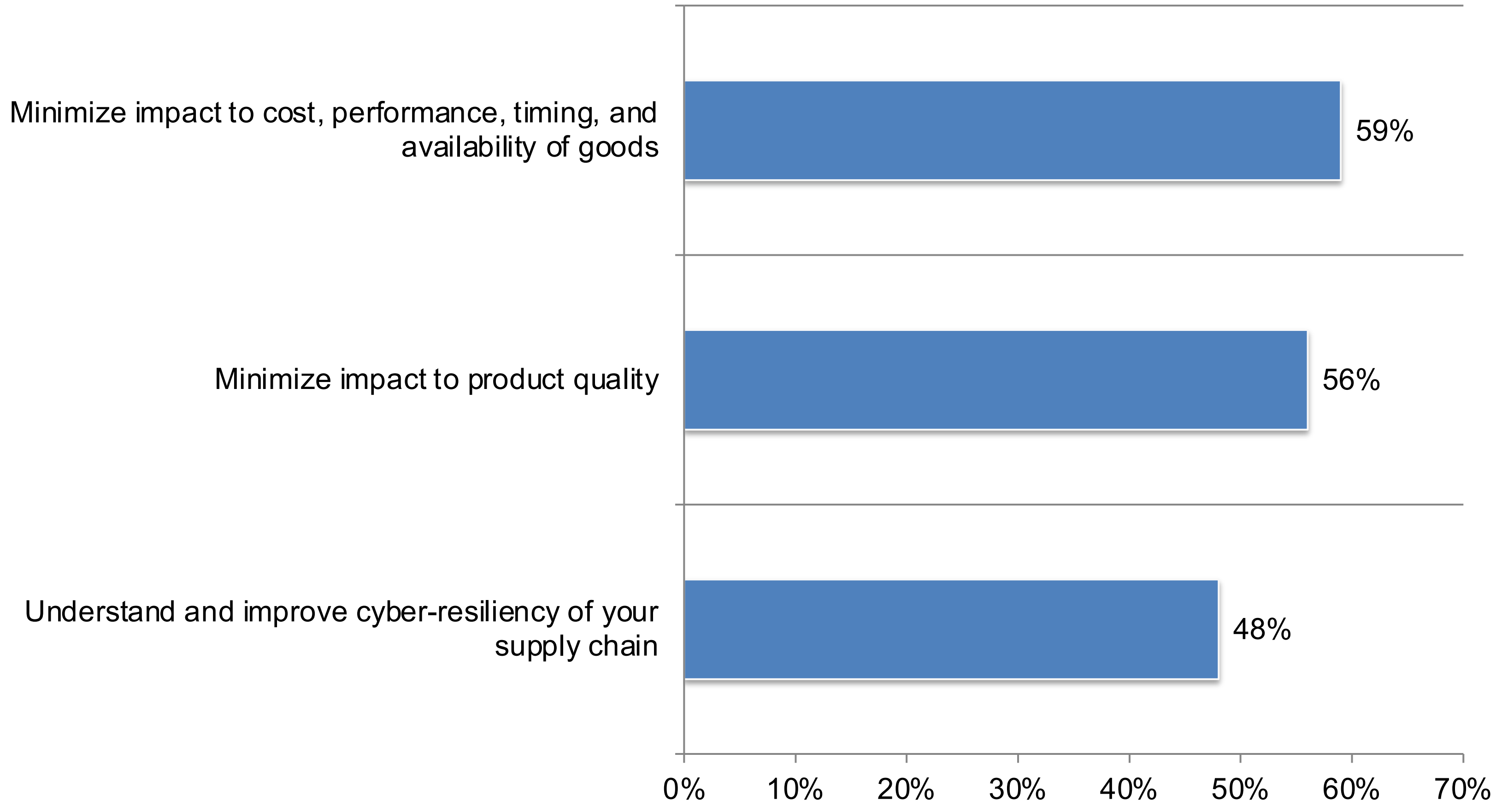
www.ponemon.org

The current and future state of SCRM healthcare programs

