

Prioritizing Aspects of Technology Risk Assessment and Mitigation

Joel Lanz

Joel Lanz is a former Big 5 Partner who leads a CPA technology assurance and advisory practice. He can be reached at jlanz@itriskmgmt.com.

Recent world events, economic challenges, and regulatory pressures are forcing operational risk managers (ORMs) to cost-effectively mitigate technology-related operational risk in an ever more complex environment. When managing technology risk, the ORM is confronted with multiple high-priority items, for example, ensuring a high level of information security vs. implementing new systems quickly to capture competitive advantage vs. increasing return on investment (ROI) on technology investments. Unlike financial risk, technology risk cannot be easily quantified or measured.

Current literature suggests that the ORM should manage (and mitigate) all of these risks simultaneously; however, the same literature does not mention how to prioritize these equal needs when resources to manage these needs are very tight or not available. Many external parties and stakeholders—be they regulators, insurance carriers, customers, or electronic trading partners—require financial organizations to perform technology risk assessments (TRAs). Competing methods and lack of generally accepted standards for performing these TRAs enhance the challenges faced by ORMs in adequately assessing and effectively measuring technology risk. The increasing requests by external parties and stakeholders of ORMs to disclose the results of TRAs, even while corrective actions are being prioritized and developed, further challenge the ORM in mitigating vulnerabilities based on prioritized rather than externally perceived risk.

The goal of this article is to provide ORMs with the information needed to successfully assess technology risks in their organizations. We will provide information on current technology-risk-assessment activities by comparing and sharing real-world insights on the use of these assessments; discuss the evolving corporate governance role in assessing and monitoring information technology (IT) risk; identify common critical vulnerabilities and popular corresponding risk-mitigation strategies; describe how properly performed vulnerability and penetration testing helps in identifying more than just security risks; and provide a number of targeted questions that ORMs can ask to obtain a high level of understanding of the effectiveness of their organizations' existing technology-risk-management activities.

WHY THE NEED TO PERFORM TRAS?

Banks can realize a substantial number of financial and operational benefits by conducting an effective TRA. These include enhancing corporate governance over IT activities, proactively identifying vulnerabilities and implementing risk-mitigation strategies, effectively aligning risk-management activities with business imperatives, and efficiently using corporate risk-management resources, including audit, in ensuring a cost-effective control environment. Even with these benefits, many banks rely on external drivers, such as Basel Committee expectations, regulatory requirements, or insur-

Prioritizing Aspects of Technology Risk Assessment and Mitigation

ance underwriting standards, in order to perform a TRA.

The Basel Committee on Bank Supervision's "Sound Practices for the Management and Supervision of Operational Risk" significantly influenced how bankers view operational risk. As identified in Principle 4:

Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. (In a risk assessment) a bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify strengths and weaknesses of the operational risk environment.¹

Obviously not limited to IT, the impact of the guidance has resulted in banks identifying and reviewing risks in all major operational areas. Larger banks, with their global reach and complexity, have seized upon the Basel Committee's expectations and guidance in initiating proactive risk-management initiatives.

In the community banking sector, regulatory requirements—especially the interagency Guidelines Establishing Standards for Safeguarding Customer Information, as mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999—have driven the need to perform TRAs. The corresponding examination procedures,² intended to assist examiners in assessing compliance with the guidelines, provide a basis on which community bankers can evaluate the quality of their TRA programs. TRAs performed to comply with these standards generally enable banks to establish the foundation on which security programs can be managed and maintained.

With recent global events, many banks have enhanced their awareness of cyber threats, including traditional frauds and new cyberterrorist concerns. Some banks choose to transfer this risk to a third party through the purchase of an e-commerce insurance policy. These policies can range from adding an appropriate rider to an existing policy to purchasing a new policy specifically addressing electronic risks. In either event, insurance underwriters will require the bank to assess its technology risk to effectively and properly quote the required coverage. These assessments can include the bank's performing any of the following:

- Completing a high-level questionnaire (typically three to six pages)
- Engaging the insurance broker to perform the assessment
- Engaging an independent party to perform the assessment
- Having appropriate staff complete the risk assessment

Regardless of the reason for performing a TRA, the ability of the bank to identify vulnerabilities and to prioritize and proactively manage strategies to mitigate the threats that could exploit vulnerabilities is key. Given limited budgets, competing strategic initiatives, and various economic challenges, the bank's ability to prioritize the numerous threats and vulnerabilities that exist in today's environment is crucial for enterprise financial and operational success. Given the various existing TRA methodologies, the bank must choose a methodology that best reflects the needs of the enterprise and stakeholders.

