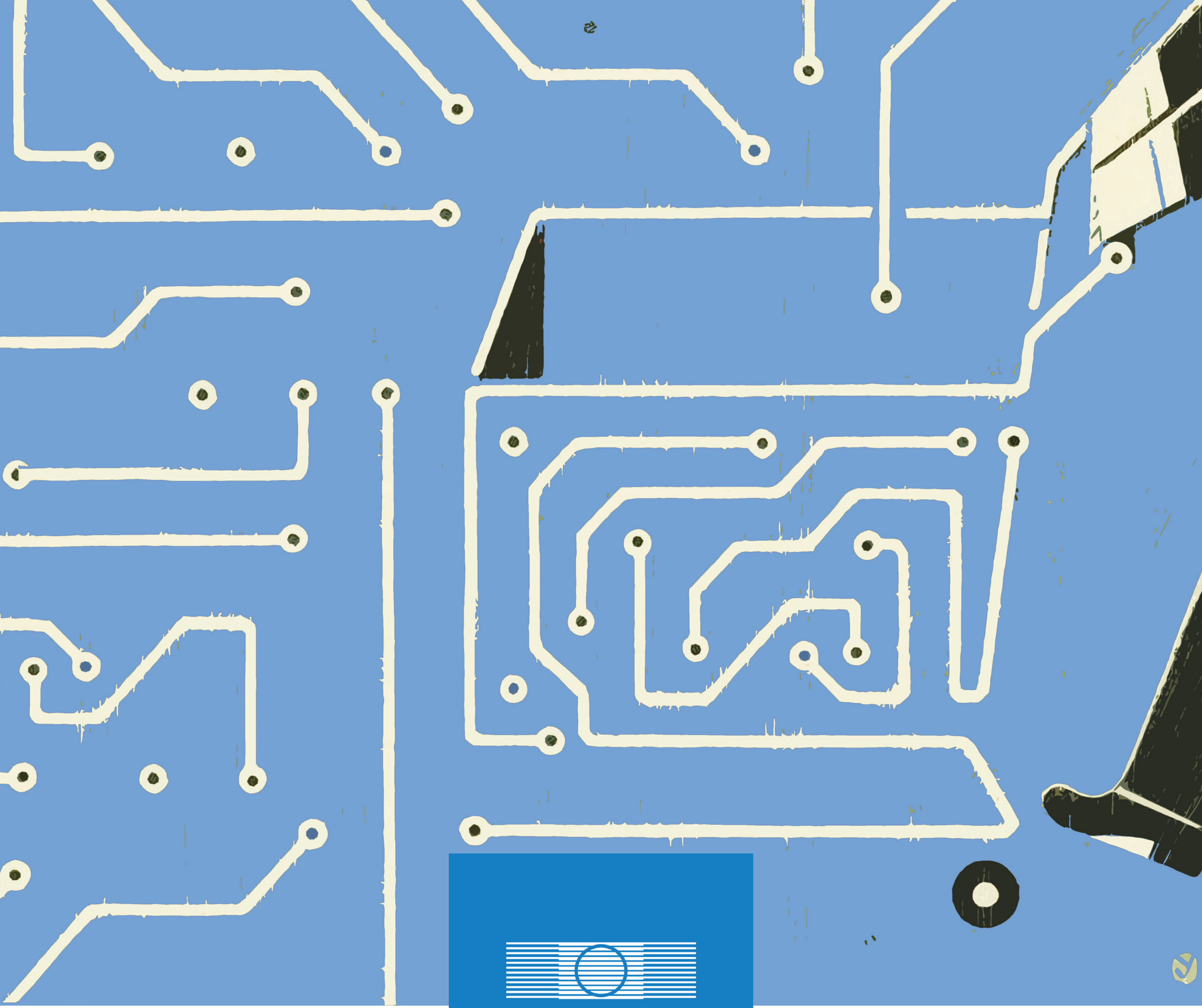


EastWest
INSTITUTE

Purchasing Secure ICT Products and Services: A Buyers Guide

The views expressed in this publication do not necessarily reflect the position of the EastWest Institute, its Board of Directors or staff.

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow, Washington, D.C and San Francisco.

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
+1-212-824-4100

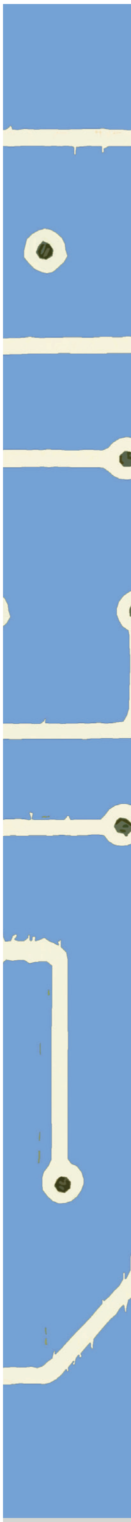
communications@eastwest.ngo
www.eastwest.ngo

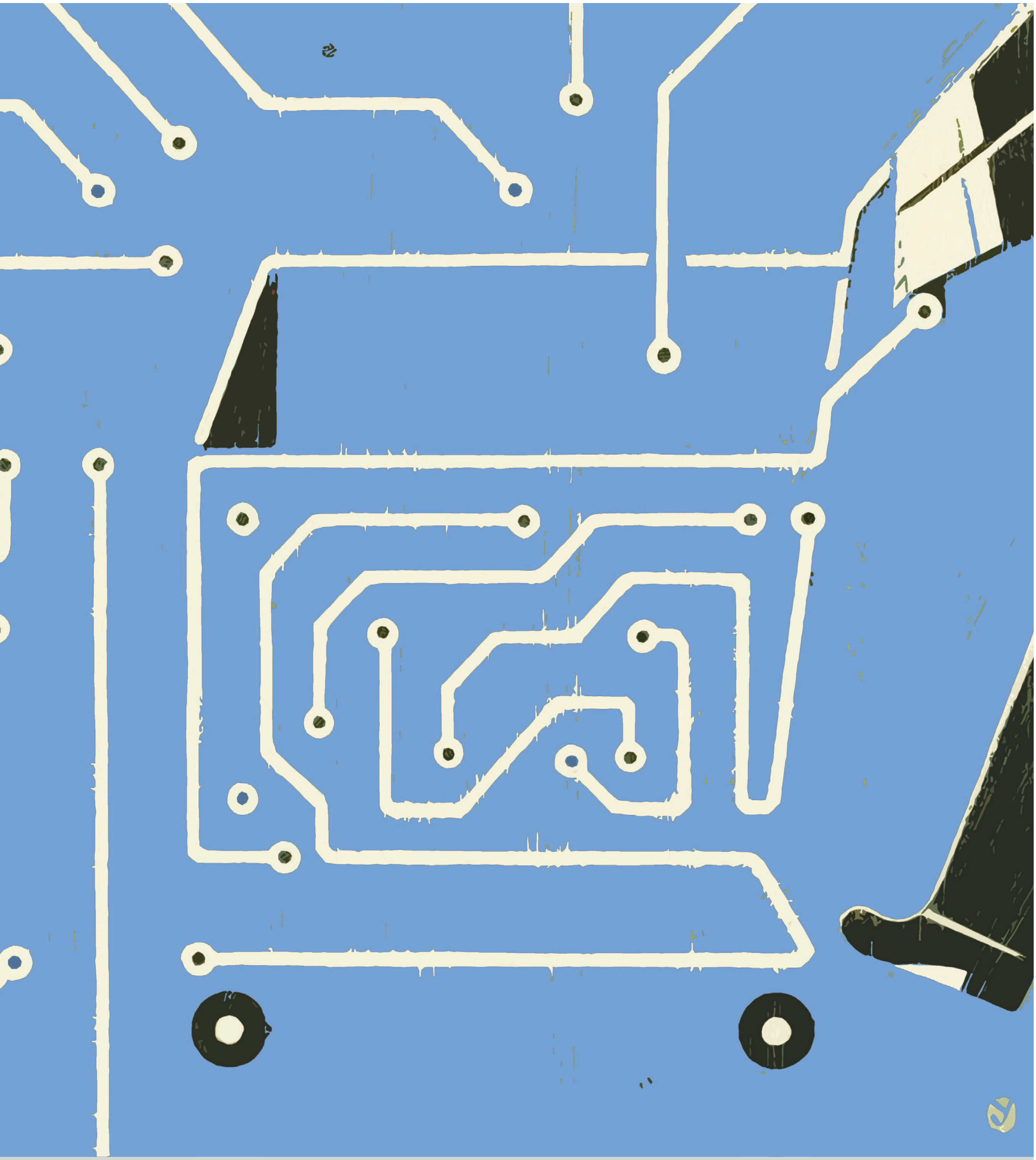
ICT Buyers Security Guide

Summary

This Buyers Guide is intended to help the buyers, suppliers, and users of information and communications technologies better understand and address the cybersecurity and privacy risks inherent in information and communications technology (ICT) products and services. These individuals include senior executives and members of their governing boards and parent organizations, chief information and information security officers, risk management professionals, acquisition officers, insurers, auditors, other third-party risk evaluators, and design, manufacturing and supply chain professionals. The Guide provides these three overarching recommendations for ICT buyers and suppliers:

1. Engage in a dialogue about risk management.
2. Use questions in this Guide to frame the dialogue (see Figure 3 on page 22).
3. Rely on international standards to increase confidence in the results.