Ponemon INSTITUTE

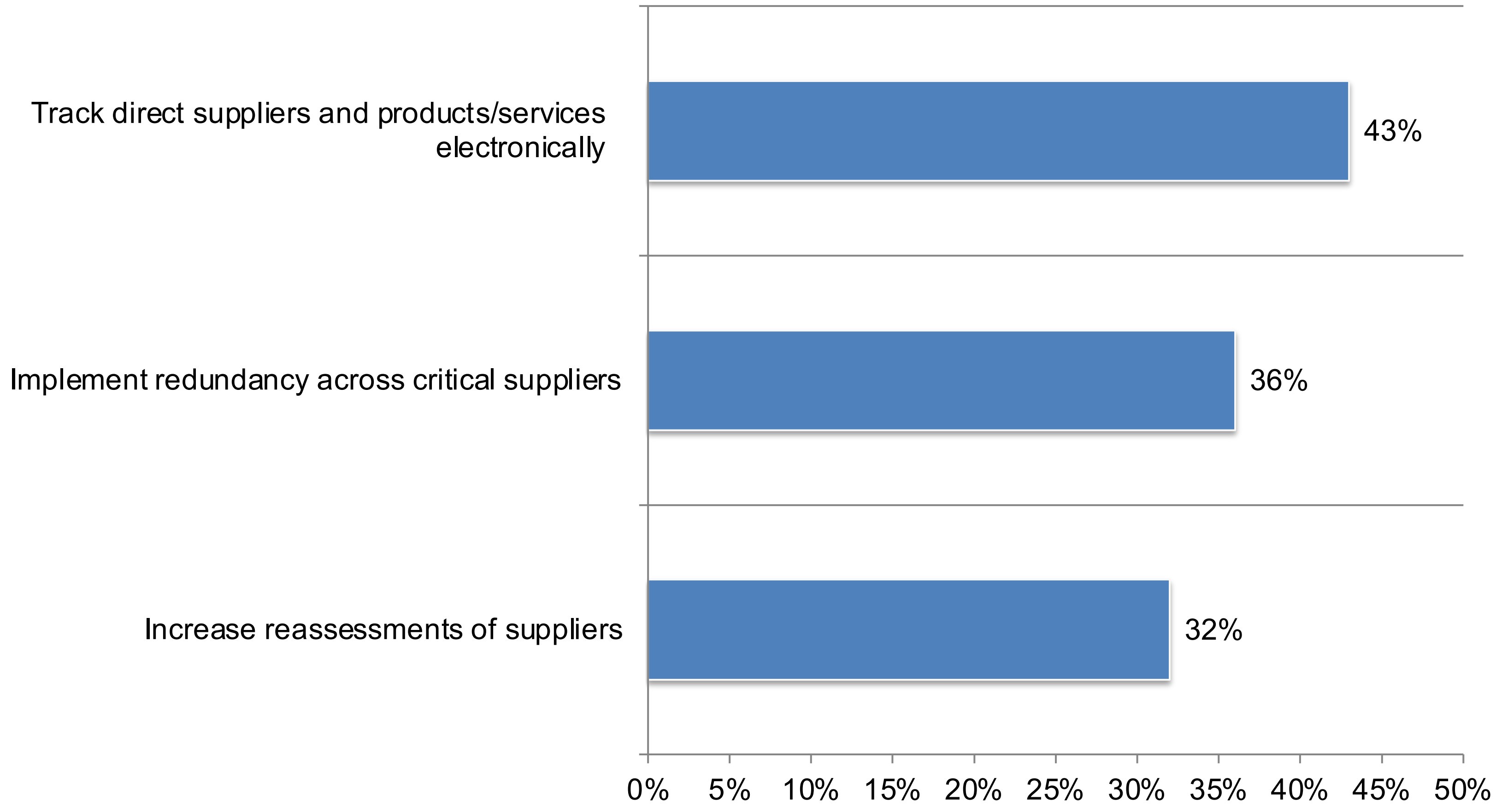
What are your organization's top three business goals for SCRM?

