

Better Protect Your Organization from Cyber-Risks

THE FOUR-STEP ACTION PLAN THAT YOU CAN APPLY TODAY

Technology—powered by software—underlies every aspect of the way businesses run, from office productivity, to HR systems, to point of sale, to data gathering and management, to accounting and finance. Because technology is now mission critical to every aspect of business, the acquisition and deployment of technology, including software, is increasingly occurring outside of a centralized IT function. Today 35% of IT spend happens outside IT departments.¹

As software has become an integral part of every business, the risks associated with its deployment have increased. On average an organization experiences a cyber-attack every seven minutes,² and IDC projected that in 2014 enterprises spent \$491 billion because of malware.³

Although managing cyber-risk is complex, there is a critical first step—understanding what is installed and running in a company's own network, and making sure that software is both genuine and fully licensed. Failure to take this threshold step can have serious consequences. A recent study by IDC found that there is a strong positive correlation (0.79) between the presence of unlicensed software and the likelihood of encountering malware.⁴ By comparison, the correlation between education and income is 0.77.

Cybersecurity risks are of such concern that the 2013 expanded COSO Framework—the recognized global standard for internal controls—includes a recommendation

that companies adopt internal controls related to the legal use of technology, including software license compliance.

In addition, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published a standard specifically on Software Asset Management (SAM), which is designed

DID YOU KNOW?

The ISO/IEC 19770—1:2012

SAM standard covers all aspects of the software lifecycle, including acquisition, deployment, and retirement, regardless of the departments in an organization responsible for these activities.

to help companies ensure they're properly managing their software in a way that ensures continuous compliance, minimizes exposure to risks, and maximizes the benefit companies derive from this critically important asset.

THE FOUR KEY STEPS TO IMPLEMENTING ISO-ALIGNED SAM

STEP 1: Conduct an Assessment

Gather and maintain reliable and consistent data that you can use to assess whether or not you are properly licensed.

STEP 2: Align to Your Business Needs

Match your current and future business needs to the right licensing model.

STEP 3: Establish Policies and Procedures

Ensure that SAM plays a role in the IT lifecycle in your business. For ISO-aligned SAM to be effective, the practices need to support the business's IT infrastructure and management needs to support the SAM process.

STEP 4: Integrate within the Business

Ensure that SAM is integrated and supports the entire business.

CONTINUE READING FOR [A DETAILED LOOK AT THIS STEP-BY-STEP PROCESS](#) ▶

1. TechInsights Report: The Changing Role of IT and What To Do About It, CA Technologies, 2013. <http://rewrite.ca.com:80/content/rewrite/us/articles/management-cloud/the-changing-role-of-it-and-what-to-do-about-it.html>.
2. Fighting Cybercrime with Actionable Insights, IBM Corporation, 2014. <http://www.slideshare.net/IBMBDA/infographic-fighting-cybercrime-with-actionable-insights>.
3. The Link between Pirated Software and Cybersecurity Breaches: How Malware in Pirated Software Is Costing the World Billions, IDC, 2014. https://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf.
4. Unlicensed Software and Cybersecurity Threats, IDC, 2015. <http://bsa.org/malware>.

THE FOUR KEY STEPS TO IMPLEMENTING ISO-ALIGNED SAM

Effective SAM practices support the overall strategy and goals of the business, not just its IT structure. A sound SAM program will work to improve efficiency and the effectiveness of the organization's existing IT operations and services. Having sound SAM policies, procedures and controls embedded into internal controls enables your organization to benefit from an environment that produces continuous compliance and improvement. Implementing the following four steps is your organization's first line of defense against malware and other cyber-risks.

STEP 1: Conduct an Assessment

Gather and maintain reliable and consistent data that you can use to assess whether or not you are properly licensed.

- Find out what software is running on your network;
- Understand whether or not that software should be there; and
- Determine whether all software running in your network is legitimate and properly licensed.

STEP 2: Align to Your Business Needs

Match your current and future business needs to the right licensing model.

- Look at new forms of licensing that may be more cost-effective, such as cloud subscriptions;
- Identify possible cost savings. Example: reuse licenses (if allowed by the vendor); and
- Make better use of maintenance clauses in your software license agreements to ensure you are getting appropriate value for the expenditure.

STEP 3: Establish Policies and Procedures

Ensure that SAM plays a role in the IT lifecycle in your business. For ISO-aligned SAM to be effective, the practices need to support the business's IT infrastructure and management needs to support the SAM process.

- Acquire software in a controlled manner with records to support the choice of platform on which the software will run and the procurement process;
- Deploy software in a controlled manner which also assists with the on-going maintenance of the software deployed in the business;
- Remove software from retired hardware and properly redeploy any licenses within the business; and
- Routinely install software patches and upgrades in a timely manner.

STEP 4: Integrate within the Business

Ensure that SAM is integrated and supports the entire business.

- Integrate SAM into all relevant life-cycle activities within the business, not just IT lifecycles;
- Improve on the data management processes built in Step 1; and
- Ensure employees understand the proper use of software and the legal, financial, and reputational impact their software related actions can have on the organization.

ABOUT BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

Copyright 2015, BSA | The Software Alliance. All rights reserved. Learn more at www.bsa.org.