Why This Guide is Needed

Governments and enterprises around the globe depend on information and communications technology (ICT) products and services. They depend on ICT for national and economic security, public safety and law enforcement, and the confidentiality of their data and the data of the individuals they serve. These users of ICT are also increasingly aware of and concerned about cybersecurity risks.

In the last 18 to 24 months, security professionals, executives, and boards of directors have engaged and invested more in efforts to enhance cybersecurity. For example, in Pricewaterhouse Cooper's *The Global State of Information Security® Survey 2016*, respondents reported that 45 percent of boards participate in the development of an overall security strategy, and cybersecurity budgets increased by 24 percent in 2015.[1]

Such attention is overdue. Widespread news reports of increasingly severe cyber attacks from criminal and other malicious actors reveal only the tip of the iceberg. According to Lloyds of London, an insurance company, cyber crimes alone cost global businesses $400 billion per year, representing tens of thousands of corporate victims.[2] And, such direct economic losses do not include loss of customer confidence, reduced share prices, increased insurance premiums, and diverted management attention. The increased focus on and investment in cybersecurity is significant and meaningful; yet it is still insufficient. Executive engagement and investment are developing, but many efforts are limited to managing operational risks to enterprise ICT systems and data. Executives are not yet considering the impact of their purchasing decisions on the security or integrity of the technologies the organization uses. More specifically, many ICT buyers are not yet having conversations with their suppliers about how those suppliers govern and manage risk in their environments, develop technology products and services, manage security of those over time, and demonstrate their practices in these areas.

Technological innovation and development leverage global resources—cyber, physical, and human. This global approach drives down costs and enables people and organizations around the world to use and realize the benefits of ICT products and services. However, it also introduces risks because of the number and diversity of individuals, entities, services, and

[1] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[2] http://www.cyberinsurance.co.uk/cyber-news/lloyds-ceo-cyber-crime-cost-businesses-up-to-400-billion-a-year/.

components, and the complexity of the products and services themselves. In particular, ICT products and services often contain vulnerable components, which increase cyber risk exposure and often add direct and indirect costs across the lifecycle of products and services. The burgeoning deployment of cost-effective cloud services which often rely on multinational hosting and maintenance, decreases the transparency of risk and contributes to the importance of addressing these issues.

Through their purchasing priorities and decisions, ICT buyers have at least two crucial roles to play in cybersecurity:

- First, buyers can reduce risk by procuring and using products and services that have sufficient security and integrity for their environments.
- Second, by factoring security into procurement decisions, buyers incentivize ICT suppliers to develop and provide more secure ICT.

Buyers wanting more secure ICT products and services should develop or leverage informed security requirements and use them in procurements. Those requirements should take the form of risk-informed, fact-based procurement practices based on widely recognized international standards and best practices. They should be enforced by objective conformance regimes that are flexible and consistent with risk. By asking informed questions and imposing commercially reasonable requirements on ICT providers, buyers can significantly reduce the risk of a range of cyber threats and, by doing so, reduce overall risk in cyberspace.

When practicable, buyers should also collaborate with like-minded buyers to leverage their collective purchasing power and signal their collective requirements to the market.

Approach: Principles, Surveys, Interviews

The EastWest Institute's (EWI) Breakthrough Group on Increasing the Global Availability and Use of Secure ICT Products and Services[3] has created this Guide. In 2015, the breakthrough group developed a set of five principles for market participants demarked simply as government and industry. Government and industry act in multiple roles as stakeholders in the ICT marketplace. The government acts as a policymaker and sometimes as a regulator of ICT, industry develops and provides ICT products and services, and both government and industry are buyers of ICT products and services. Accordingly, cyber stakeholders have varying responsibilities and capabilities to effect an increase in the security of ICT products and services, and in the use of more secure ICT. These roles and responsibilities are summarized in Figure 1.

The group also conducted an industry survey, which produced insights into how both buyers and suppliers think about the security of ICT products and services.[4] In addition, it conducted confidential interviews with senior security and risk management experts in key sectors—finance, transportation, telecommunications, retail and government—to learn how they evaluate suppliers and make sourcing decisions around the security of ICT products and services.

This Guide is version 1.0. EWI will revise this Guide in early 2017 prior to our Global Cyberspace Cooperation Summit (to be held March 14-16, 2017, at the University of California, Berkeley). We welcome your comments and feedback. Please feel free to use the Feedback Form in Appendix C, or send your observations and suggestions to cyber@eastwest.ngo. Comments received by December 1, 2016 will be reflected in version 2.0.

[3] See, https://www.eastwest.ngo/info/increasing-global-availability-and-use-secure-ict-products-and-services. EWI appreciates the leadership and support of its partners in creating this Guide, and in particular the dedication and perseverance of Sally Long of The Open Group, Angela McKay of Microsoft and Andy Purdy of Huawei Technologies USA.

[4] A description of the survey results can be found at https://www.eastwest.ngo/sites/default/files/words-images/Survey-Results-Summit-2015.pdf.

Figure 1: Roles and Responsibilities of Cyber Stakeholders

Actor **>**	Government		Industry
Role **>**	Policymaker	ICT Buyer*	ICT Provider
The Five Principles			
Maintain an **open market** that fosters innovation and competition and creates a **level playing field** for ICT providers	●		
Create procurement practices that utilize **fact-driven, risk-informed, and transparent requirements** based on international standards and approaches		●	
Avoid requirements or behavior that **undermine trust** in ICT (e.g., by installing back doors)	●		●
Evaluate the practices of ICT providers in terms of creating product and service integrity		●	
Create and use tools and approaches to **address risk** and **assign high value** to cybersecurity investments	●	●	●

*Government and industry organizations both act as buyers of ICT products and services.

How to Use This Guide

This Buyers Guide is intended to help facilitate and structure informed conversations between ICT buyers and suppliers about how suppliers manage cybersecurity risk in their offerings. While this Guide may help raise awareness of the importance of cybersecurity generally, it is specifically designed to help organizations reduce the risk they face from cybersecurity vulnerabilities[5] in the commercial products and services upon which they rely. Accordingly, it provides guidance and practices intended to assist buyers in developing and implementing security-minded purchasing requirements to reduce risks from product and service vulnerabilities. Buyers can use the mechanisms described to assure that their suppliers manage cybersecurity risk in their offerings appropriately.

This document is not a checklist. Dialogue and exchange between buyers and suppliers can be more valuable for both parties, providing greater insight into the concerns of buyers and the practices of suppliers, and because buyers can and should have different risk priorities.

Differences in risk priorities exist both between organizations and within a single organization based on different threats, risk tolerances, and management resources. For example, protecting the confidentiality of data will be paramount in some business areas; in others, the need for availability will dominate.

The recommendations in this Guide are meant to complement an organization's existing enterprise cybersecurity risk management practices, which often tend to focus on managing operational cybersecurity risks by using tools such as network security, data loss prevention, user training, exercising resilience, etc., and by transferring risk to others via insurance or other means. Organizations must manage ICT supplier risk, like other risks, with a level of effort appropriate to the risk. Although the practices recommended here could extend the time to complete procurements and may increase purchasing costs, these tradeoffs must be evaluated against the security risks resulting from not adopting the practices. Sound metrics for evaluating investments in cybersecurity remain a work in progress.

This Guide may be used in various ways by different organizations. Small and medium sized enterprises, and smaller business units responsible for their own ICT procurements within

[5] A cybersecurity vulnerability is a weakness in a product or service that could allow an attacker to compromise the integrity, availability, or confidentiality of that product or service, or of the information that it stores, processes, or provides.

larger companies, may choose to use the Guide more as an internal awareness tool than as a template for discussions with large commercial product and service suppliers. The nature of the buyer-supplier relationship will also affect the dialogue. Conversations between buyers and long-term suppliers will often focus on changes, whether those are changes in threats facing the buyer or changes in suppliers' processes and practices. Conversations with new, potential suppliers will often be more comprehensive as buyers seek to understand more broadly how those suppliers approach risk management in their organizations and across the product and service lifecycle.

Finally, while this Guide recognizes the value of international process-based standards and certifications to help assure conformance to those processes, it does not emphasize product or service certification, which may be appropriate for some technologies but can be slow and costly. Product certification may not adequately consider processes to promote version integrity and authenticity more consistently throughout the technology development and manufacturing/production lifecycle and supply chain. Traditional product certification approaches are challenged to accurately reflect security and integrity for constantly evolving software code and approaches to manage operational security, particularly in the cloud services environment.

This Guide is divided into three main sections: **Enterprise Security Governance**, **Product and Service Lifecycle—from Design through Sustainment and Response**, and **Creating Assurance**. Each section includes a brief introduction of the topic and a series of subsections (e.g., Sourcing/Supply Chain) that highlight common sources of risk and associated processes and practices to mitigate them. Each section suggests one or more questions that buyers can ask suppliers as a way of opening or advancing the buyer-supplier conversation and improving buyer understanding and confidence. In some cases, the Guide suggests artifacts the supplier could provide that will document the measures taken. Finally, the document contains three appendices: a feedback form, a list of relevant international standards, and the "Top 100" requirements.[6]

[6] The questions in this Guide were adapted and combined from the eleven categories of 100 questions contained in the Top 100 Requirements white paper developed by Huawei Technologies Co., Ltd. (see Appendix B). EWI agreed to launch a process to gather input from government and industry experts and evolve those 100 questions to the next level of practicality and usability. This Guide represents the first detailed product of that process.