Top three responses presented



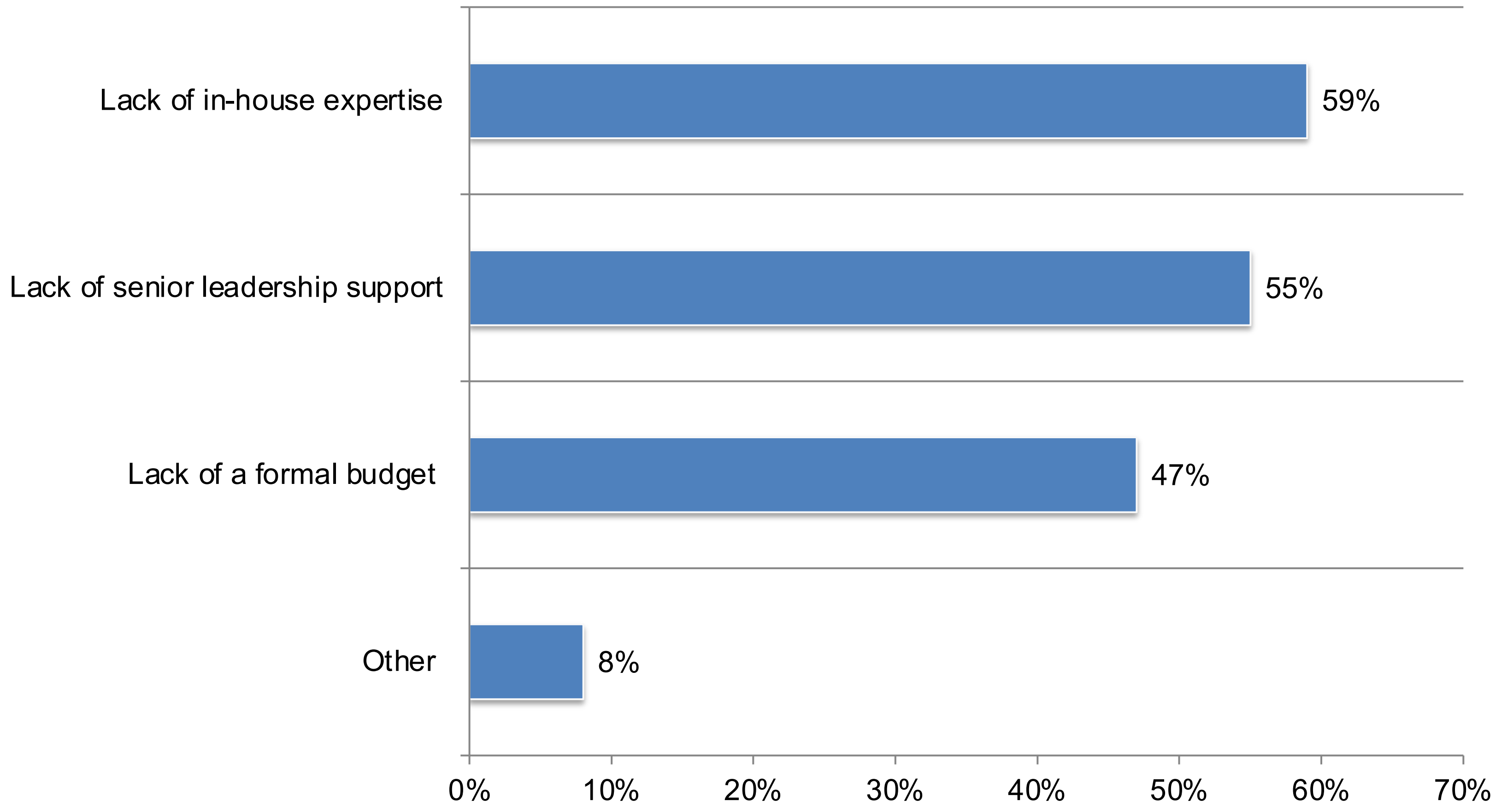
What are the top three priorities of your organization's SCRM program?

Top three responses presented



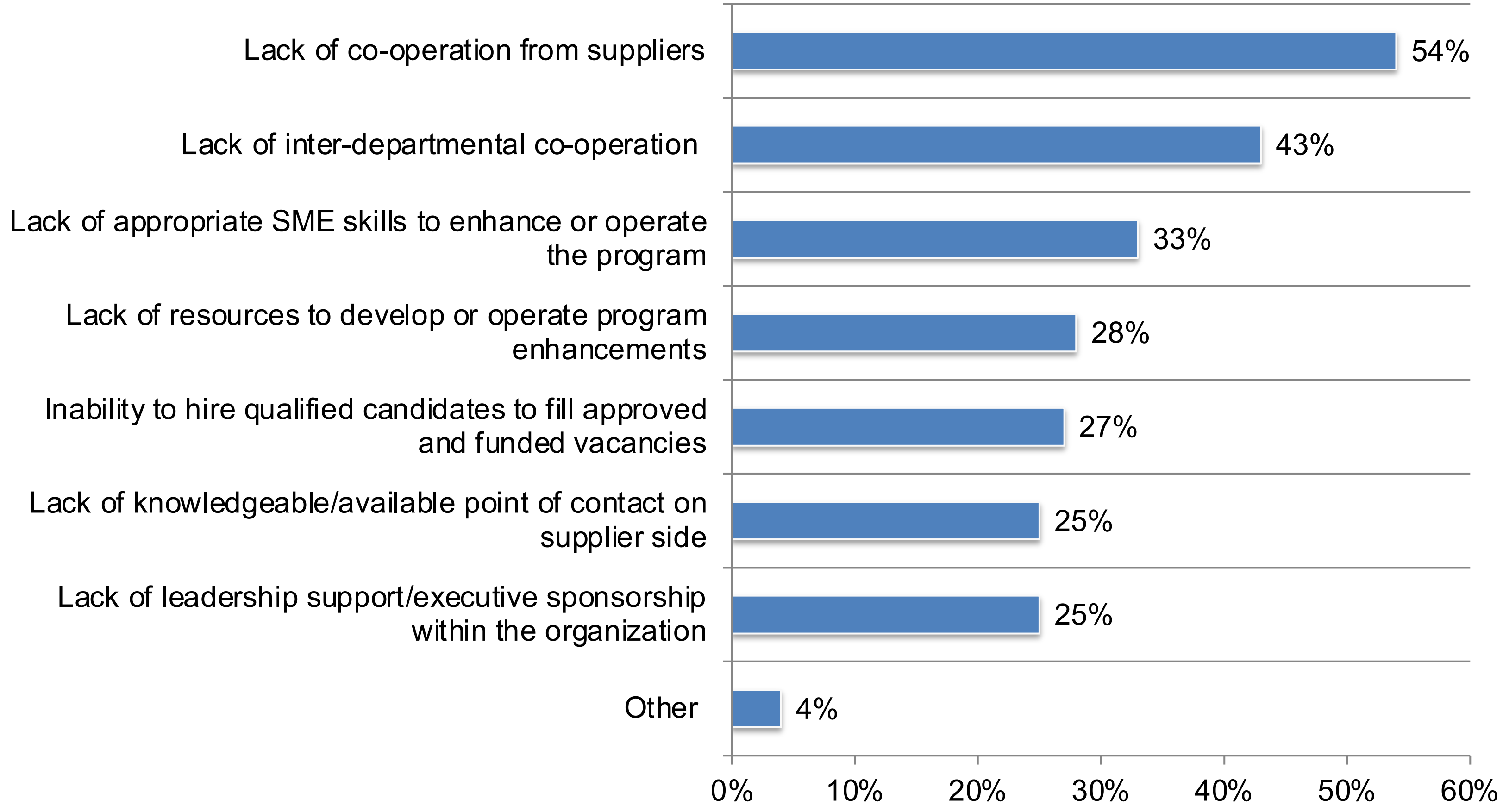
What are your organization's barriers to having a successful SCRM program?

