

Additional thought leadership resources

EY regularly publishes **Insights on governance, risk and compliance**, including thought leadership on information security topics. These perspectives are designed to help clients by offering timely and valuable insights that address issues of importance for C-suite executives. Please visit www.ey.com/GRCinsights

Beating cybercrime. Security Program Management from the Board's perspective.

Most organizations struggle to keep pace with the breakneck velocity of these changing technologies and threats, creating hazardous gaps between the true risks that threaten their viability and their ability to respond and mitigate these risks effectively. Organizations can benefit from an objective assessment of their information security programs and structures via EY's Security Program Management approach.

www.ey.com/spm



Cybersecurity: considerations for the audit committee

Cybersecurity is not just a technology issue; it's a business risk that requires an enterprise-wide response. Boards of directors are starting to take note, particularly members of the audit committee, who now list cybersecurity among their top concerns.

[http://www.ey.com/Publication/vwLUAssets/Cybersecurity_Considerations_for_the_audit_committee/\\$FILE/Cybersecurity_considerations_for_the_audit_committee_GA0001.pdf](http://www.ey.com/Publication/vwLUAssets/Cybersecurity_Considerations_for_the_audit_committee/$FILE/Cybersecurity_considerations_for_the_audit_committee_GA0001.pdf)



Security Operations Centers against cyber crime. Top 10 considerations for success.

Understanding that security information attacks can never be fully prevented, companies should advance their detection capabilities so they can respond appropriately. A well-functioning Security Operations Center (SOC) is at the heart of all such efforts. We explore the top 10 considerations critical to the success of your SOC.

www.ey.com/soc



Identity and access management (IAM): beyond compliance

IAM is evolving into a risk-based program with capabilities focused on entitlement management and enforcement of logical access controls, leveraging new technologies to transform from a compliance-based program into a true business enabler.

www.ey.com/iam



Business continuity management

Approximately 50% of companies neglect to take steps to safeguard their businesses in the event of a disaster, which could potentially threaten their existence. Disasters and the resulting non-availability of resources can be devastating, and leading companies have increasing awareness of the need to develop, maintain and sustain effective business continuity management programs.

www.ey.com/bcmtrends



Privacy trends: the uphill climb continues

As the privacy landscape continues to evolve and mature, trends are forming around how market conditions are impacting organizations' privacy decisions. Our report highlights the three megatrend categories playing increasingly large roles as we enter a new era in privacy protection: governance, technology and regulation.

www.ey.com/privacy2013



Key considerations for your internal audit plan: enhancing the risk assessment and addressing emerging risks

The internal audit risk assessment and the ongoing refresh processes are critical to identifying and filtering the activities that internal audit can perform to provide measurable benefit to the organization. The processes begin by identifying these emerging risks and focus areas and their corresponding practical, value-based audits.

www.ey.com/iaplan



Please also see this book on cybersecurity published by EY and ISACA: http://www.ey.com/US/en/Newsroom/News-releases/News_Five-Things-Every-Organization-Should-Know-about-Detecting-and-Responding-to-Targeted-Cyberattacks