TRA METHODOLOGIES

The effectiveness of risk-based decisions is limited to the quality of the TRA. With the increasing interest in operational risk management and concerns about corporate governance, it is no surprise that various vendors have rushed to market recently developed or revised proprietary enterprise risk-management methods to help banks navigate the assessment challenge. Although these methods provide an adequate perspective from a credit, financial, and environment standpoint, they tend to be weak in areas relating to technology. This may be because the methodologies are developed by and geared to traditional risk managers (i.e., risk managers whose pedigree is financial or credit) rather than to those who truly understand technology risk and its complexity.

To adequately assess and prioritize technology risk, the ORM must supplement risk-assessment tools with methodologies specifically geared to technology. Although the regulators do not specify or recommend TRA methodologies by name, fortunately for the ORM, much guidance is available. As they do with enterprise-risk-assessment tools, ORMs can use methods developed by vendors. A number of challenges face ORMs using this approach, however:

- Not all vendor methodologies appropriately consider technology to the extent recommended by key technology experts.
- The bank becomes dependent on the vendor and its consultants to perform, maintain, and complete the assessment.
- Because of the fees associated with outside consultants, the bank may not continually update the TRA throughout the year to reflect the rapid changes in technology risk and direction.

The American Bankers Association lists the following recommended resources for TRAs:³

- International Standards Organization (ISO) 17799 (ISO Standards)
- Control Objectives for Information Technology (COBIT)

- SysTrust
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
- National Institute of Standards and Technology (NIST)

The author believes that ORMs will find any one of these resources effective for TRAs. For the most part, these resources are inexpensive to implement. They are based on extensive research from government and professional security experts; vendor neutral; leveraged in proprietary methods; and enjoy excellent reputations among corporate governance experts.

A summary description of each TRA method follows.

ISO Standards

The ISO along with the International Electrotechnical Commission form the specialized system for worldwide standardization. The stated purpose of the ISO Standards is to “provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.”⁴ Originally developed in Britain, the standard has gained much popularity and is a favored TRA approach in Europe. It is typically used in larger organizations, especially those involved with international activities. The standard is often referenced and leveraged by other prominent methods. This international code of practice for information security management comprises 10 areas:

1. Security policy
2. Communications and operations management
3. Organizational security
4. Access control
5. Asset classification and control
6. System development and maintenance
7. Personnel security
8. Business continuity management
9. Physical and environment security
10. Compliance

COBIT

COBIT has been developed as a generally applicable and accepted standard⁵ for good IT security and control practices that provides a reference framework for management, users, and information systems (IS) audit, control, and security practitioners.⁶ Sponsored by the IT Governance Institute, which was established by the Information Systems Audit and Control Association (ISACA), COBIT addresses risk from both the business and technology perspectives. Internationally recognized, it is a well-regarded tool, incorporating both operational management and audit concerns, that has been adopted in organizations including the US House of Representatives, Charles Schwab & Co., and Swift.

The framework comprises 34 high-level control objectives. For each control objective, audit procedures and management guidelines are provided. The latter guidelines uniquely provide COBIT with a business management perspective; maturity models, critical success factors, key goal indicators, and key performance indicators are provided for each of the high-level control objectives.

SysTrust

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) recently introduced a service to provide assurance on the reliability of systems. The purpose of this service, known as SysTrust, is to increase the comfort of management, customers, and business partners with the systems that support a business or particular activity. The service considers four principles to evaluate whether a system is reliable:⁷

1. Availability: The system is available for operation and use at times set forth in service-level statements or agreements.
2. Security: The system is protected against unauthorized physical and logical access.
3. Integrity: System processing is complete, accurate, timely, and authorized.
4. Maintainability: The system can be updated when required in a manner that continues to provide for system availability, security, and integrity.