More than one response permitted



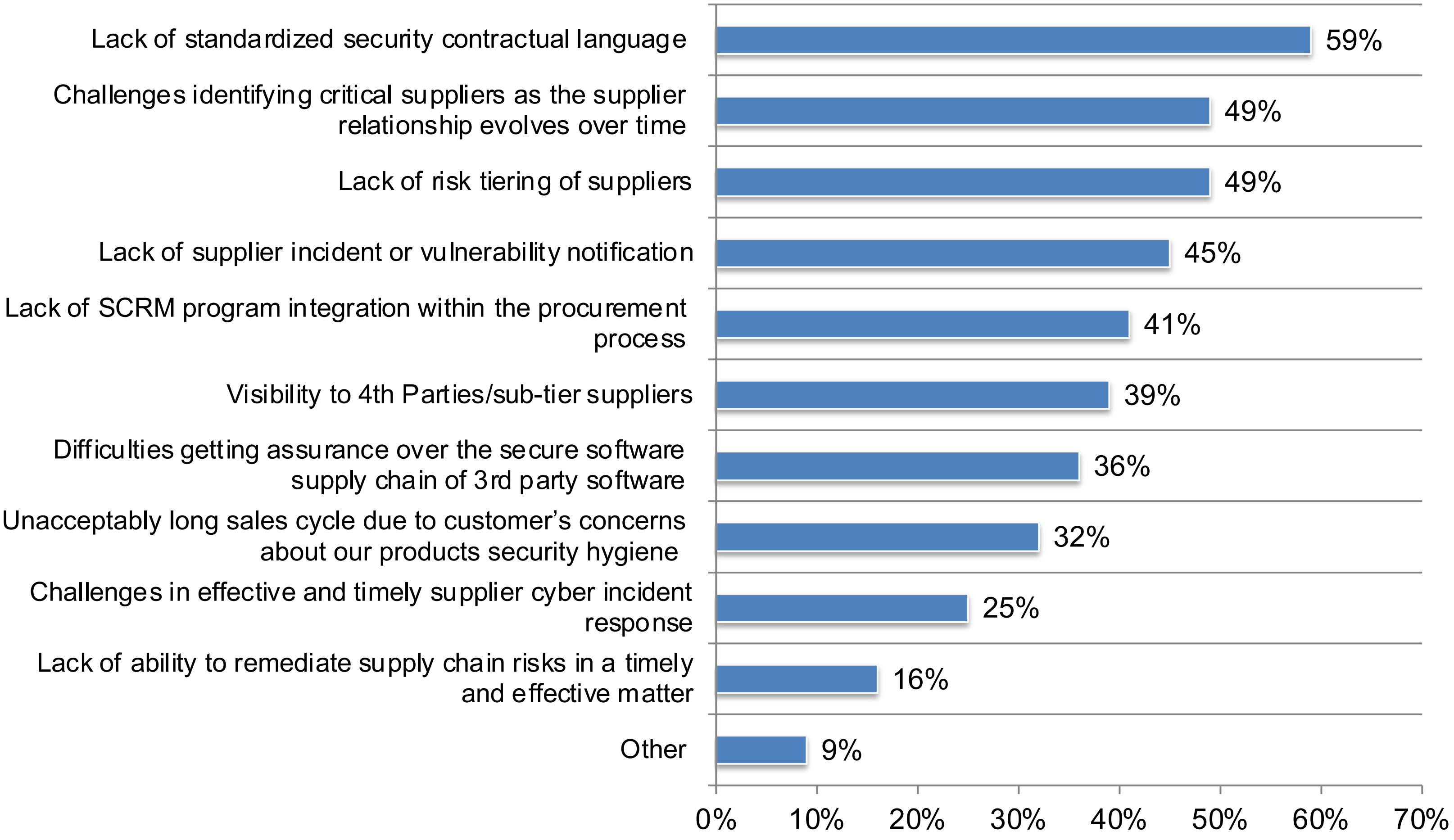
What are the main people-related impediments or challenges to achieving an effective SCRM program?