1. Enterprise Security Governance

This section of the document provides guidance to help buyers determine the extent to which their suppliers have the necessary strategy and governance processes in place to manage cybersecurity in their environments. Suppliers should have an organization-wide governance framework to consistently manage cyber risks, including risks associated with product and service integrity and supply chain security. The leadership of the supplier organization owns all such risk and should ensure that the most appropriate processes and practices are in place and continuously improved. There must be effective oversight and verification mechanisms to give the leadership adequate and timely visibility into the management of the risk.

Strategy and Control

Organizational leaders recognize that a part of their fiduciary responsibility is to address risk that could negatively impact their organization's core mission, operation and reputation. As noted, there is growing awareness among corporate boards of directors, executives, and senior managers that such risks can have a cybersecurity causal connection and that cybersecurity risk—like other risk—is owned by the board of directors. In other words, cybersecurity risk must be part of an organization's enterprise-wide risk management program. Accordingly, the board and CEO must have ongoing visibility into and exercise their ownership and responsibility for cybersecurity risk management.

Once cognizant of this responsibility, the organization should make a firm commitment to address cybersecurity risk and should create an organization-wide committee or other entity to address this risk (or, alternatively, incorporate cybersecurity risk management into an existing entity that addresses risk generally). Because the key stakeholders of the organization—including business/mission groups, key departments, IT, HR, legal, and security—are relevant to one or more components of cybersecurity risk (threat, vulnerability, and consequence), senior representatives from each should be part of the high-level committee that evaluates and oversees risk management and provides ongoing visibility to the board and C-level executives (regular reporting, quarterly or semi-annually, and more often when necessary).

Under the oversight of this entity, internal requirements (corporate policies, standards, and procedures) for cybersecurity should be developed for all key functions, including those specific to delivery of products or services (e.g., research and development, manufacturing, service delivery) and those that support and ensure organizations are fulfilling their legal and fiduciary responsibilities (e.g., human resources, laws and regulations, standards, compliance, auditing).

These requirements should be built not only into the performance metrics and milestones of the relevant business group or department, but also into the performance standards of individual employees who have responsibility for the particular initiative or actions. Mechanisms such as internal evaluation and audits should be used to track and monitor cybersecurity-related functions and activities managed by the organization or performed by third-party suppliers. Such mechanisms enable groups and individuals that have cybersecurity responsibilities to be held accountable. Organization-wide oversight committees can then have visibility into how effectively cybersecurity risk is managed and provide timely, meaningful visibility to the board.

Questions Related to Strategy and Control:

- How does the supplier integrate and manage information and cybersecurity risk into the core strategic and operational focus of the business?
- To what extent can the scheduled release of products or services to customers be delayed in order to address unexpected security concerns?

Standards and Processes

Achieving consistent quality in products and services requires that employees and their organization's suppliers follow processes and practices that are consistent, repeatable, and scalable. Training and tools to support these processes, practices, and personnel are also required. The same holds true for an organization seeking to manage cybersecurity risk effectively. For both quality and cybersecurity, the processes and practices that have proven most effective are usually based on commonly recognized international standards and best practices.

The set of appropriate standards and related processes and practices that should be followed is one important component of the set of requirements the organization will communicate internally (i.e., to its managers, employees, and contractors) and externally (i.e., to vendors and suppliers). One best practice gaining increasing support is the Cybersecurity Framework, which was developed by the National Institute of Standards and Technology (NIST) in collaboration with industry stakeholders.[7] The Cybersecurity Framework relies on international standards to support a risk-analytic tool that describes operational risk analysis and management processes and practices—an essential foundation for an organization to assess and systematically address cybersecurity risk as part of enterprise risk management. ICT buyers should consider the practices outlined in the Cybersecurity Framework not only to enhance their own operational cybersecurity, but also to evaluate that of their suppliers.

Other factors that impact requirements and should be considered by the internal oversight entity include national statutes or regional regulation (such as in the European Union), as well as the needs of particular customers or industry sectors. In addition, each organization needs to keep abreast of the changing cyber threat landscape and advances in industry practices, while constantly assessing the implications of increasing requirements, including costs and potential impacts to innovation.

Questions Related to Standards and Processes:

- What commonly accepted international standards and best practices support supplier security processes and practices? Where gaps exist, how are they being addressed?

[7] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Human Resources

The human capital of an organization is one of its most important assets and should be managed as such, both in terms of the value employees create as well as how they contribute to increasing, managing, and reducing risk. The best organizations seek to instill, maintain, and regularly refresh a culture that supports the ability of employees to contribute to the organization's goals. Accordingly, they should recruit, hire, train, and motivate their employees to understand goals and requirements—including cybersecurity risk management.

This human resources goal should apply at all levels of the organization, from line employees to the most senior executives. Every employee should have some level of cybersecurity awareness (customized for the specific requirements of the employee's role) that is refreshed on a regular basis and tested periodically. Regular training should include legal and internal policy compliance and sharing examples of non-compliance. All employees need to be aware of what conduct is permissible, discouraged, or forbidden, and experience a culture in which employees are encouraged to report violations and are held accountable for complying with policies.

Organizations may also consider conducting random compliance evaluations; for example, they may send test phishing emails and test social engineering attacks, conduct anonymous surveys of employees, and publicize the responsibility of employees to report improper conduct. Employees should know that the organization cares about policy compliance and is making real efforts to ensure it across all levels of the organization.

Question Related to Human Resources:

- How are key personnel vetted, selected, trained, and held accountable for trustworthiness?

2. The Product and Service Lifecycle – from Design through Sustainment and Response

The global threat landscape continues to change dramatically, and cyber attacks are growing in sophistication and prominence. Malicious attackers rapidly adapt and change strategies, including creating or exploiting vulnerabilities in global technology development and manufacturing supply chains.

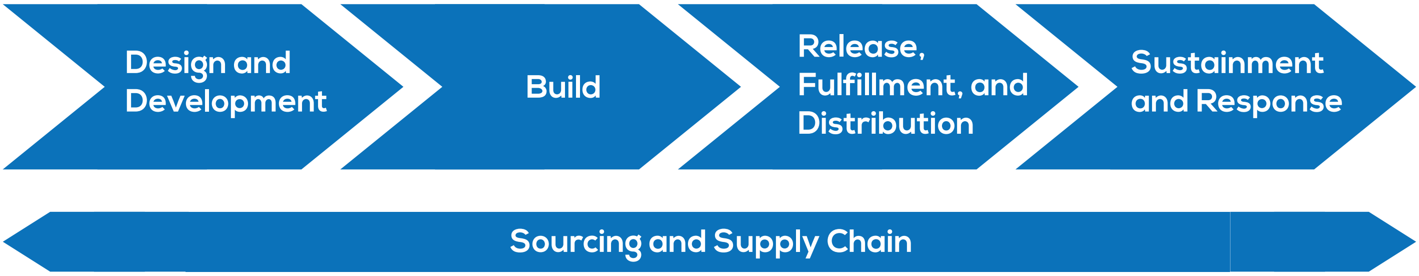
In this evolving threat landscape, suppliers must focus on securing products and services throughout their lifecycle. More specifically, every technology provider in the supply chain—including developers of software code, component suppliers, manufacturers, distributors and value-add resellers—must do its part to mitigate risks along the supply chain. Processes, practices, training, and tooling should address a variety of potential risks and include efforts that: reduce the number and severity of vulnerabilities during the development of software code, reduce the risk of maliciously tainted code, and mitigate against counterfeit components making their way into a finished product or service.

This section provides guidance to help buyers determine whether their current and potential suppliers are managing cybersecurity and supply chain risk appropriately throughout the lifecycle of products and services. The product and service lifecycle is described slightly differently in almost all organizations, but most use one of two approaches. One approach makes a distinction between what is developed by providers "in-house" and what is outsourced and then brought back into the product (e.g., hardware components, open source, other third-party software); the other approach describes the full lifecycle using a series of functions involved in the development and delivery of products and services. In the latter approach, each function is considered to be part of the supply chain because in the current global ICT marketplace, activities or functions could be—and frequently are—outsourced to third-party suppliers.

In this document, the product and service lifecycle has been partitioned according to functions, as shown in Figure 2.[8] For each of the functions, the document highlights broad categories that buyers and providers should be concerned about from a cybersecurity and supply chain security perspective. The document also offers a brief overview of the best practices within those categories, promoting buyer awareness of the supplier practices that most effectively help an organization manage security and integrity across the product or service lifecycle.

[8] The simple representation of the product and service lifecycle provided here does not conflict with the modern spiral development lifecycle (SDLC) for software. (See, e.g., Barry Boehm, 1986, "A Spiral Model of Software Development and Enhancement"). In reality, feedback loops exist in all mature manufacturing and distribution processes.

