Abstract – The document "Choosing Secure and Verifiable Technologies" provides a comprehensive analysis of the essential aspects of selecting secure digital products and services. This analysis covers various critical areas including Secure-by-Design principles, manufacturer transparency, risk management, supply chain risks, and post-purchase considerations such as maintenance and end-of-life policies. Each section offers a detailed examination of the strategies and practices that enhance the security and reliability of technological procurements.

The document is particularly beneficial for cybersecurity professionals, IT managers, and procurement specialists across various industries. It serves as a valuable resource by outlining the necessary steps to ensure that the technologies acquired not only meet the current security standards but also adhere to ongoing security practices to mitigate future vulnerabilities. This analysis aids in making informed decisions that safeguard organizational data and infrastructure from potential cyber threats, thereby enhancing overall business resilience. By integrating these practices, professionals across different sectors can significantly reduce the risks associated with digital technologies and enhance their operational security.

I. Introduction

The document "Choosing Secure and Verifiable Technologies" provides comprehensive guidance for organizations on procuring digital products and services with a focus on security from the design phase through the lifecycle of the technology.

Document emphasizes the critical importance of selecting technologies that are inherently secure to protect user privacy and data against the increasing number of cyber threats. It outlines the responsibility of customers to evaluate the security, suitability, and associated risks of digital products and services. It advocates for a shift towards products and services that are secure-by-design and secure-by-default, highlighting the benefits of such an approach, including enhanced resilience, reduced risks, and lower costs related to patching and incident response.

- **Secure-by-Design and Secure-by-Default**: the necessity for technologies to be designed and developed with security is a foundational element, ensuring that products are secure from the outset with minimal need for additional configurations.
- **Procurement Process**: a two-stage procurement approach – pre-purchase and post-purchase assessments includes evaluating the security features of the product, the manufacturer's transparency, and the ongoing support and updates provided by the manufacturer.
- **Manufacturer Considerations**: Organizations are advised to assess the manufacturer's commitment to security, including their ability to provide transparent information about the product's security features and vulnerabilities. Manufacturers should adhere to practices like publishing complete and timely CVEs.
- **Risk Management**: the importance of continuous risk management, both during the procurement process and throughout the lifecycle of the product or service includes regular updates and patches from the manufacturer to address new vulnerabilities.
- **Supply Chain Risks:** there is a focus on managing risks associated with the supply chain, emphasizing the need for organizations to ensure that their suppliers adhere to secure-by-design principles.
- **Security Incident Management**: it covers the necessity for effective security incident and event management (SIEM) and security orchestration, automation, and response (SOAR) integration to manage and mitigate potential security incidents.
- **End of Life and Post-Purchase Considerations**: the need for clear policies regarding the end of life of products and services, including secure data disposal and transitioning to new technologies.
- **Regulatory and Compliance Issues**: organizations are encouraged to ensure that the products and services comply with relevant regulations and standards, which may vary depending on the industry and type of data handled.

II. Audience

The document is targeted at a broad audience within the realm of digital technology procurement and manufacturing.

- **Organizations that procure and leverage digital products and services**: This encompasses a wide range of entities known as procuring organizations, purchasers, consumers, and customers. These organizations are the main focus of the guidance provided in the document, aiming to enhance their decision-making process in procuring digital technologies.
- **Manufacturers of digital products and services**: The document also addresses the manufacturers of digital technologies, providing them with insights into secure-by-design considerations. This is intended to guide

manufacturers in developing technologies that meet the security expectations of their customers.

Key personnel encouraged to read and utilize this guidance include:

- **Organization Executives and Senior Managers**: Leaders who play a crucial role in decision-making and strategy formulation for their organizations.
- **Cyber Security Personnel and Security Policy Personnel**: Individuals responsible for ensuring the security of digital technologies within their organizations.
- **Product Development Teams**: Those involved in the creation and development of digital products and services, ensuring these offerings are secure by design.
- **Risk Advisers and Procurement Specialists**: Professionals who advise on risk management and specialize in the procurement process, ensuring that digital technologies procured do not pose undue risks to the organization.