More than one response permitted



What are the main process-related impediments or challenges to achieving an effective SCRM program?

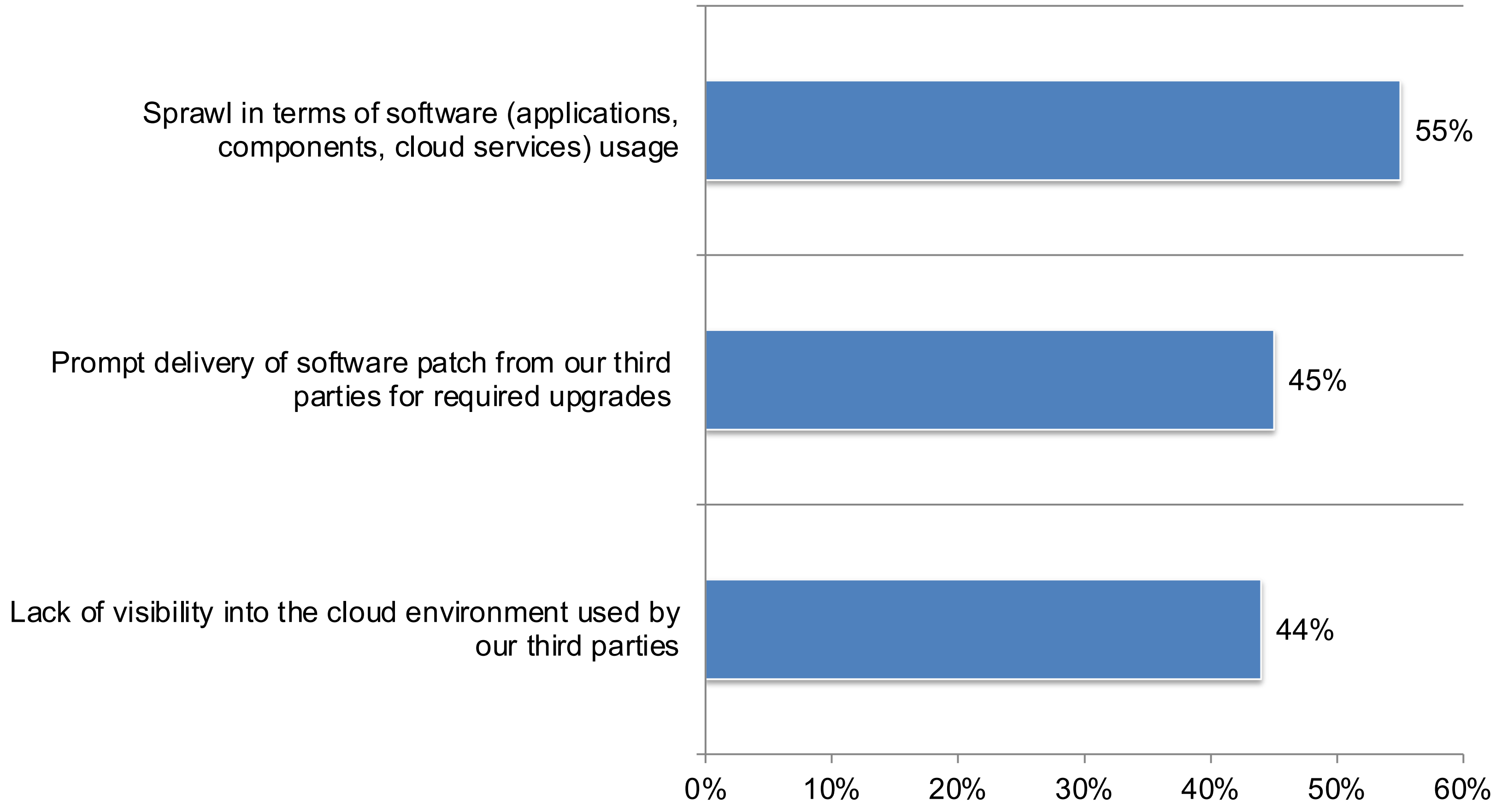