Figure 2: The ICT Product and Service Lifecycle


Design and Development
Build
Release, Fulfillment, and Distribution
Sustainment and Response
Sourcing and Supply Chain

Product and Service Lifecycle Best Practices

A. Design and Development

Within design and development, buyers and their suppliers should be concerned with two core categories of efforts: how suppliers manage software development, and the extent to which they are using secure engineering practices.

1. Software Development Practices
Suppliers should have core processes and practices in place for all products and services to create and manage basic quality and security for the development, operation, and maintenance of software. These practices should be followed, irrespective of any additional secure engineering, supply chain risk management, and/or manufacturing methodologies that may be utilized to increase security and integrity. Practices in this category should address such basics as: design; development policies and processes; quality and test management; configuration and vulnerability management (recall, not all vulnerabilities are security vulnerabilities); and product maintenance and disposal.

2. Secure Engineering Practices
Suppliers should follow practices designed specifically to reduce the number and severity of unintentional vulnerabilities in the products, services, or components they are developing. This covers activities like: threat modeling, analysis, and mitigation; secure coding practices; run-time protection techniques; security vulnerability analysis, response, and remediation (i.e., patching); and continuous improvement (i.e., monitoring and assessing changes in the threat landscape and successful attacks and, as appropriate, evolving engineering practices).

Questions Related to Design and Development:

- How does the supplier manage its software development processes, and are those based on industry standards or best practices? If yes, which?
- Does the supplier have a lifecycle strategy that ensures that products and services are conceptualized (i.e., during R&D), designed, developed, and maintained from a security perspective over their lifecycle? Are cybersecurity requirements embedded throughout, and are they based on any industry standard or best practice?
- Are secure coding practices in place throughout the lifecycle?
- How does the supplier identify and trace vulnerabilities (security and non-security) and ensure that they are appropriately prioritized based on risk and addressed in every product and service that might use the vulnerable code/component?
- How does the supplier monitor changes in the threat landscape and take them into account in the design, development, and deployment phases?

B. Build

This category includes converting source code files into software that can be run on a computer, as well as the manufacture, assembly, and integration of various software and hardware components into finished products and services. Throughout build, mitigating the risk of tainted or counterfeit components being inserted before or during manufacturing and assembly is important. Good product development and secure engineering practices (as discussed above), and supply chain best practices (see below) during the build phase will help prevent product and service compromise from a security or counterfeit perspective. Within those broad practices, code and component quality reviews that managing code or component integration, version control, and compilation and manufacturing are essential.

Questions Related to Build:

- What are the security processes used for compilation and/or manufacturing processes?
- How are products and services continually tested for security vulnerabilities?
- What international standards and best practices does the vendor comply with in terms of compilation and/or manufacturing?

C. Release, Fulfillment, and Distribution

When products and services are finished and ready to be shipped or provided, release practices should again be documented and followed consistently. These steps are essential to assure that all of the channel partners are following best practices in the release cycle, as well as strong security and supply chain practices so that physical and logical access are not compromised during distribution to the customer.

Questions Related to Release, Fulfillment, and Distribution:

- How do suppliers identify and authorize partners to distribute their products and services, and how do they verify partners are meeting their commitments?
- How are security and integrity of products and services maintained until final customer acceptance?
- How does the supplier help the customer integrate products and services into existing infrastructure safely and securely?

D. Sustainment and Response

The activities related to this category help assure that when a product or service has been delivered to the customer, there is an agreement in place that governs product and service maintenance and sustainment. Buyers should understand what their providers will commit to in terms of maintaining the product, including patching for functionality and for security as well as how they will respond to reported incidents and communicating about and correcting vulnerabilities that may be reported or discovered after delivery.

Question Related to Sustainment and Response:

- How do ongoing maintenance, patching, incident resolution, and upgrade procedures maintain and enhance product and service functionality and security?

E. Sourcing and Supply Chain

This category covers the outsourcing of any of the functions described above for hardware and software to third-party developers and manufacturers. Buyers should be concerned about whether suppliers and manufacturers, as well as any distributors or value-added resellers, are trustworthy. Therefore, buyers should try to determine from their suppliers the extent to which their supply chains and their outsourcing partners are similarly carrying out best practices for design and development, build, release, fulfillment, distribution, as well as sustainment and response.

Processes and practices in this category cover the overall supply chain, including: selection and authorization of suppliers and business partner such as original equipment manufacturers (OEM), component suppliers, integrators, value-added resellers and distributors; the protection of the suppliers' environment (e.g., physical and logical access control); and the security and integrity of the manufacturing processes (e.g., practices, training, and tooling for secure transmission and handling, open source, counterfeit mitigation, and malware detection).

Questions Related to Sourcing and Supply Chain:

- Are third-party inputs evaluated for security prior to selection and tracked/validated upon entering the supply chain?
- How does the supplier conduct security management with its suppliers? Has the vendor established relevant security criteria and passed the criteria onto its suppliers?
- How does the supplier describe its manufacturing process flow and provide details on how it assesses the process, both upstream and downstream, to discover the existence of any tainted or counterfeit components?

3. Creating Assurance

The previous two sections of this Guide describe considerations and questions to help ICT buyers assess if and how their suppliers govern and manage cyber risks generally, as well as throughout the lifecycle of their products and services, enabling buyers to make more informed decisions based on risk tolerance. Supplier statements that describe governance and product or service development policies are useful, but they may not be sufficient in all cases. Buyers may also request, and in some cases require, ICT suppliers to demonstrate assurance by disclosing information and showing evidence that they are adhering to the commitments that they describe. With assurance, buyers gain trust in suppliers' implementations of risk mitigations.

This section provides guidance to help buyers understand the various approaches that can be used to foster greater assurance. It also covers the different approaches suppliers can use to demonstrate that their processes and practices provide greater assurance.

Both fostering and demonstrating assurance help to build and continually enhance trust among ICT buyers and suppliers:

- Approaches to foster assurance, including laws and regulations, contracts, and transparency, increase the likelihood that: buyers will either require or request greater security and integrity in their ICT products and services; and, suppliers will increasingly use processes and practices to enhance those areas. Fostering assurance helps incentivize and encourage a market for more secure ICT products and services.

- Methods of demonstrating assurance, including external attestation (often via certification) and self-attestation, are means by which concrete evidence or other information is shared to show how various standards, processes, or practices are being used by suppliers. Sharing such information helps to advance trust. Buyers and suppliers should consider multiple approaches, flexibly based on risk, to request or require information that can help demonstrate assurance. These approaches can contribute to efforts to establish, maintain, and increase trust, but they may also have associated costs, including delaying the adoption of more secure products and services or unduly stifling innovation.

Fostering Assurance

How does the ecosystem advance ideas about the need for and value of assurance? Along a spectrum of conduct from less to more voluntary, there are multiple approaches that governments, suppliers, and buyers can undertake to foster assurance, including through laws and regulations, contracts, independent evaluations or attestations, and transparency.

Laws and regulations: Government policymakers may require public and private sector ICT buyers that operate within their jurisdictions to comply with certain security, privacy, or related requirements or commitments; in turn, those organizations must ensure that their suppliers also comply. In other words, buyers must be confident that the products and services they procure will meet the demands of their governments; as a result, laws and regulations that stipulate such commitments may help to foster assurance.

For example, the European Union requires that organizations operating within its jurisdiction adhere to various privacy commitments, and the European Commission has developed Model Clauses—also known as Standard Contractual Clauses—that are consistent with those commitments. Standard Contract Clauses are used to facilitate the transfer of personal data outside of the EU in a manner that is consistent with the spirit of the requirements of 95/46/EC, the Data Protection Directive. Both the EU requirements and the Model Clauses help to foster assurance by establishing benchmarks against which ICT buyers can evaluate their suppliers, incentivizing suppliers to pursue methods to assure customers that they meet or exceed those benchmarks. Other jurisdictions are developing different approaches, and inconsistency across jurisdictions is increasing costs to buyers because suppliers must build and maintain different products/services for different jurisdictions.

Contracts: ICT buyers and suppliers make mutual commitments through the process of contracting—including security, privacy, quality, or related commitments. In their contracts with suppliers, ICT buyers may, for instance, stipulate that particular risk management standards or guidelines must be followed by their suppliers; examples include the ISO 27000 series (e.g., ISO 27002, ISO 27034, 27036, 27018, 27019), ISO 20243 or the NIST Cybersecurity Framework. (For more information see Appendix A). Contracts are a particularly powerful way to foster assurance because they are flexible, market-based mechanisms that can much more rapidly drive and evolve ecosystem behavior in a changing threat landscape. Using contracts, buyers can articulate specific needs, focus suppliers on areas of concern, and drive suppliers towards approaches that have demonstrated effectiveness.

Transparency: In addition to legal mechanisms like government-developed requirements or contractual commitments, ICT buyers and suppliers can benefit from more voluntary approaches to fostering assurance. In particular, suppliers offering their customers greater transparency into their security processes and practices, and into the products and services themselves, create more opportunities for buyers to understand suppliers' commitments, helping to build trust. Buyers can help by requesting greater transparency from their suppliers regarding the steps suppliers are taking to advance and ensure security. As discussed below, self-attestation is a method of sharing information and evidence to increase transparency.