The document is designed to be comprehensive, encouraging all audiences to read it in its entirety for several purposes:

- To inform organizations about secure-by-design considerations for the procurement of digital products and services, leading to better-informed assessments and decisions.
- To inform manufacturers about secure-by-design considerations for their products and services, aiming to increase the development of secure technologies. It provides manufacturers with key security questions and expectations they can anticipate from their customers.

The document emphasizes that it is not a checklist for perfect digital procurement outcomes but rather a guide to assist procuring organizations in making informed, risk-based decisions within their unique operational contexts. It acknowledges the uniqueness of every organization in its structure and approach to procurement and suggests that not every item in the document may be relevant to every organization. Additionally, it may be necessary for organizations to consider other factors not covered in the document, which may be unique to their specific situation or the industry or region in which they operate.

III. “Secure-by-Design” Concept

The concept of "Secure-by-Design" (SbD) is a proactive and security-centric approach adopted by software manufacturers during the development of digital products and services. This approach necessitates a deliberate alignment of cybersecurity objectives at all organizational levels involved in the manufacturing process.

- **Proactive Security Integration**: SbD requires that security considerations are integrated from the very beginning of the product development process, rather than being added as an afterthought. This integration occurs across all stages of design, development, and deployment.
- **Purposeful Alignment of Cybersecurity Goals**: The approach demands that cybersecurity goals are aligned with business objectives and product design from the outset. This alignment ensures that security measures are embedded within the architecture of the product or service.
- **Consideration of Cyber Threats**: Manufacturers must consider potential cyber threats during the initial stages of product design. This foresight allows for the implementation of mitigative measures early in the development process, reducing the likelihood of vulnerabilities in the final product.
- **Core Value of User Privacy and Data Protection**: The primary aim of SbD is to safeguard user privacy and data. By designing products with fewer vulnerabilities, manufacturers enhance the security of user data against unauthorized access and potential breaches.
- **Guidance for Procuring Organizations**: Understanding the principles and practices of SbD is crucial for organizations that procure digital products and services. This knowledge helps them make informed decisions, ensuring that the products they acquire are built with security as a foundational element

IV. Shifting the Balance of Cybersecurity Risk

The document “Choosing Secure and Verifiable Technologies” relates to another whitepaper "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default", led by the Cybersecurity and Infrastructure Security Agency (CISA), is a collaborative effort aimed at guiding technology manufacturers in enhancing the security of their products. This publication is significant as it represents an international endeavor to mitigate exploitable vulnerabilities in technology utilized by both government and private sector organizations. The whitepaper is supported by a coalition of global security agencies, including CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and international partners from Australia, Canada, New Zealand, the United Kingdom, Germany, and the Netherlands, among others.

A. Founding Principles

- **Take Ownership of Customer Security Outcomes**: Manufacturers are encouraged to prioritize the security of their customers by integrating security considerations from the initial stages of product development. This principle emphasizes the importance of designing products that are inherently secure, thereby reducing the risk of cyber threats to end-users.
- **Embrace Radical Transparency and Accountability**: This principle advocates for manufacturers to be open and transparent about the security features of their products. It calls for the disclosure of potential vulnerabilities and the steps taken to mitigate them, fostering a culture of accountability.

- **Lead from the Top**: The whitepaper underscores the critical role of senior executives in embedding security into the corporate culture. It suggests that leadership should champion security as a core business goal, ensuring that it is considered a priority throughout the product development lifecycle.

B. *Impact and Implementation*

The whitepaper provides a roadmap for manufacturers to develop products that are secure by design and default, offering protection against prevalent cyber threats without requiring additional configurations or costs for end-users. It suggests that adopting these principles can shift the burden of security from consumers to manufacturers, reducing the likelihood of security incidents resulting from common issues like misconfigurations or delayed patching.

