Using Open Source Tools to Support Technology Governance

Most practitioners are already very accustomed to using technical tools for specific tactical purposes when it comes to security or assurance within their environments. These tools can be open source or commercial: For example, practitioners might employ open-source tools such as Clam, Wireshark or OpenVAS to accomplish specific tasks (antivirus, network analysis and vulnerability assessment, respectively) or they might leverage commercial products to provide anything from intrusion detection systems (IDS) to firewalls to data loss prevention (DLP) to cloud access security broker (CASB) capability (and beyond). In short, tools—the careful selection and the judicious use thereof—are an important part of being a practitioner in these subject areas.

Ed Moyle
Is director of thought leadership and research at ISACA. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers and senior security analyst with Trintech. Moyle is coauthor of *Cryptographic Libraries for Developers* and a frequent contributor to the information security industry as an author, public speaker and analyst.

However, when it comes to technology governance (governance of enterprise IT [GEIT]), it can often be harder to find specific tools that can assist the practitioner. The reasons for this are not hard to understand. First and foremost, governance is, by definition, an exercise that requires significant customization from organization to organization; how governance is implemented in organization A is likely quite different from organization B. This is due, in part, to differing goals (both enterprisewide goals as well as the technical goals that cascade from stakeholder needs), differing metrics and key performance indicators (KPIs) used to ensure continuous improvement, different culture and risk appetites, and numerous other organization-specific factors. This, in turn, makes it hard to find and use one-size-fits-all tools that can ubiquitously support implementations across a number of organizations.

That said, there are a few tools that practitioners with an eye toward holistic and systematic governance can employ to help them along the path. In this column, some of these tools and how they can be used in a broader governance implementation are highlighted. There are, of course, more tools than can be covered in a cursory overview such as this one; that said, this column calls out a few that can be of use in an organization's governance efforts.

Moreover, since it is a truism that budgetary considerations can be a factor (particularly in times such as these when budgets are lean and scrutiny is high), open-source tools that can be used for this purpose are highlighted. Note that this is not to imply that there are not commercial tools out there that can do similar things or help in different ways; in fact, nothing could be further from the truth as there are hundreds (if not thousands) of commercial products that can assist in GEIT implementation. But, given that not every organization will have the same level of budgetary support available (not to mention that the vendor landscape is often mutable), this column puts the spotlight on open-source options.

For the organization undertaking a GEIT implementation, it can be challenging to get traction and get started. Budgetary considerations can sometimes be a limiting factor in terms of making progress. Where this is the case, open-source tools can have the benefit of a rapid "on ramp" that might not otherwise be the case.

1 Asset Inventory

As every practitioner knows, asset management is challenging to do well. Consequently, leveraging tools that bolster asset management can have broad-reaching benefits in a number of areas. In the context of GEIT specifically, though, tools that support asset management can be particularly valuable. Why? Because during the implementation phases of a GEIT rollout, organizations undertake a few key activities: (i.e., risk assessment and evaluation, establishment of KPIs and performance metrics, setting of appropriate scope). At a macro level, these tasks will not (necessarily) require a component-level awareness of every system, application or node that an environment has fielded. But, as an organization starts scratching the surface and goes beyond the macro level into the more detailed planning of any of these activities, accounting for the unique nuances of an environment (which presupposes one knows what is in it) can mean the difference between success and failure.

With this in mind, tools that support asset inventorying and discovery, such as GLPI *(www.ubuntugeek.com/glpi-it-and-asset-managemet-software.html)* and OCS Inventory NG *(www.ocsinventory-ng.org/en/)* can be beneficial. Organizations can use them to discover what they already have in place to assist in risk management efforts. They can also use them to keep a record of what they have fielded and tie that information together with metrics gathering to assist in establishing ongoing performance improvement metrics. Further, organizations can tie the information contained within that system to support everything involved in the implementation phase of their GEIT planning.

2 Risk Management

ISACA's *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT* highlights the need for a risk assessment during the implementation phase of a GEIT rollout: Specifically, the guide outlines that, "Risk assessments and monitoring should also be performed for the implementation of the GEIT initiative to ensure that program risk—whether it is resource commitments, budgeting or schedule—is addressed to keep the program on track."[1] This indicates that assessing risk—and responding accordingly—is part and parcel of the implementation of GEIT itself. It is in this area that free and open-source tools can help support the implementation.

There are few ways in which this is true. First, tools such as SimpleRisk *(https://www.simplerisk.it)* can help keep track of risk at a high level by recording what the areas of risk are, providing a way to track them over time, supporting tying together mitigation strategies to the risk areas themselves and recording remediation progress. Likewise, there are free tools that can help organizations understand what the risk factors are and identify/contextualize them. For example, a tool such as Practical Threat Analysis (PTA) *(www.ptatechnologies.com)* can help develop a systematic threat model to ensure that the organization is looking at risk systemically. Depending on the level that stakeholders want to reach in doing this, they can, potentially, leverage tools such as OpenVAS or Vega to help identify vulnerabilities in the surface of applications and infrastructure that can inform the risk profiling that they do. Granted, not every GEIT implementation will take the risk assessment portion of the implementation to this granular a level, but the option is there should the organization choose to do so.

3 Monitoring

The goal of a GEIT implementation is to get to a feedback loop of continuous improvement. Meaning, by monitoring the organization in an ongoing way—and being alert to the metrics and KPIs that tie back to stakeholder requirements—organizations can see areas of improvement and build upon them to get better. It is here where there are a number of options that can assist.

First, there are a number of tools out there to support performance monitoring. This includes tools such as Icinga 2 *(https://www.icinga.com/products/icinga-2/)*, Nagios *(https://www.nagios.org)*, OpenNMS *(https://www.opennms.org/en)* and Zabbix *(www.zabbix.com)*. Any information about performance can directly speak to reliability and accessibility information that will likely be of interest as the organization completes a governance implementation. Thinking more broadly, though, tools that build upon this such as Observium *(https://www.observium.org)* or Cacti *(www.cacti.net)* can provide additional layers of detail depending on how deep the organization intends to go. Of course, some organizations may already have tools in place that provide similar information, but for those that do not, this might provide the needed information.

Doing the monitoring is important, of course, but so is the ability to render monitoring information into a format that enables the organization to act upon it. Tools that assist in data visualization, for example, Datawrapper *(https://www.datawrapper.de/gallery)* and the like, can likewise be of benefit to an organization from a governance point of view.

Endnotes

1 ISACA®, *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT*, USA, 2016, *www.isaca.org/getting-started-with-GEIT*