Questions Related to Fostering Assurance:

- What are the various cybersecurity and privacy laws and requirements in the jurisdictions in which the buyer and/or supplier operate, and how can the buyer and supplier ensure compliance with them?
- What are the appropriate commitments to be included in the contract?
- How does the supplier seek to provide the buyer transparency into its relevant commitments?

- Does the supplier organize security-oriented customer feedback sessions and enable buyers to interact collectively around product and service security concerns?

Demonstrating Assurance

Buyers can determine both what and how suppliers are doing to improve the security of their products and services in several ways, starting with the questions provided in this Guide. They should ask their providers to tell them what they are doing to govern and manage cybersecurity as part of enterprise risk management, and what they are doing to manage security and integrity as part of the product and service lifecycle.

Buyers may ask suppliers if they are following published methodologies or international standards. Suppliers can demonstrate assurance through two different approaches: self-attestation and external attestation. Audits and certification against international standards are forms of external attestation—where such certification programs exist. Either approach can help to contribute to a buyer's confidence in a supplier's adherence to its commitments, but each has tradeoffs.

If suppliers are not yet following any international standards, then buyers may recommend that suppliers begin adopting those they consider to be most relevant and effective, such as those in Appendix A, including obtaining external attestation/certification where relevant programs for those standards exist.

In the meantime, buyers should probe the current state of a provider's practices with a standard set of questions—such as those in Appendix B—and verify their answers to those questions through mechanisms like those described in this section.

Self-attestation involves a process through which a supplier attests and usually provides evidence that it is adhering to its security, privacy, or related requirements or commitments, which may be embedded in standards, best practices, or other positions about which it has made public or private statements. Self-attestation is particularly relevant for those issues or buyer considerations that are not able to be readily assessed by independent third-party assessment organizations (referred to by the U.S. federal government as 3PAOs). If certification is not yet possible or suppliers have not yet achieved that certification status, then buyers should inquire about what international standards suppliers are following. The buyer could then use the mapping reference in Appendix A to help determine the relevance of various standards to the product lifecycle functional areas described earlier in this section.

One example of a best practice that is not yet readily assessed by 3PAOs or other external evaluators is the NIST Cybersecurity Framework, introduced above. Suppliers can demonstrate assurance and build trust with buyers about their operational cybersecurity by providing information about, and evidence of, how they have adhered to the risk management practices embedded within the Cybersecurity Framework. Other good examples include ISO 31000 and ISO 27036, which provide helpful best practices but are not readily assessable by external auditors.

Self-attestation may also be relevant when ICT buyers require a more granular understanding of how a supplier develops its products or services. For example, buyers making long-term procurement commitments may require elevated confidence in a supplier's ability to comply with relevant laws and regulations or contract commitments. Because suppliers that engineer products and services with laws and regulations in mind are more likely to continue to demonstrate compliance in the future, buyers may inquire about how suppliers take laws and regulations into consideration as they develop ICT products and services. Moreover, the way in which suppliers provide such information and show evidence of their commitments and conformance is significant. Disclosures and demonstrations that involve clear, complete, and timely communications enable buyers to make informed decisions about whether to trust and rely on a supplier or what additional assurances might enable them to do so.

In addition to encouraging suppliers to provide clear communication about their cybersecurity processes and commitments to protect their products and services, some buyers may seek to partner with suppliers that disclose more information to inform an ICT buyer's choice and meet its requirements. For instance, suppliers may provide certain buyers with particularly elevated cybersecurity risk concerns the ability to review and/or to test their product or service code, enabling those buyers a unique opportunity to develop and deepen their trust in a supplier. Such suppliers could also offer to dialogue with interested ICT buyers, creating opportunities for buyers to visit their campuses and learn more about their cybersecurity practices. In addition, companies such as Huawei Technologies and Microsoft operate centers in various jurisdictions to enable customers to inspect their products for security purposes. These more rigorous approaches to self-attestation are appropriate for buyers with unique and elevated concerns and are not universally applicable because they have higher costs, and the level of information exchanged would not be consumable or meaningful to most buyers.

External attestation involves a process through which an entity other than the ICT supplier evaluates and potentially attests to or certifies the supplier's adherence to certain security, privacy, or related requirements or commitments. The external entity, which may be a government or sector-specific entity, an independent 3PAO, an independent testing laboratory, or the buyer itself, conducts an evaluation of the supplier's relevant processes or practices. Such an evaluation may be conducted through an audit or other mechanism. At the conclusion of the evaluation, the external entity shares its findings with the ICT buyer and, where relevant, attests to or certifies the supplier's adherence to its commitments.

Audits or evaluations by 3PAOs can provide buyers with assurance. Audits are most readily available for a subset of global standards and best practices, such as ISO 27001, a leading information security standard, and ISO/IEC 20243, which addresses product integrity and supply chain security best practices to reduce risk associated with taint and counterfeit across the full product and service lifecycle.

For such auditable standards, independent and professional assessors develop proficiency in the requirements and in the architecture, operations, security control implementations, or development and manufacturing practices associated with the product(s) or service(s) that they are responsible for testing. 3PAOs award certifications when they independently determine that a supplier's commitments meet or exceed what those standards require.

There are benefits to certifying suppliers against recognized global standards. Independent third-party certification not only provides more assurance but also saves buyers the time and resources they would need to spend asking questions and validating the answers from each of their suppliers. Suppliers can then demonstrate assurance to ICT buyers by sharing their certification as well as the details of the 3PAO's assessment. Where appropriate, certification materials and other audit artifacts can also be shared with other customers; such global reuse of existing artifacts results in significant efficiency and cost savings.

Questions Related to Demonstrating Assurance:

- How is external attestation, including audits of compliance with global standards, being utilized?
- Where buyer concerns or considerations are not captured within auditable global standards, how can a supplier self-attest to commitments that are responsive to those concerns or considerations?

4. Conclusion

Today, the increased focus on and investment in cybersecurity is significant and meaningful, yet it remains insufficient. Most efforts focus primarily on managing risks to the ICT systems and data they operate; they are not yet adequately considering the security or integrity of the technologies they are buying and how those purchasing decisions can increase or decrease their cyber risk exposure. Many buyers of technology products and services are not yet having conversations about how suppliers govern and manage risk in their environment, how suppliers develop technology products and services and manage security of those over time, and how suppliers can or should demonstrate their practices in these areas.

The questions in this Guide (see Figure 3 on pages 22-23) are designed to facilitate those conversations.

Version 1.0 of this Buyers Guide suggests considerations and practices intended to assist buyers in developing and implementing security-minded purchasing practices to reduce their risk. It is designed to provide buyers with mechanisms to assure that their suppliers are appropriately managing cybersecurity risk in their offerings. We welcome your comments and feedback.