Four responses permitted



Ponemon INSTITUTE

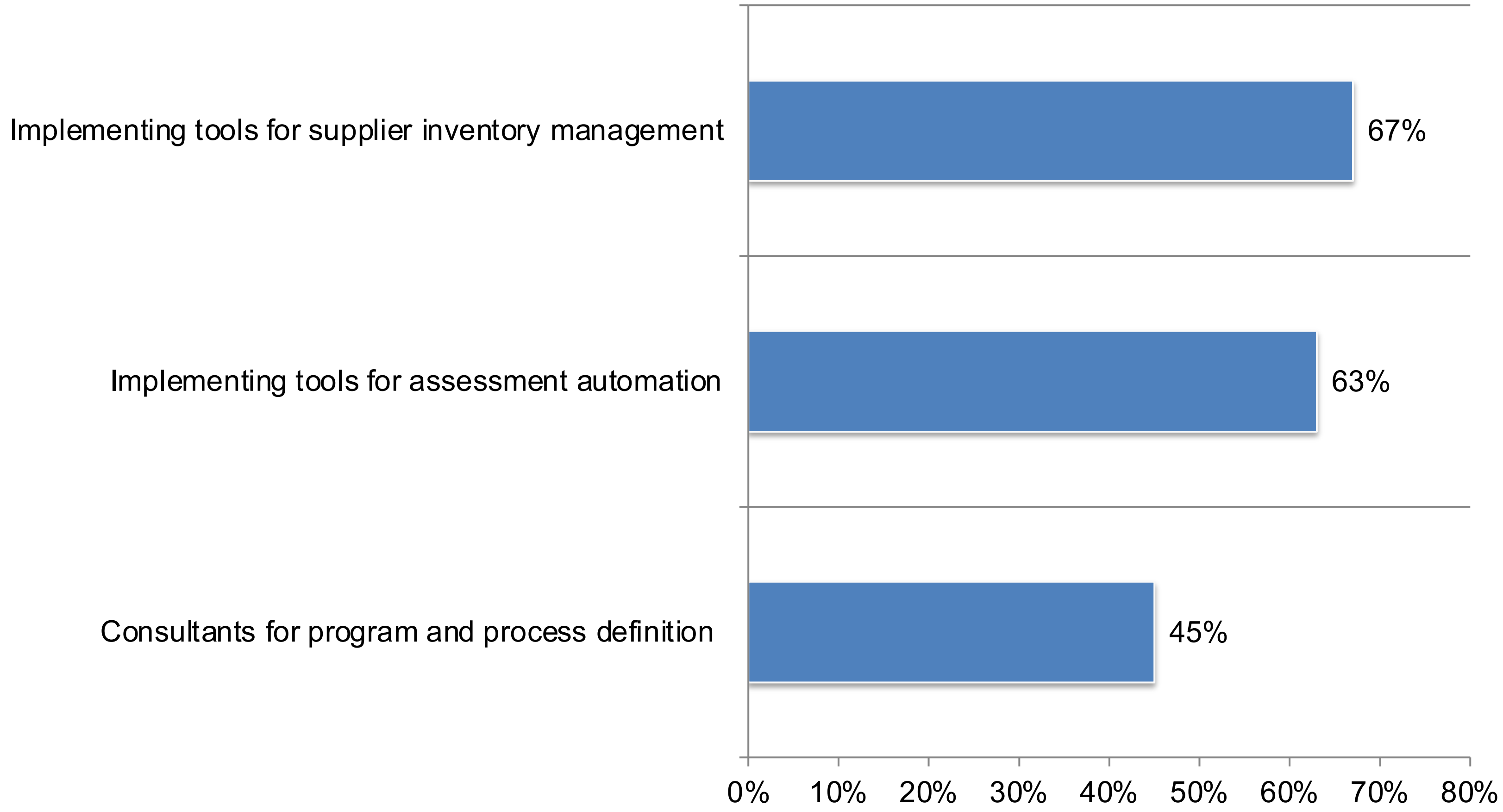
What are the main technology-related impediments or challenges to achieving an effective SCRM program?