The document highlights the need for a strategic focus on software security, urging manufacturers to make difficult trade-offs and investments, including adopting programming languages that mitigate common vulnerabilities and prioritizing security over appealing but potentially risky features

V. Categories of Digital Products and Services

The various categories of digital products and services emphasize the importance of understanding these categories to ensure secure procurement and usage.:

A. *Software*

- **General Definition**: Software encompasses all types of programs and applications, including operating systems and embedded systems.
- **Proprietary Software**: This is software developed by manufacturers and distributed under specific licensing or purchasing agreements. It often has restrictions such as user limits and prohibitions on resale or modification.
- **Open-source Software (OSS)**: OSS includes software with source code that is freely available under an open license, allowing anyone to view, use, study, or modify it. Managed by a community of volunteers, OSS facilitates rapid product development due to its collaborative nature.

B. *Embedded Software and Firmware*

- **Embedded Software**: This software controls embedded systems designed for specific functions within larger systems, typically constrained by available processing resources and designed for real-time operations.
- **Firmware**: A type of embedded software, firmware is permanently stored in a device’s non-volatile memory and provides low-level control over the device’s hardware components.

C. *Software Bill of Materials (SBOM)*

- **Functionality**: An SBOM lists the software components or libraries that make up a software package. It applies to all software types, including proprietary, OSS, embedded, and firmware.
- **Utility**: SBOMs help manufacturers and consumers identify the components and their versions within a product, facilitating the monitoring of updates and vulnerabilities. SBOMs are typically machine-readable to support automated monitoring and reporting.

D. *Hardware*

- **Scope**: Hardware includes any physical device designed to process, store, or transmit data. This category covers network devices (e.g., firewalls, routers), storage devices, and servers.
- **Hardware Bill of Materials (HBOM)**: An HBOM describes the physical components that make up a hardware device. It is crucial for understanding the materials used in hardware and assessing potential supply chain risks.

E. *Internet of Things (IoT)*

IoT generally falls under hardware and includes devices and sensors that connect to the internet to exchange data and provide functionality. This category includes consumer products, medical devices, and operational technologies.

F. *Cloud Services*

Cloud service providers offer on-demand computing resources, including infrastructure, platform, storage, networking, and processing services. Security considerations like those for software and hardware procurement apply here.

G. *Software as a Service (SaaS)*

SaaS allows consumers to use software without the need to install or manage it themselves. It reduces management overheads and infrastructure costs and can be offered under various agreements, including free access.

H. *Managed Service Providers (MSPs)*

Role: MSPs provide specialized services to help organizations manage, secure, and optimize their cloud infrastructure. Services include cloud infrastructure management, security, and data backup and recovery, allowing clients to focus on core business activities

VI. External procurement considerations

External procurement considerations are divided into the pre-purchase and post-purchase phases to ensure secure and informed decisions when acquiring digital products and services.

A. *Pre-purchase phase*

The pre-purchase phase focuses on several key areas to ensure that organizations make informed and secure choices when procuring digital products and services.

1) *Transparency and Reporting*

- Organizations should verify the transparency of the information provided by manufacturers, which can include industry reports, independent testing, and security feature updates.

- Manufacturers are expected to notify customers of any vulnerabilities found and provide guidance on mitigations, ideally at no extra cost.

- The publication of complete and timely Common Vulnerabilities and Exposures (CVEs) is crucial for maintaining transparency.

2) *Secure-by-Default*

- Products should be secure out of the box, requiring minimal security setup from the consumer to operate safely.

- Secure-by-default features might include multifactor authentication and security logging, with default settings configured to the highest security level.

3) *Security Requirements*

- Organizations must define and understand their specific security needs to ensure that procured products meet these requirements.

- Considerations include encryption standards and identity credentials management.

4) *Supply Chain Risk Management*

- Assessing the security of a manufacturer's supply chain is vital as vulnerabilities can be inherited by the procuring organization.

- Manufacturers should have a supply chain risk management plan to address potential risks.

5) *Open-source Software Usage*

- The use of open-source software (OSS) should be managed carefully to avoid security risks.

- Manufacturers should ensure OSS components are regularly updated and secure.

6) *Data Sharing and Sovereignty*

- Understanding what data will be shared, how it will be used by the manufacturer, and ensuring compliance with data protection laws are critical.