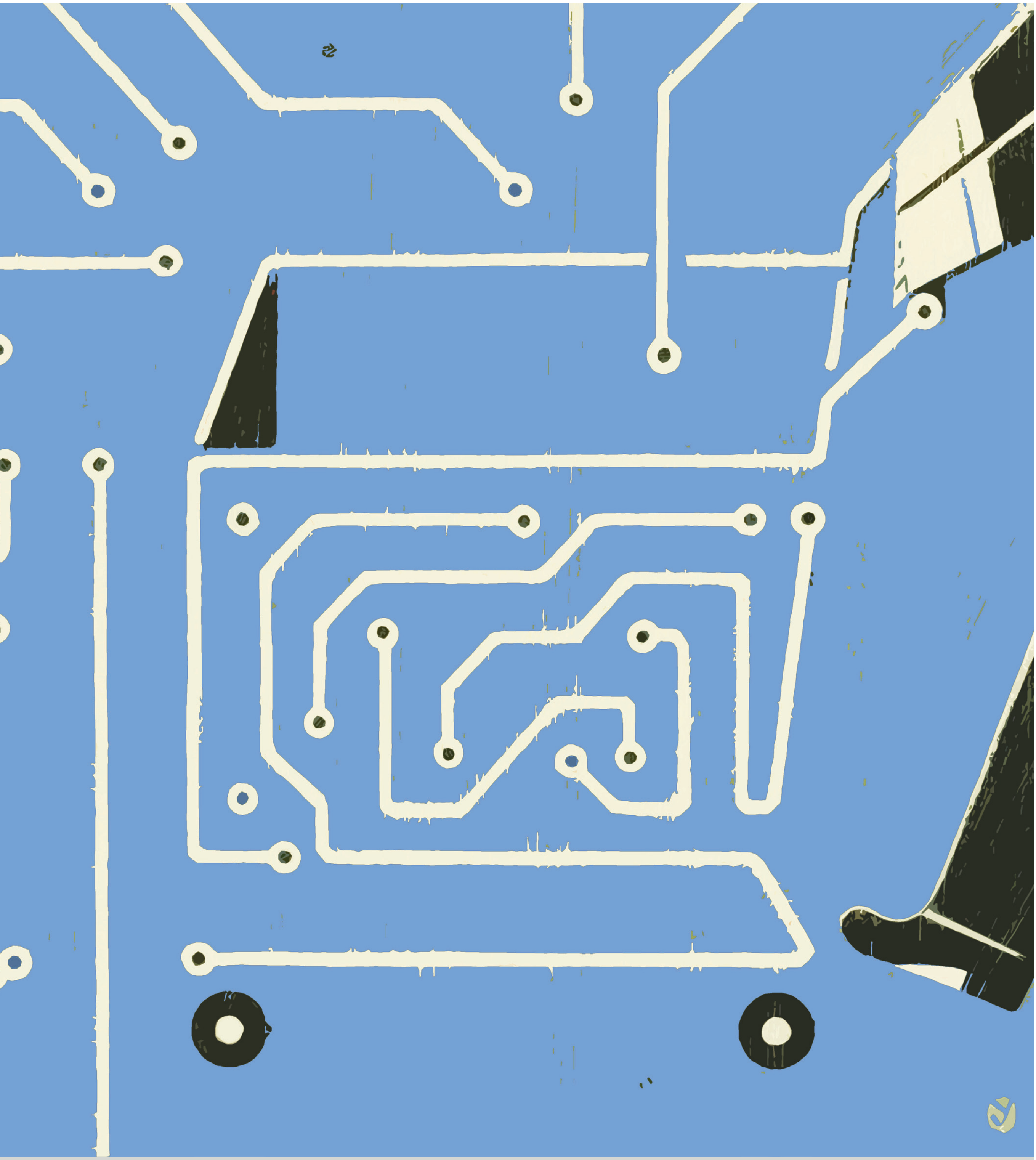


Figure 3: The 25 Questions*

<table>
<tr><th colspan="2">Enterprise Security Governance</th></tr>
<tr><td>Strategy and Control</td><td><b>1.</b> How does the supplier integrate and manage information and cybersecurity risk into the core strategic and operational focus of the business?
<b>2.</b> To what extent can the scheduled release of products or services to customers be delayed in order to address unexpected security concerns?</td></tr>
<tr><td>Standards and Processes</td><td><b>3.</b> What commonly accepted international standards and best practices support supplier security processes and practices? Where gaps exist, how are they being addressed?</td></tr>
<tr><td>Human Resources</td><td><b>4.</b> How are key personnel vetted, selected, trained, and held accountable for trustworthiness?</td></tr>
<tr><th colspan="2">The Product and Services Lifecycle—from Design through Sustainment and Response</th></tr>
<tr><td>Design and Development</td><td><b>5.</b> How does the supplier manage its software development processes, and are those based on industry standards or best practices? If yes, which?
<b>6.</b> Does the supplier have a lifecycle strategy that ensures that products and services are conceptualized (i.e., during R&D), designed, developed, and maintained from a security perspective over their lifecycle? Are cybersecurity requirements embedded throughout, and are they based on any industry standard or best practice?
<b>7.</b> Are secure coding practices in place throughout the lifecycle?
<b>8.</b> How does the supplier identify and trace vulnerabilities (security and non-security) and ensure that they are appropriately prioritized based on risk and addressed in every product and service that might use the vulnerable code/component?
<b>9.</b> How does the supplier monitor changes in the threat landscape and take them into account in the design, development, and deployment phases?</td></tr>
<tr><td>Build</td><td><b>10.</b> What are the security processes used for compilation and/or manufacturing processes?
<b>11.</b> How are products and services continually tested for security vulnerabilities?
<b>12.</b> What international standards and best practices does the vendor comply with in terms of compilation and/or manufacturing?</td></tr>
</table>

* The questions in this Guide were adapted and combined from the eleven categories of 100 questions contained in the Top 100 Requirements white paper developed by Huawei Technologies Co., Ltd. (see Appendix B).

Release, Fulfillment, and Distribution	**13.** How do suppliers identify and authorize partners to distribute their products and services, and how do they verify partners are meeting their commitments? **14.** How are security and integrity of products and services maintained until final customer acceptance? **15.** How does the supplier help the customer integrate products and services into existing infrastructure safely and securely?
Sustainment and Response	**16.** How do ongoing maintenance, patching, incident resolution, and upgrade procedures maintain and enhance product and service functionality and security?
Sourcing and Supply Chain	**17.** Are third-party inputs evaluated for security prior to selection and tracked/validated upon entering the supply chain? **18.** How does the supplier conduct security management with its suppliers? Has the vendor established relevant security criteria and passed the criteria onto its suppliers? **19.** How does the supplier describe its manufacturing process flow and provide details on how it assesses the process, both upstream and downstream, to discover the existence of any tainted or counterfeit components?
Creating Assurance	
Fostering Assurance	**20.** What are the various cybersecurity and privacy laws and requirements in the jurisdictions in which the buyer and/or supplier operate, and how can the buyer and supplier ensure compliance with them? **21.** What are the appropriate commitments to be included in the contract? **22.** How does the supplier seek to provide the buyer transparency into its relevant commitments? **23.** Does the supplier organize security-oriented customer feedback sessions and enable buyers to interact collectively around product and service security concerns?
Demonstrating Assurance	**24.** How is external attestation, including audits of compliance with global standards, being utilized? **25.** Where buyer concerns or considerations are not captured within auditable global standards, how can a supplier self-attest to commitments that are responsive to those concerns or considerations?

Appendix A – Standards Referenced

This Appendix is intended to inform ICT buyers and suppliers on the availability and relevance of existing international standards that address the challenges of cyber and supply chain security in IT. The purpose of the information is threefold: 1) for buyers, so they can be more aware of international standards focused on assessing and managing those risks in their operational environments; 2) for suppliers, so they understand the standards they should be utilizing to address cyber and supply chain risks in their ICT products and services; and 3) for buyers, for procurement purposes, so they can increase their awareness of which international standards and practices they should be requiring of, or recommending to, their suppliers to help assure the suppliers are following best practices throughout the full lifecycle of their products and services including the supply chain.

This Appendix will be maintained and revised over time to account for additional input from government and industry. EWI welcomes input to expand and refine this compendium of cybersecurity and supply chain standards.

Standard Name & Link	General Area of Focus	Specific Areas of Application	3rd Party Certification	Includes Product Development Requirements	Includes Supply Chain Security Requirements	% of Survey Respondents
Standards Related to Governance, Security Management and Risk Assessment						
ISO 27001 and 27002	Information security management: the international standard ISO 27002 defines guidelines for the implementation of controls listed in ISO 27001	Standard for managing the security of an organization's information assets.	YES (27001 only)	NO	NO	43%
ISO 27005	Security risk management for information technology and security techniques	Guidelines for information security risk management—supports the general concepts specified in ISO/IEC 27001.	NO	NO	NO	31%
NIST Cybersecurity Framework (CSF)	Operational requirements for critical infrastructure operators	Risk management and governance.	NO	NO	NO	30%
O-FAIR	The Open Group (FAIR standard) risk analysis taxonomy and methodology	A set of standards for various aspects of information security risk analysis—offers a taxonomy and methodology for risk analysis.	YES: Certification program for practitioners	NO	NO	26%
NIST 800-30	Risk Management Guide for Information Technology Systems	Risk assessment and management.	NO	NO	NO	25%
ISO 31000	Risk management—principles and guidelines	Generic guidelines—not specific to any industry or sector.	NO	NO	NO	23%
COBIT	Standard from ISACA—provides a framework for IT governance and control	IT governance and controls.	YES: Certification program for practitioners and auditors	NO	NO	13%

Standard Name & Link	General Area of Focus	Specific Areas of Application	3rd Party Certification	Includes Product Development Requirements	Includes Supply Chain Security Requirements	% of Survey Respondents
Standards Related to Product and Services Lifecycle - Design through Disposal						
NIST 800-53	Security and privacy controls	Applies to U.S. federal information systems and the environments in which the systems operate—800-161 is an overlay to 800-53 and 800-161 does cover supply chain.	YES	YES	NO	33%
ISO/IEC 20243	Best practices for product integrity and supply chain security (focus on preventing tainted and counterfeit ICT products)—the standard (also known as O-TTPS) can be downloaded from ISO.org or from The Open Group publication site.	Applies to processes used throughout an ICT product's lifecycle (design through disposal, including software, hardware and supply chain). Includes requirements for suppliers.	YES: For ICT Providers (OEMs, hardware and software component suppliers, integrators and value-add resellers)	YES	YES	28%
NIST 800-161	Supply chain risk management practices	For U.S. federal information systems and organizations —overlay for NIST 800-53. Includes requirements for buyers and suppliers.	NO	NO	YES	23%
ISO 27034	Software application security	Applies to processes in full lifecycle development of software applications—does not include supply chain processes.	YES: For practitioners. Professional certifications are available	YES	NO	20%
ISO 27036	Information security for supplier relationships—broad focus on all supplier relations	Processes apply primarily to sourcing and supply chain and the supplier relationships throughout.	NO	NO	YES	13%
Top 100 Questions. See Appendix B.	Procurement questions buyers can ask of their ICT providers	Questions buyers can ask of ICT providers to understand what they are doing to produce secure quality ICT products.	NO	YES	YES	7%
ISO/IEC 15408	Product security through Common Criteria standard	Applies to versions of a product (primarily focused on design, product development and secure methodology of a specific product)—does not include supply chain.	YES: For versions of a product or Target of Evaluation (TOE)	YES	NO	7%

Appendix B – Cybersecurity Perspectives: 100 Requirements When Considering End-To-End Cybersecurity With Your Technology Vendors[9]

Strategy, Governance and Control

1. Does the vendor have a formal strategy and approach to risk management, information and cybersecurity risk?

2. Do your vendors have appropriate governance, organizational design, policies and procedures to support their strategies? And regularly update their strategies to adapt to the latest cybersecurity environment and requirements?

