




[Activate yo](#)

ADVERTISEMENT


  **Read how CIOs are bringing business and IT together.**
[Download "The New CIO: Change Partner and Business Leader" now.](#)


 what makes y



HOME NEWS MAGAZINE CIO RESOURCES WEBCASTS WHITE PAPERS WEEKLY PODCASTS TOPI

SEARCH:  ADVANCED SEARCH | SITE INDEX search powered by: 

AD  TechTarget Events, the most targeted events for today's top enterprise IT pros. [View full schedule of upcoming topics and dates!](#)

[HOME](#) > [CIO News](#) > Risk management: Think policy first, technology second

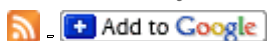
CIO News: Headlines

RISK MANAGEMENT: THINK POLICY FIRST, TECHNOLOGY SECOND

By Kate Evans-Correia, News Editor

05.10.2007 | SearchCIO.com

RSS FEEDS: [IT news and analysis for CIOs](#)



NEW ORLEANS -- Security and compliance needs are driving improvements in technologies such as identity management and content monitoring. But too many businesses are relying on technology rather than policy to deal with risk management issues.

You need to build a defensible case.

Paul Proctor
 research vice president,
 Gartner Inc.

"I get calls all the time from companies who want to know what technology they should buy," said Paul Proctor, research vice president at Stamford, Conn.-based Gartner Inc. "I always ask first, 'What value are you trying to achieve?' You have to start with a policy."

The primary objective of a compliance audit, Proctor said, is to confirm you have the right controls in place and that you've anticipated risk.

Technology is not the answer, however, warned Proctor, who shared the stage with analyst Mark Nicolett at Gartner's Compliance and Risk Management Summit Wednesday. Indeed, if an auditor finds fault with your controls, it will more likely be due to your failure to implement policy or process, not because you chose the wrong technology, they said.

"A risk assessment is a key driver in figuring out what you need to do and where you should be spending your money," he said. At the end of the day, the auditor wants to know if you've taken "due care" -- have you done at least what your peers are doing?

"You need to build a defensible case," Proctor said. Once you have a policy in place, technology can help you do that, he added, listing six new technologies you need to know about:

1. Identity and access management (IAM).
2. Security information and event management (SIEM).

3. Configuration auditing.
4. Content monitoring.
5. Database activity monitoring.
6. IT governance risk and compliance.

Security = People, policy, technology

IAM is the cornerstone of compliance, and if you implement only one technology, this should be the one, Proctor said. It's basic technology for meeting Securities and Exchange Commission (SEC) and security requirements, he said, adding that it should encompass the enterprise. "Most security and risk efforts are worthless if you cannot bind an ID to an individual." Auditors will look for who has access and to what. IAM is so important to security and compliance that Gartner expects IAM investment by businesses to increase by 60% this year.

Dave Kilgus, an IT audit manager at educational publishing company Pearson, is likely to help fuel some of those sales of IAM technology. He admits to being a compliance newbie (the company recently relocated to the U.S. from the U.K., so it now must adhere to SEC regulations), but he added that a number of compliance-related technologies are "still very young and immature" -- and unfamiliar to users. He said he anticipates some resistance to some of the blocking and tracking technologies he'll have to put into place. Still, he said, it can be done if buy-in "comes from the top."

Although still beset by ambiguity and high cost, a growing number of businesses are also looking at [security information and events management](#). SIEM is technology that collects and analyzes security events, making it easier to detect malicious activity. Compliance issues are driving about 80% of the SIEM business, Nicolett noted. The technology goes hand in hand with IAM -- SIEM tells you how effectively you're using IAM, he said.

[Content monitoring systems \(CMS\) and filtering tools](#) flag questionable content to prevent sensitive data from being leaked outside company walls. "It looks for sensitive data" and shows "great promise," Proctor said.

"This is one of those areas where you have to think about what you consider sensitive data," he said. "Figure it out before you buy the technology."

In addition, businesses need to be aware of legal implications, so it's important to develop a monitoring policy with human resources. "CMS is [for finding] bad business practices, not [for finding] the bad guys," Proctor said. Without exception, companies are shocked by some of the content flagged by CMS, he said. "But CMS doesn't stop it from happening." Let users know what is acceptable usage and what is not. Develop an effective policy, he said, and "train them not to do that."

More on monitoring and CIOs

[CIOs: Monitoring employees thwarts Internet abuse](#)

[Employee monitoring facts every CIO should know](#)

[Compliance drives security configuration management](#)

[Content monitoring tags questionable email activity](#)

Configuration auditing technology red flags unauthorized changes in your network, including downtime due to system failure, the introduction of security vulnerabilities and insider security threats. But configuration auditing solutions require well-defined configuration policies and change management processes -- something that's down the road for all but the largest businesses, which are already using the technology. "This is a newer area," Nicolett said, and not a lot of auditors require it -- not across the board, anyway. "It's a nascent technology. One you should keep your eye on."

Databases are everywhere, but they are, by nature, particularly difficult to secure. As a result, Nicolett said he sees a "huge pickup" in interest in database activity monitoring technologies. You only have to look as far as the [TJX security breach](#) and regulations such as the [Payment Card Industry Data Security Standard](#) to understand why -- a database breach is costly in more ways than one,

he said. Proctor and Nicolett suggest businesses look at "database activity monitoring as a viable stopgap for legacy systems, while systems are re-engineered for encryption."

IT governance and policy management technology collects all your security policies -- IT security standards, control objectives and best practices -- and organizes them into a common set of process, access and configuration controls so they can be distributed, read and acknowledged. Proctor said this will help businesses "strengthen external audit posture and reduce cost of control measurement and compliance reporting." But, the technology should not be used as a substitute for "policy development work," he added.

Proctor and Nicolett suggest businesses investigate these technologies as part of an overall strategic plan and chose technology only after assessing need and carefully analyzing what's required.

At the end of the day, Proctor said, technology only "automates good process."

Let us know what you think about the story; email: [Kate.Evans-Correia, News Director](mailto:Kate.Evans-Correia@NewsDirector.com)

Share - [Digg This!](#) [Bookmark with Del.icio.us](#)



CIO RELATED LINKS

Ads by Google

IT Guidebook

Information Technology Resources, Articles, Careers, Computer Tech!
www.itguidebook.com

Help Desk Outsourcing

Identify, manage, report & solve IT issues with Track-It!® - Demo
www.NumaraSoftware.com

Report For IT Consultants

Get A Free White Paper For Systems Integrators and Consulting Firms.
SAP.com/USA

Unlimited Offshore Talent

Out-of-the-box Outsourcing Simplified, Streamlined and Secured!
www.i-Shore.com

BS Information Technology

Online, accredited, self paced pro -grams designed for busy adults
www.ColumbiaSouthern.edu



RELATED CONTENT

▪ Risk management

Second Life a security risk for businesses, Gartner cautions
Staffing for security, risk management and compliance
Risk management staffing isn't always part of IT
Enterprise risk management for CIOs
Tips for building a cost-effective risk management plan
Content monitoring tags questionable email activity
Risk Management Strategies for CIOs
Identity and access management strategies for CIOs
(on the job) - Security as You Like It
Why did Microsoft delay IE Patch?

▪ Information security management

Experts: Wi-Fi eavesdropping persists despite stronger security
Second Life a security risk for businesses, Gartner cautions
Blog: Data loss rarely leads to ID theft, or does it?
CIOs overconfident about protecting intellectual property
Managing mobile computing policies