- Considerations include the geographical locations where data is stored and processed.

7) *Development Process*

- Organizations should verify that manufacturers follow secure development practices.

- This includes assessing whether products are developed in a secure environment and adhere to relevant standards.

8) *Geopolitical Risks*

- Manufacturers should be aware of and manage geopolitical risks that could impact their products and services.

- This includes understanding the political stability of the regions where they operate and their supply chains.

9) *Regulated Industries*

Products must be assessed for compliance with specific regulatory requirements relevant to the industry in which they are used.

10) *Manufacturer Access*

- Assessing the need for and security of any manufacturer access to the organization's systems is crucial.

- This includes both remote and physical access controls.

11) *Insider Threat*

- Consider potential risks from insiders within the manufacturer's organization who could harm the procuring organization.

- Controls such as robust hiring practices and monitoring should be in place.

12) *Open Standards*

- The use of open standards promotes interoperability and reduces the risk of vendor lock-in.

- Organizations should verify that products adhere to these standards.

13) *Connected Systems*

Understanding all systems that the product will connect to is essential to assess potential risks and manage them effectively.

14) *Product Value*

Evaluating the overall value of a product, including its cost, expected lifespan, and the security posture it brings to the organization, is crucial for making informed procurement decisions

B. Post-purchase phase

The post-purchase phase addresses several critical aspects of managing digital products and services after acquisition. These aspects are crucial for ensuring ongoing security, compliance, and operational efficiency.

1) *Risk Management*

- Organizations must ensure continuous risk management to address new and evolving threats.

- Regular assessments and updates are necessary to adapt to changes in the threat landscape and to maintain the security integrity of the technology throughout its lifecycle.

- Security Incident Event Management and Security Orchestration, Automation, and Response (SIEM and SOAR)

- Integration of SIEM and SOAR solutions is vital for detecting and rectifying malicious activities effectively.

- These tools require detailed logs from applications to function optimally, and manufacturers should work with SIEM and SOAR providers to ensure their products are logging sufficient information.

2) *Maintenance and Support*

- Organizations must verify that manufacturers adhere to maintenance and support commitments stated during the procurement phase.
- This includes providing timely updates and patches as well as support for addressing any vulnerabilities discovered post-purchase.

3) Contracts, Licensing, and Service Level Agreements

- It is crucial to ensure that all contractual obligations and service level agreements are upheld by the manufacturer.
- Organizations should regularly review these agreements to confirm ongoing compliance and to address any changes that may affect service quality or security.

4) Loosening Guides

- Manufacturers should provide guides that detail the configuration settings that users can change within a product.
- These guides should explain the security implications of altering configurations from their default settings and suggest possible compensating security measures.

5) End of Life

- The end-of-life process for a product should be managed carefully to avoid security risks associated with unsupported or outdated technologies.
- Organizations should plan for the secure disposal or transition of the product at the end of its life, ensuring that all data is appropriately handled and that the product is decommissioned in a manner that maintains security

VII. Internal Procurement Considerations

Internal procurement considerations are divided into three phases: pre-purchase, purchasing, and post-purchase. Each phase addresses specific aspects that organizations need to consider internally when procuring digital products and services.

A. Pre-purchase phase

The pre-purchase phase focuses on ensuring that the internal aspects of an organization align with the procurement of digital products and services. This phase involves consultations and evaluations across various departments within the organization to ascertain that the product or service being considered meets the organizational needs and security standards.

1) Senior Management

- **Risk Assessment and Approval**: Senior management is responsible for establishing the organizational risk threshold and approving the procurement based on a comprehensive risk assessment. This includes understanding the potential risks associated with the product or service and ensuring these are within acceptable limits.
- **Incident Response Plan Inclusion**: It is crucial for senior management to ensure that the product or service is included in the organization’s incident response plan, indicating preparedness for potential security incidents.