3. What governance structure does the vendor have in place that demonstrates that cybersecurity is a core strategic and operational focus of the business? Do they have a dedicated board committee on cybersecurity? How does this committee operate?

4. How does the vendor ensure that cybersecurity gets addressed in its business? How are board members connected into what is happening in the business, and how are they held accountable?

5. What approach does the vendor take to ensure that every part of their business considers the impact of security? How is this done in a consistent and repeatable way?

6. What is the vendor's approach to resourcing cybersecurity activities? Is it all done via a central dedicated team or is each part of the business involved, including regional security resources?

7. Every company has security incidents. How does the vendor learn from their security incidents? How are they reviewed by their senior executives so that learning is incorporated back into what they do?

8. Have the vendor's internal IT systems ever been a victim of a cyberattack, and how have they learned from this to improve their products and services?

Standards and Processes

9. Does the vendor adopt and support any global standards within the broad definition of cybersecurity? What standards do they conform to and in which standards bodies do they hold senior roles or actively participate?

[9] Source: Huawei Technologies, December 2014, http://usahuawei.com/wp-content/uploads/2014/12/Top100-cyber-security-requirements.pdf.

10. How does the vendor determine what best practices and standards (or laws) should be followed? What processes did they go through to determine and resolve conflict between laws and standards and how do they keep this up-to-date?

11. In an effort to conform to a range of technical standards, what teams or capabilities does the vendor have to support a wide range of management and technical standards including cryptography?

Laws and Regulations

12. How does the vendor assess and attempt to understand the cybersecurity and privacy laws and requirements in the countries in which they operate? How is this information used in the design, development and operation and maintenance of their products and services?

13. How does the vendor ensure that their processes are aligned with local laws and requirements? What do they do when a local law conflicts with their policies, standards or processes? Has your vendor made public statements in relation to its relationships with governments?

14. How does the vendor ensure that their processes and products conform to export control and operating laws (including cryptography) of the country in which they are deployed?

15. What is the vendor's corporate policy on intellectual property rights?

16. How does the vendor ensure that their sales team only sells products and services that comply with local laws and regulations, including any export controls or trade sanctions?

17. How does the vendor review contracts to ensure that they contain accurate information on their capabilities in terms of cybersecurity?

18. Given that all large high technology-based companies use other vendors' technology, does the vendor clearly describe licensing and control mechanisms in place?

Human Resources

19. Does the vendor include the management team in the cybersecurity awareness education of all employees? If so, how is this done? Do their senior executives and board of directors receive continuous training on legal compliance?

20. Not all positions carry the same risk in terms of the insider threat. Does the vendor identify "sensitive" or "critical" positions when it comes to cybersecurity?

21. What approach does the vendor take to recruiting and vetting employees in "sensitive" or "critical" positions? Does the vendor undertake background checks, exit vetting and sign appropriate contractual clauses?

22. What processes and mechanisms does the vendor have in place to provide regular awareness and specific training on cybersecurity that is consistent with employees and contractors' duties, policies, procedures and other requirements? How do they know people have completed the training satisfactorily?

23. Does the vendor have any policies that focus on increasing the competence and understanding of those undertaking "sensitive" or "critical" positions?

24. Many countries have laws on anti-bribery and anti-corruption. How does the vendor deal with this with their employees?

25. Does the vendor have a mechanism where staff can notify management (in an appropriate way) when they feel that things may not comply with policies, laws or regulations?

26. What is the vendor's employee exit strategy and how do they use the knowledge gained from that process in the improvement of their policies, procedures, and culture?

27. Does the vendor have a formal disciplinary guide on cybersecurity?

28. When disciplinary action is taken with an employee, how does the vendor account for the potential failure of their manager or supervisor, i.e., do they address any management or supervisory issues as well?

Research and Development

29. Does the vendor have a formal set of R&D processes that cybersecurity requirements are embedded in, and are they based on any industry standard or best practice?

30. How does the vendor's R&D processes cater to, and assess the effectiveness of, cybersecurity requirements including a dynamic threat environment? What mechanisms do they use to determine what is mandatory and what is just good practice?

31. Customers around the world have differing and sometimes conflicting security and functional requirements; does the vendor have a set of integrated processes that takes a customer requirement all the way through to the end of the relationship and assesses what can and should happen?

32. Does the vendor have a product life-cycle strategy that ensures the product is maintained from a security perspective over its lifespan? What does this tell you and how do they use it?

33. Does the vendor detail how their main product development process works and how progress is reviewed and continuously improved from a technical and quality perspective? Do they detail what reviews, checkpoints and go/no-go decision points are built into that process?

34. Modern software is very complex. It usually contains millions of lines of computer code and thousands of components from different suppliers. What procedure and technology does the vendor use to ensure the right components are used at the right time?

35. Configuration management is a systems engineering process, and supporting technology for establishing and maintaining consistency of a product's performance, functional and physical attributes is required throughout its life. In complex technology environments this mechanism is a cornerstone for consistent, high quality and secure code. What is your vendor's approach?

36. Segregation of duties is important to limit threats and potential damage. How is this implemented by the vendor in R&D, especially for software engineers?

37. Many technology companies embed third-party software and open-source software into their own computer code. How does the vendor track and manage what is in each of their products?

38. Open-source and third-party software can often be found on many websites. How does the vendor know that the software they are downloading is legitimate and does not contain malware or backdoors?

39. Before your vendor uses software from a third-party, what process do they go through to ensure any known vulnerabilities are resolved before it is accepted for use and after it has been deployed?

40. How does the vendor ensure that the defect in a third-party piece of software, or an open source component, or even a common software routine is fixed wherever that code is used?

41. Does the vendor use multiple development languages and tools in their products? If so, how do they catalogue those tools and confirm whether they are up to-date and supported?

42. Is the vendor able to describe their approach to track and trace their end-to-end R&D process and the software tools they use – by each open source or third-party software they use?

43. Complex products tend to generate millions of lines of computer code. Does the vendor have automated code scanning environments to automatically test for coding practice as part of their R&D process?

44. Can the vendor describe their mechanisms for determining if a product can be released to the market, and the authorization process?

45. Throughout the product development cycle and the life of the product, defects will be found. How does the vendor trace all defects and ensure that the defect has been fixed in every product that might use that component?

46. The vendor should describe how they maximize the growth in their competence on cybersecurity. Do they have centers of excellence or a security skills center? How does this work?

47. Threats are constantly evolving. How does the vendor monitor these and take them into account in their design, development and deployment phases?

48. The vendor should detail how their processes are supported by the relevant technology. For instance, how do they use any threat databases in their testing? Or, have they built a library of test cases?

49. The vendor should describe their approach to release management. Some vendors have a single code base for all customers for all countries; some vendors have a code base and then branches for specific regions or countries and customers. Both core methods have strengths and weaknesses. Which approach do they take?

Verification: Assume Nothing, Believe No One, Check Everything

50. Does the vendor have a cybersecurity laboratory that independently verifies (i.e., tested/verified by people who did not develop the product) their products, in addition to the R&D process, before they are released to the market?

51. Can the vendor's R&D or Marketing ignore the findings of this laboratory?

52. Does any internal laboratory that the vendor might have, undertake penetration tests, static and dynamic code scanning to ensure that the code conforms to the cybersecurity design and coding requirements? Do they use an evaluation report to push product teams to make improvements?

53. Does the vendor subject their products to any other independent security verification outside of their HQ's control? If so, what verification and how does this work?

54. Does the vendor allow customers or governments to test their products in their internal or an external laboratory with their own staff, or with security advisers?

55. If a customer or government wanted to use an independent security laboratory run by a third-party or adopt Common Criteria (or similar approach), is this something your vendor would do or would consider?

56. Does the vendor's HQ (or business groups), if at all, control or interfere with the independence of the internal or external laboratories? Does the vendor HQ or their company have the right to see and modify any report or assessment before the customer or government sees it?

57. Does the vendor's HQ R&D get access to any of the tools, processes or scripts that are used by the external laboratories? Could the vendor HQ "second guess" the tests so that the vendor could influence the test results?

58. When one of the vendor laboratories or verification centers discovers a defect or potential vulnerability, what is the process for ensuring that R&D fixes the issue so that it does not recur in future products?

59. Does the vendor laboratory or verification center have the ability to re-test the software after it has been fixed/patched to ensure that the problem has truly been resolved and nothing else has been added?

60. How does the vendor systematically integrate the learning from their verification centers into their business processes?

Third-Party Supplier Management

61. How does the vendor conduct security management with their suppliers? Has the vendor established relevant security criteria and passed them on to their suppliers? How frequently does the vendor update their criteria to ensure they keep up-to-date with the latest thinking?

62. What procurement process requirements do the vendor's suppliers take with their suppliers?

63. Does the vendor have contractual clauses or security agreements in place with their core technology suppliers that provide a comprehensive, risk-informed set of requirements that they must meet?

64. What processes does the vendor have in place to assess the conformity of their suppliers to any security clauses or agreements? Does the vendor maintain scorecards or other metrics to facilitate accountability and drive performance?