Top three responses presented



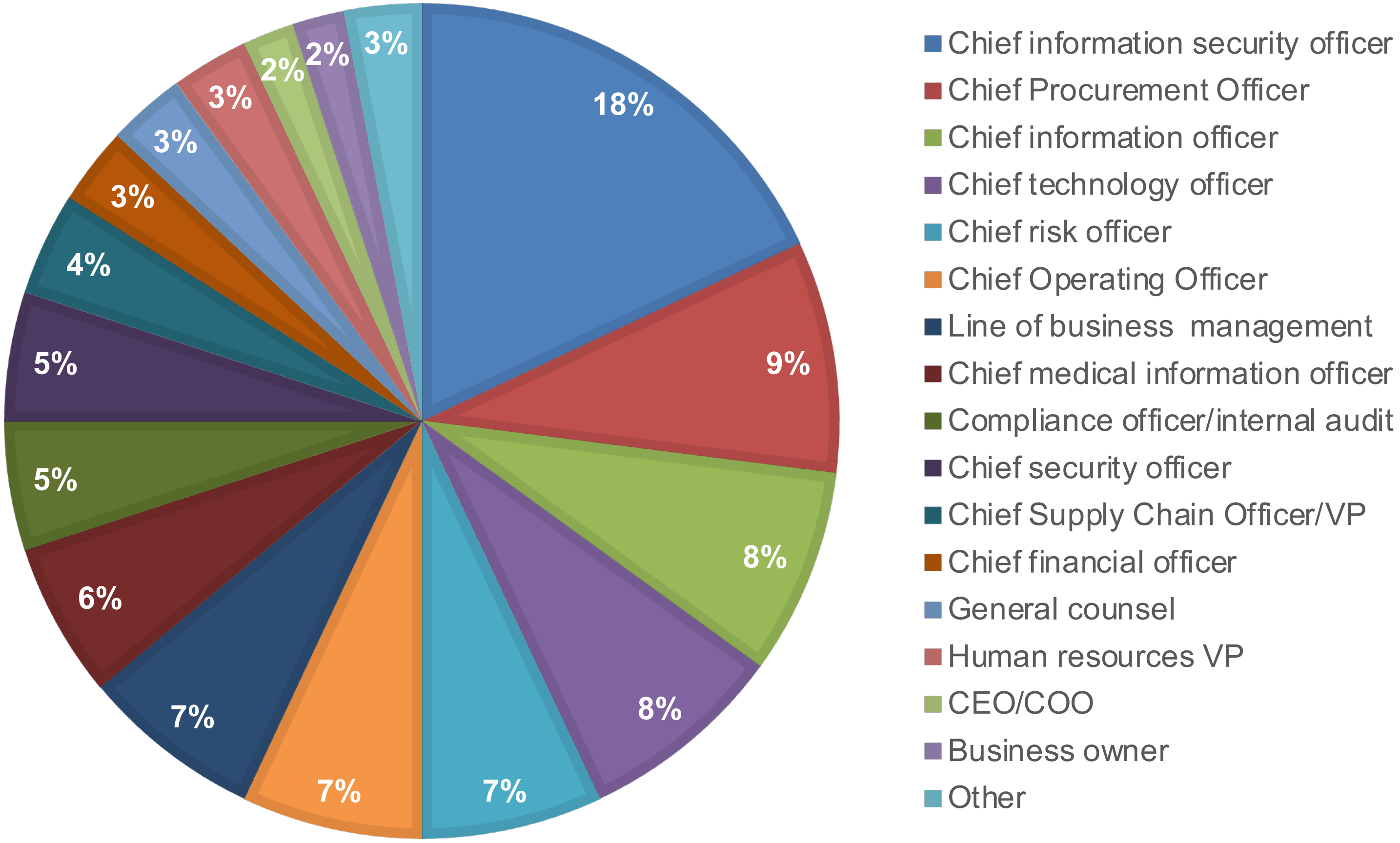
What are your organization’s top three priorities for SCRM investments?