Although SysTrust was not necessarily developed as a risk-management tool, many organizations have found that the SysTrust principles could be adopted as an effective TRA tool since the principles provide a stakeholder’s perspective on the impact of technology on business activities. The AICPA/CICA is currently considering a new version of the SysTrust tool that would also incorporate e-commerce activities.⁸ Under the revision, five principles would replace the four above. Principles considered would include security, availability, processing integrity, online privacy, and confidentiality.

OCTAVE

Developed by the Software Engineering Institute (SEI) at Carnegie Mellon University, OCTAVE is a comprehensive self-directed approach to TRA. It differs from traditional TRAs in that it first determines which information assets really need to be protected and then evaluates the technology infrastructure to determine the vulnerability of those assets.⁹ OCTAVE presents an exciting TRA to ORMs because the SEI is home to the CERT Coordination Center (CERT/CC), a center of respected technology expertise and distributor of CERT alerts and other information relating to managing security vulnerabilities. This pedigree provides ORMs with a TRA that is well researched and thor-

Prioritizing Aspects of Technology Risk Assessment and Mitigation

ough. The robustness of tools, workshops, and publications relating to OCTAVE significantly enhances an effective assessment by the ORM.

Specifically, OCTAVE uses a three-phased approach to identify the technology-risk-management needs of an enterprise:

- Build asset-based threat profiles: Identify important information assets, the threats to those assets, security, and current risk-mitigation strategies.
- Identify infrastructure vulnerabilities: Examine technology infrastructure for vulnerabilities that can be compromised.
- Develop security strategy and plans: Based on the results of the first two phases, develop a strategy based on business priorities to mitigate risks.

NIST

The Information Technology Laboratory (ITL) at the NIST provides technical leadership for the nation's measurement and standards infrastructure. These include developing standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. Through the issuance of the Special Publication 800 series, ITL reports on research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.¹⁰

Like the other organizations mentioned previously, NIST provides a detailed checklist of IT-related risk-mitigation strategies that should be assessed as part of a TRA. This checklist is contained in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems." In addition to its detailed coverage of security issues, the checklist enables the ORM to determine if risk is managed by using five "levels of effectiveness":

- Level 1: Control objectives documented in a security policy
- Level 2: Security controls documented as procedures
- Level 3: Procedures have been implemented
- Level 4: Procedures and security controls are tested and reviewed
- Level 5: Procedures and security controls are fully integrated into a comprehensive program

Figure 1 summarizes perceived strengths and concerns of the above methods.

THE RISK-ASSESSMENT PROCESS

Although the above methods all contain comprehensive checklists to assess technology risk, the process to assess the risk is not fully defined in the methods.¹¹ Two notable exceptions are the NIST and OCTAVE methodologies.

Because its process can be applied more generically to the other methodologies, we've adapted the NIST TRA process to describe a typical TRA approach.

The NIST process for assessing technology risks is provided in NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."¹² The guide distinguishes between risk assessment and risk mitigation. Risk assessment determines the extent of potential threat and the risk associated with an IT system; risk mitigation controls or eliminates the risk.

Specifically, the NIST's TRA approach comprises nine steps. These steps are primarily geared to the IT department, so ORMs should enhance the process to include key users who would address business issues and the use of IT on service delivery. These users would include but are not limited to operations, auditing, controllers, and risk management.

Gathering and Confirming the Understanding

Before performing actual risk-assessment procedures, the ORM should obtain an understanding of the bank's technology and the business environment in which it operates. Steps to accomplish this would include obtaining background on the business, identifying technology assets supported, identifying impact on customer privacy, and confirming applicability of regulatory requirements.

Obtain background on the business. Obviously, the ORM will have access to internal business activity reports. To identify existing challenges and potential risks that the enterprise may be facing, however, the ORM should also review external business-related publications that discuss challenges faced by the enterprise and the industry. This could include reviewing selected publicly available Security and Exchange Commission filings of both the enterprise and its main competitors, analysts' reports on the enterprise and the industry, and annual financial reports and trends.