65. Does the vendor require their suppliers to notify them in the event that they find vulnerabilities in their products? What does the vendor do with this information? Do they have a vulnerability management process?

66. What approach does the vendor take if one of their suppliers does not, will not or cannot conform to their cybersecurity requirements?

67. Does the vendor conform to international best-practice standards such as those from the Trade Partnership Against Terrorism (C-TPAT) and the Transported Asset Protection Association (TAPA)? Are they certified?

68. Does the vendor conduct onsite audits on the security of their suppliers? What is the scope of those audits? Can the vendor describe how they work with their suppliers to resolve problems found in an audit?

Manufacturing

69. What international standards and best practices does the vendor comply with in terms of manufacturing?

70. Can the vendor describe their manufacturing process flow and provide details on how they assess the process, both upstream and downstream, to discover the existence of any tainted and counterfeit products?

71. How does the vendor ensure that the components that they buy from a supplier are the ones that they receive in their manufacturing centers and meet expectations/standards?

72. How does the vendor ensure that no components are tampered with by their own staff when in their manufacturing center?

73. How does the vendor tamperproof their products when they have been built but not yet dispatched?

74. How does the vendor ensure that the products customers receive are the same as those that left the vendor's manufacturing center?

75. How does the vendor plan their demand of new components so that they have the latest component as frequently as possible?

76. If a customer's specific software is loaded onto their final equipment how does the vendor ensure that this is the same software that was authorized by R&D and has not been tampered with?

77. How does the vendor ensure that someone in the manufacturing center cannot load malware onto a product?

78. In the vendor's manufacturing center, how do they ensure that all the test ports are closed by default when the products leave and cannot be accessed after it leaves the manufacturing center?

79. During the manufacturing process, how does the vendor ensure that unauthorized people do not know what customer the equipment is destined for so that they cannot tamper with specific customer equipment?

80. When products are returned "unused" from customers because they ordered too many or because they cancelled the contract, how does the vendor ensure that the product has not been tampered with before it is returned?

81. When a faulty product is to be returned, what processes does the vendor have in place to ensure that no customer data exists on disks or storage before it is sent to one of their return centers?

82. When a faulty product is fixed in one of the vendor's centers, how do they ensure that all of the replaceable units are original (i.e. not been swapped with a fake item) and that the product contains no malware? Do vendors re-test their products?

83. Does the vendor have a traceability capability and processes for components? Problems can arise anywhere: in a vendor's hardware or software, from a vendor's personnel, or from a third-party. In the event of an issue, how can they trace the "who", "what," "why," "when" and "where" associated with that issue?

Delivering Services Securely

84. What access do the vendor's service engineers need to their customer's installed and operational equipment and services? Can they gain access to what they want, when they want?

85. In what way does the vendor protect the system default accounts or the accounts that the customer gives them to undertake support and maintenance?

86. What controls does the vendor put around the use of laptops or engineering technology their engineers carry? For example, can the vendor's engineers load their own software tools onto their laptop?

87. What processes and controls does the vendor have in place to ensure that their engineers only use the right software for each customer?

88. How does the vendor ensure that their service or support engineers cannot tamper with installed software or install vulnerable or malicious software?

89. Can the vendor detail the approach they take to hardware hardening, software and hardware checks and security products (such as firewalls) for specific customers?

90. When vendors have to capture data for troubleshooting, do they get customers' official authorization and only capture the data within the authorization scope? How do they control what is captured and protect personal data?

91. If the vendor's support engineer cannot fix the issue on-site, and captured data needs to be sent to another country for review, how is this controlled to ensure compliance with the customer's requirements and local laws?

92. What are the vendor's processes for handling data that they captured for troubleshooting when they no longer need it?

93. Audit logs form an important part of proving what has occurred on a system. How can the vendor confirm that their audit logs contain all the relevant information?

94. Customers rely on their vendors especially in times of crisis (e.g., service disruption, natural disaster) for business continuity. How well-equipped and willing is your vendor to support you in difficult times? Ask for real examples.

Issue, Defect and Vulnerability Resolution

95. Does the vendor have a PSIRT/Vendor CSIRT (Product Security Incident Response Team/ Vendor Computer Security Incident Response Team), or equivalent? The vendor should detail their operations and how they can be contacted. What are the processes and requirements that the PSIRT/Vendor CSIRT team is required to follow?

96. What mechanisms does the vendor put in place to deal with a customer CSIRT or coordinators so that they can notify your company of issues and work together to expeditiously address them?

97. Does the vendor have an approach to working with the security researcher community?

98. In the event of a major incident, how is the vendor equipped to ensure that their customers can and will be informed in a timely manner and that the right resources are made available within their company to respond to the incident? The vendor should be able to clearly describe escalation processes.

Audit

99. What processes and mechanisms does the vendor have for internal security auditing and reporting to ensure that the relevant board of directors committee has visibility into the organization's actual risk posture and incident status and consequences, rather than what may be reported to them?

100. Does the vendor have the mechanism to allow external stakeholders or their delegated organizations to conduct the audit?

Appendix C – Feedback Form

The EastWest Institute welcomes any and all feedback on version 1.0 of the Buyers Guide. We welcome your specific comments, and your thoughts on the document more generally. We have provided some questions below for your consideration.

Please send your feedback to **cyber@eastwest.ngo**, with the words "Buyers Guide" in the subject line. We will keep you in the loop!

Questions for reviewer consideration:

1. How useful is the Guide in its present format? How can it be made more useful?
2. How clear is the purpose/intent of this Guide? How well does the Guide accomplish it?
3. Should it be longer? Shorter? If so, what should be added (or taken away)?
4. Are there major questions or considerations that are missing?
5. Does it refer to the right international standards? Are there others that should be added, and if so, in connection with what part of the Guide?
6. Is the relationship between the draft Guide and the NIST Cybersecurity Framework clear enough?

Thank you for your interest. We look forward to hearing from you.

Board of Directors

OFFICE OF THE CHAIRMAN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC

H.E. Dr. Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Ambassador Extraordinary and Plenipotentiary
Embassy of the Republic of Armenia to the United Kingdom
Former Prime Minister of Armenia

R. William Ide III (U.S.)
Counsel and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
Dentons US LLP

Cameron Munter (U.S.)
CEO and President
EastWest Institute
Former Ambassador
Embassy of the United States to Pakistan

CO-FOUNDERS

John Edwin Mroz* (U.S.)
Former President and CEO
EastWest Institute

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.

* Deceased

MEMBERS

Hamid Ansari (U.S.)
President and Co-Founder
Prodea Systems, Inc.

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
Compass-EOS

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Executive Chairman and Co-Founder
The Chertoff Group

David Cohen (Israel)
Chairman
F&C REIT Property Management

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Hu Yuandong (China)
Chief Representative
UNIDO ITPO-China

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Amb. Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

Ralph Isham (U.S.)
Managing Director
GH Venture Partners LLC

Anurag Jain (India)
Chairman
Laurus Edutech Pvt. Ltd.

Gen. (ret) James L. Jones (U.S.)
Former U.S. National Security Advisor
Former Supreme Allied Commander Europe
Former Commandant of the Marine Corps

George Kadifa (U.S.)
Managing Director
Sumeru Equity Partners

Haifa al Kaylani (Lebanon/Jordan)
Founder and Chairperson
Arab International Women's Forum

Zuhal Kurt (Turkey)
Chairman of the Board
Kurt Group

Gen. (ret) T. Michael Moseley (U.S.)
President and CEO
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

Karen Linehan Mroz (U.S.)
President
Roscommon Group Associates

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Amb. Tsuneo Nishida (Japan)
Professor
Institute for Peace Science at Hiroshima University
Former Permanent Representative of Japan to the United Nations

Ronald P. O'Hanley (U.S.)
President & CEO
State Street Global Advisors

Admiral (ret)
William A. Owens (U.S.)
Chairman
Red Bison Advisory Group LLC
Chairman of the Board of Directors
CenturyLink

Sarah Perot (U.S.)
Director and Co-Chair for Development
Dallas Center for Performing Arts

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
CEO
Asurion

Alexander Voloshin (Russia)
Chairman of the Board
JSC Freight One (PGK)
Non-Executive Director
Yandex Company

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Management, LLC

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co. LTD

CHAIRMEN EMERITI

Martti Ahtisaari (Finland)
2008 Nobel Peace Prize Laureate
Former President of Finland

Berthold Beitz* (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher* (Germany)
Former Vice Chancellor and Minister of Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Former Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

George F. Russell, Jr. (U.S.)
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, the OSCE and the United Nations in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Leo Schenker (U.S.)
Former Senior Executive Vice President
Central National-Gottesman Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead* (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

Global Cooperation in Cyberspace Initiative

SUPPORTERS

Microsoft
Huawei Technologies
Unisys
Sonus Networks
Qihoo 360
NXP Semiconductors
CenturyLink
The Hague Centre for Strategic Studies
The William and Flora Hewlett Foundation

PARTNERS

IEEE Communications Society
Munich Security Conference
The Open Group
Fudan University
University of New South Wales
Webster University Cyberspace Research Institute

EastWest INSTITUTE

New York | Brussels | Moscow | Washington, D.C. | San Francisco
www.eastwest.ngo | **t:** @EWInstitute | **f:** EastWestInstitute