Top three responses presented

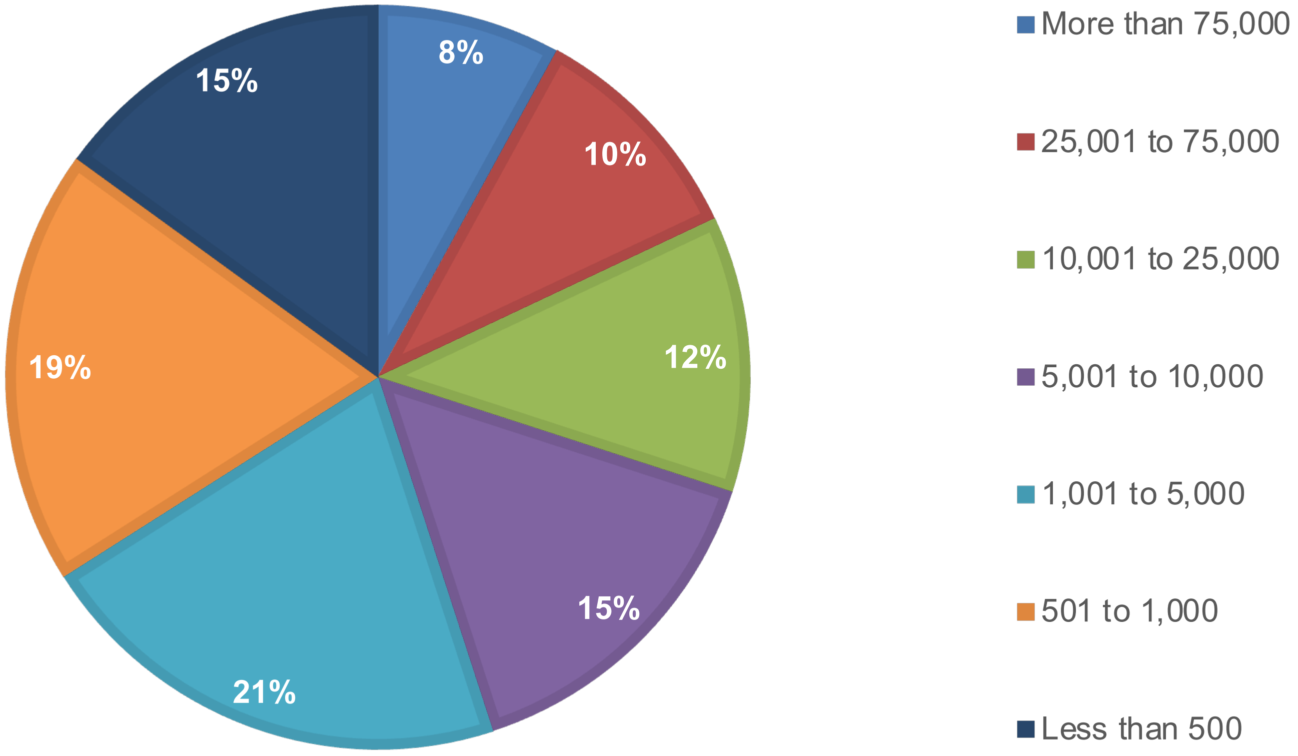


Methodology

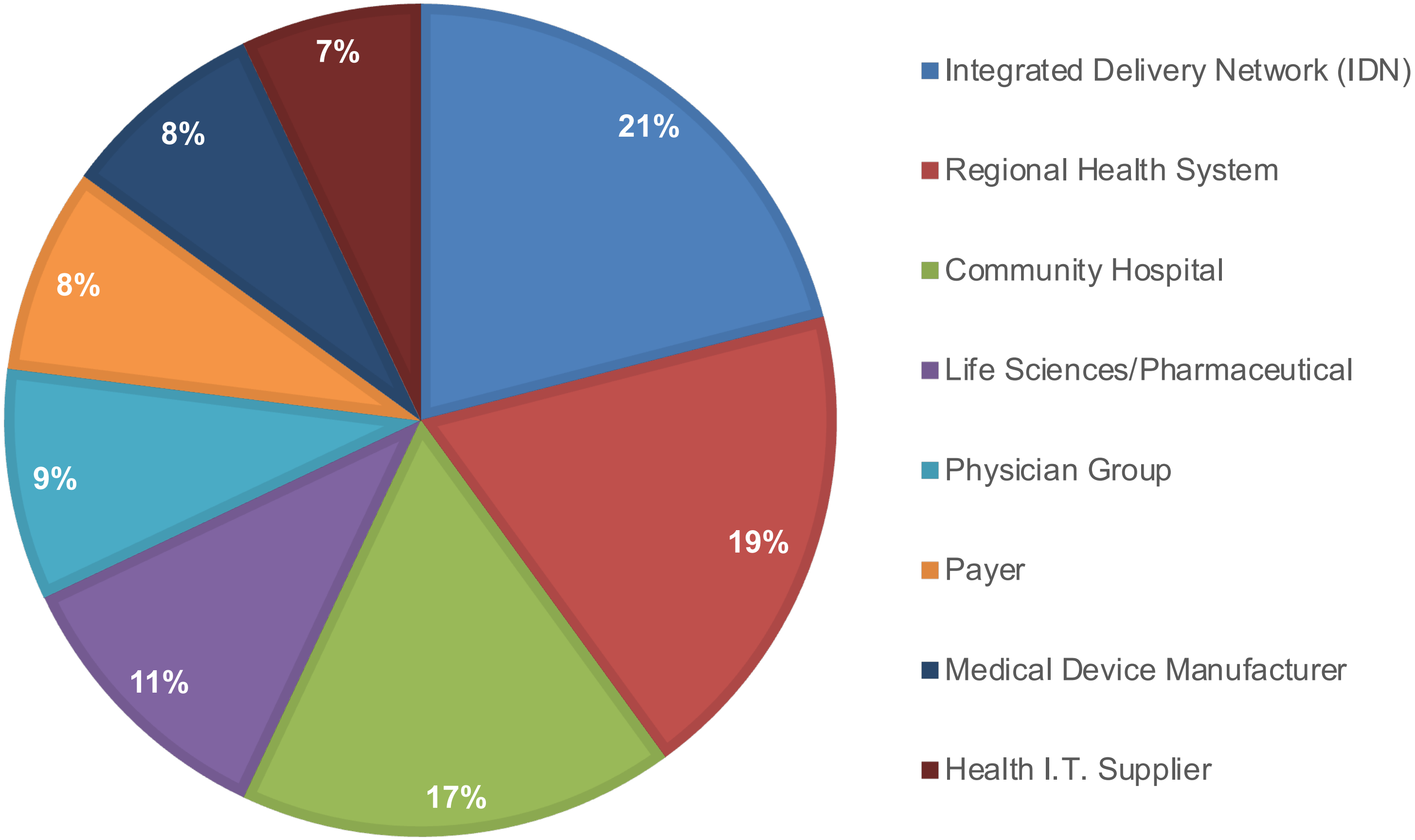
Direct reporting channel



The number of employees within the organization



The type of organization



Caveats to these studies

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 individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT security professionals. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would 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 subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Questions

Ponemon Institute
Toll Free: 800.887.3118
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
research@ponemon.org