Identify technology assets supported. This would include reviewing an inventory listing of the enterprise's software and hardware assets. The lack of an existing up-to-date inventory of these assets could be an early indication that significant exposures in managing technology risk currently exist. For example, if an inventory listing does not exist, is incomplete, or is inaccurate, the ORM should immediately question how the technology group can effectively monitor and manage known security vulnerabilities if it does not have an accurate understanding of the software used in the enterprise. Another immediate concern would be how the business continuity plan can accurately address resumption issues if the enterprise does not have an accurate understanding of the technology currently in use.

Identify impact on customer privacy. Ideally, this has already been completed before the TRA. If not completed, a

FIGURE 1

Comparison of Methods for Technology Risk Assessments

METHODOLOGY	STRENGTHS	CONCERNS
ISO Standards	<p>Very detailed guidance 10 focus areas Standard of standards Common language Well known</p>	<p>Overkill for most banks Few “free” tools to leverage Strict copyright policy Last updated in 2000</p>
COBIT	<p>Well respected and recognized tool- even by regulators</p> <p>Excellent methodology for getting various parts of an organization to speak the same language</p> <p>Looks at IT in general- not just security</p> <p>Facilitates communication with top-level executives</p> <p>Excellent senior management perspective (<i>e.g., key performance indicators, critical success factors</i>)</p>	<p>Current supporters are primarily in the IT audit community</p> <p>More of a general assessment tool- detailed issues to consider are in the form of audit programs</p> <p>Some practitioners consider it to be too burdensome or theoretical- yet, it has received the support of many organizations</p>
SysTrust	<p>Good high-level questions that provide an overview on overall reliability</p> <p>One of the four areas focuses on security</p> <p>Facilitates communication with non-IT department</p> <p>Provides opportunity for recognized independent third-party audit opinion (<i>e.g., CPA opinion</i>)</p>	<p>Relatively new</p> <p>May not be detailed enough for intended objectives</p> <p>More of an “executive-level” assessment perspective rather than “fix-it” – although intended to provide third-party assurance using professional standards.</p>
OCTAVE	<p>Comprehensive methodology</p> <p>Leverages combination of academic research and industry practices</p> <p>Superior pedigree and project sponsors</p> <p>Full methodology and supporting tools</p>	<p>Currently geared to larger institutions (although a version for smaller organizations is planned)</p> <p>Formal training in the use of the tool required by most users</p> <p>“Cooperative” approach may be too cumbersome for some organizations</p>
NIST	<p>Very detailed guidance Leveraged by other methodology organizations and professional associations “Thought Leadership”</p> <p>Most recently issued guidance on security risk assessment (Fall 2001/current)</p> <p>Facilitates distribution of instructions and development of policies</p> <p>Used internally by regulatory agencies</p>	<p>Geared for the security of government agencies</p> <p>“Blind” following of the methodologies could be too burdensome in a smaller organization</p> <p>Could be considered “excessive” for those primarily concerned about satisfying external reviewer needs only</p>

Prioritizing Aspects of Technology Risk Assessment and Mitigation

preliminary analysis of the impact of customer confidentiality on technology resources should be performed and reviewed with appropriate departments, including compliance.

Confirm applicability of regulatory requirements. There are numerous regulatory guidelines and publications that affect technology. The ORM should confirm his or her understanding of these and determine which apply to the project. The FDIC has compiled a matrix of technology publications issued by the various regulatory agencies that can facilitate ORM effort.¹³ The ORM should confirm with the compliance officer any publications that were deemed not applicable to the enterprise.

Identifying and Defining Threats

The purpose of this step is to gain an understanding of what threats the bank is trying to protect against. Common threat sources include natural threats, human threats (intentional or deliberate actions), and environmental threats. These threats are similar to those typically addressed in many business continuity plans. The ORM may wish to and should leverage these plans appropriately to jump-start the identification.

Another good source on threats that face the enterprise is the SEI at Carnegie Mellon University. Through the CERT/CC, the ORM can obtain an overview of recent popular attack trends against businesses.¹⁴ Another SEI resource, "OCTAVE Threat Profiles,"¹⁵ provides excellent guidance for ORMs in walking through various threat situations that should be considered as part of the TRA.

Developing a Vulnerability Inventory

As discussed above, there are numerous TRA methods that can be used to create a technical vulnerability inventory. For

example, using the NIST methodology, the ORM (or designee) would work together with the chief information officer (CIO) (or designee) to self-assess the enterprise's current strategies to address the risk. Resulting from these conversations would be a conclusion as to whether the risk is mitigated or not.

To supplement the self-assessment, ORMs may seek to coordinate either vulnerability or penetration testing with the technology department. Due to the lack of professional standards that adequately define vulnerability and penetration testing, much confusion exists in the market as to what each is. The NIST, in its Special Publication 800-42, "Draft Guidelines on Network Security Testing,"¹⁶ does provide some generally acceptable guidelines as to what each of these testing procedures encompasses. In a vulnerability test, the ORM (or designee) would identify vulnerabilities using an automated tool instead of relying on human detection or interpretation of scanning results to identify known technical vulnerabilities (Figure 2). In a penetration test, the ORM (or designee) would perform a security test in which evaluators attempt to circumvent the security of a system based on their understanding of the system design and implementation by using common tools and techniques used by hackers (Figure 3).

Translating Technical Vulnerabilities into Business Vulnerabilities

After identifying technical vulnerabilities, the ORM needs to translate these vulnerabilities into business vulnerabilities. One way is to show how the technical vulnerabilities can be exploited by the threats previously identified. The problem with this method is that technology still remains the focus of the discussion.

FIGURE 2

Vulnerability Testing¹

Actions	Typical Recommendations
<ul style="list-style-type: none"> • Identify active hosts on a network • Identify active & vulnerable ports on hosts • Identify application and banner grabbing • Identify operating systems • Identify vulnerabilities associated with discovered operating systems and applications • Testing compliance with host application usage/security policies • Establishing a foundation for penetration testing 	<ul style="list-style-type: none"> • Upgrade or patch vulnerable systems • Deploy mitigating strategies • Tighten configuration management program • Monitor vulnerability alerts and mailing lists and determine applicability to environment • Modify security policies for updates and upgrades

1. See NIST Special Publication 800-42, Draft GuideLine on Security Testing, section 3.2 for further details

Another alternative is to leverage the management guidelines that are available as part of the COBIT methodology (even if the ORM did not choose to use this method, the management guidelines could still be leveraged to effectively communicate business effects). What makes these guidelines unique is that they translate technical issues into terminology with which executive management is familiar. For each of the 34 high-level control objectives presented, the following are provided in the Management Guideline:¹⁷

- The business goal (the why of the control);
- Critical success factors (what needs to occur, in business terms, to effectively mitigate the risk);
- Key goal indicators (how to determine if the business goal was achieved);
- Key performance indicators (factors to measure progress against goals);
- Maturity model level (adapted from SEI's maturity model concept) enables the ORM to determine the maturity level over the risk management of the particular high-level control objective.

Probability and Exposure

Based on traditional risk-management techniques, the ORM assigns a probability (chance of the vulnerability being exploited) and the exposure (materiality of the exploitation). Some ORMs assign a grade from 1 through 10, while others assign a high, medium, or low value. No matter the assignment, it is important that the ORM define and document in writing on what basis a particular value is assigned to ensure an objective evaluation of the vulnerabilities.

Ranking

Based on the scores, the ORM ranks the vulnerability to prioritize remediation and risk mitigation. In unusual situations, the ORM may desire to override the calculated score and thus the prioritization. The rationale for doing so should be appropriately documented.

Recommendations

The ORM develops strategies to manage the risk based on the rankings. These strategies could include accepting the risk (do nothing), transfer the risk (buy insurance), or actively manage the risk.

COMMON VULNERABILITIES

Despite their differences in customers, style, and management, many community banks share the following vulnerabilities.

Board Involvement with Technology

Recent regulatory expectations communicated as part of the privacy guidelines as well as Section 501(b) procedures require greater attention to technology, especially in information security areas. Expectations in this area are sure to increase given the recent concerns with corporate governance.

Both the Institute of Internal Auditors and the IT Governance Institute have released recommendations concerning questions that boards should be asking senior management.

FIGURE 3

Penetration Testing²

Actions	Typical Recommendations
<ul style="list-style-type: none"> • Determine specific IP address/ranges to be tested • Ascertain which hosts and vendors to subject to testing • Determine acceptable testing techniques and tools • Determine time that scanning is to be conducted • Confirm IP address of attack machine • Manage risk of false alarms to law enforcement • Specify handling procedures of information collected by the testing team 	<ul style="list-style-type: none"> • Similar to vulnerability testing – but – emphasis is on showing technical vulnerabilities exploited that enabled access rather than just listing the vulnerabilities • Depending on scope, could emphasize social engineering exploits that focus on human vulnerabilities rather than technical exploits

2. *Id.*, § 3,3

Prioritizing Aspects of Technology Risk Assessment and Mitigation

The latter has also developed management guidelines to assess overall corporate IT governance in line with the COBIT methodology.

Policies, Procedures, and Guidelines

Many banks have these to some extent. If they exist, they frequently are too generic to accomplish the desired objectives. These tools should be used to communicate specifically what is expected to be done and within what boundaries. Current policies in many banks have been developed to satisfy the minimum requirements set by the regulators rather than achieve business objectives.

Clear goals and requirements by function should be developed and distributed. Performance appraisals and control systems should monitor adherence. If exceptions are needed, appropriate risk-management personnel should approve them so that they can appropriately adjust strategies.

Security Hardening Guidelines

Vendors deliver systems so that they can be easy to use and install. As a result, many systems are delivered as open as possible to achieve this goal, sacrificing security. The purpose of security hardening is to tighten the system and to configure system parameters to enforce bank policy.

Vulnerability testing (as described above) is one method used to identify hardening opportunities. Vendor documentation, specialty security (for example, www.cisecurity.org), and auditing Web sites can be consulted to obtain more information on hardening guidelines.

Vendor Management Programs

Many banks are rushing to implement vendor management programs as the result of regulatory reviews. Surprisingly, few banks know how to manage their vendors effectively, resulting in overpayments or services paid for but not used.

All the methods described above provide elements of how to manage vendors. The ISO Standards, in particular, provide strong guidelines for contract language and communi-

cating issues to be measured and monitored.

Electronic Communications

These include email, voice mail, and private branch exchanges. As with other forms of technologies, appropriate policies on use should be developed and compliance with these policies monitored. Electronic communication equipment should be hardened in order to minimize security threats.

CONCLUSION

With so much to do and so little time or resources, the ORM needs to prioritize what gets done. As with many business situations, the 80/20 rule applies. By focusing on and assigning resources to high-priority risks and exposures, ORMs can cost-effectively mitigate risk to an acceptable level for their enterprise.

NOTES

1. Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk," July 2002, p.8.
2. See OCC 2001-35, Attachment A.
3. As visited on www.aba.com on October 4, 2002.
4. For further details on the ISO Standards, refer to ISO/IEC 17799:2000, available at www.iso.ch.
5. However, it is not recognized as a generally accepted auditing standard for purposes of independent CPA opinions.
6. For further details on the COBIT standard and adapters of the standard, refer to www.isaca.org.
7. SysTrust, AICPA/CICA SysTrust Principles and Criteria for Systems Reliability, Version 2.0, January 2001.
8. Exposure Draft AICPA/CICA Trust Services Principles and Criteria, Version 1.0.
9. For further details on the OCTAVE approach, refer to www.cert.org/octave.
10. For further details on NIST security initiatives, refer to csrc.nist.gov.
11. Although each methodology includes some guidance, the guidance for performing the assessment is not as comprehensive as those from the NIST and OCTAVE.
12. See csrc.nist.gov for full details on the NIST's risk-assessment approach.
13. See www.fdic.gov.
14. See www.cert.org/archive/pdf/attack-trends.pdf.
15. See www.cert.org/archive/pdf/octave-threat-profiles.pdf.
16. See csrc.nist.gov/publications/drafts/security-testing.pdf.
17. Management Guidelines, COBIT 3d Edition, IT Governance Institute, July 2000. Refer to page 70 for applying the guidelines for ensuring systems security.