2) Policy

- **Policy Compliance**: The procurement must be evaluated against existing policies to ensure there are no conflicts. This includes checking that the level of risk associated with the product or service does not exceed the organization's accepted risk thresholds.
- **Regulatory and Legislative Compliance**: The product or service must meet all relevant logging and auditing requirements, which may be dictated by legislative or regulatory standards. This ensures compliance and aids in the smooth integration of the product or service into the organization’s operations.

3) Infrastructure and Security

- **Security Control Compatibility**: The existing security controls, frameworks, or standards that the organization adheres to must be compatible with the new product or service. A security impact assessment should be completed to evaluate this compatibility.
- **Threat Modeling**: A thorough threat model should be developed to identify relevant threats and risks, ensuring that these are managed to an acceptable level. This helps in understanding how the product or service will fit into the existing infrastructure and what adjustments might be necessary.

4) Product Owner

- **Business Needs and Risk Tolerance**: The product owner must assess whether the product meets the business needs without exceeding the organization's risk tolerance. This includes evaluating the security classification level that the purchase needs to meet.
- **Contract and Risk Mitigation**: The proposed contract should cover an acceptable level of risk and include appropriate risk mitigation measures. The product owner plays a crucial role in ensuring that the contract terms are suitable and that a risk mitigation plan is established

B. Purchasing phase

The purchasing phase involves critical evaluations and decisions that ensure the alignment of the procurement process with organizational goals and security requirements.

1) Senior Management

- **Decision Making and Risk Acceptance**: Senior management is responsible for finalizing the procurement decisions. This includes accepting any residual risks identified during the procurement process and ensuring these risks are within the organization's risk tolerance.
- **Contract Approval**: Senior management plays a crucial role in reviewing and approving the final contracts, ensuring that all terms meet the organization's requirements and that the contracts provide adequate protection and value.

2) System Administration

- **Verification of Technical Specifications: System administrators** are tasked with verifying that the technical specifications of the procured products or services meet the organization's requirements. This includes confirming that all system configurations, integrations, and customizations are correctly implemented.

- **Security and Compliance Checks**: They ensure that the new systems comply with existing security policies and standards. System administrators also play a role in setting up and configuring new systems to maintain security and operational efficiency.

3) Infrastructure and Security

- **Integration and Compatibility**: This area focuses on ensuring that the new procurement integrates seamlessly with the existing infrastructure without compromising security or performance. It involves conducting detailed compatibility checks and planning for any necessary infrastructure upgrades.
- **Ongoing Security Assessments**: Post-integration, it is crucial to continuously assess the security posture of the integrated systems to identify and mitigate any emerging risks promptly.

4) Product Owner

- **Alignment with Business Needs**: The product owner ensures that the procured products or services align with the business needs and strategic goals. This includes verifying that the features and capabilities of the product meet the specified requirements.
- **Management of Product Lifecycle**: They are also responsible for overseeing the lifecycle of the product from procurement to deployment and beyond, ensuring that the product continues to meet the needs of the organization as those needs evolve

C. Post-purchase phase

The post-purchase phase involves ensuring that the procured digital products and services continue to align with the organization's security, operational, and strategic goals. This phase requires ongoing assessments and management practices to address any emerging risks or changes in the organization's or product's environment.

1) Senior Management

- **Continuous Risk Acceptance** and Review: Senior management should establish a process for the continuous or periodic acceptance and review of product risks. This includes ensuring that the product's risks are managed on the organization's risk register and that system security plans and business continuity plans are updated and accepted.
- **Legacy Technology Management**: Senior management must also address the risks associated with legacy technology, ensuring these are documented and managed appropriately within the organization's risk framework.

2) System Administration

- **Monitoring for Security Updates**: System administrators are responsible for setting up monitoring and notification systems for patches, CVEs, and product updates, including those related to the full supply chain. This ensures that the organization remains aware of and can respond to new vulnerabilities or updates.
- **Integration with SIEM and SOAR**: The product should be integrated within the organization's SIEM (Security Information and Event Management) system, and if applicable, SOAR (Security Orchestration, Automation, and Response) capabilities should be provisioned. This integration aids in the detection and response to security incidents.
- **Data Management** Procedures: Procedures for data management, including disposal, editing, and backup, should be established and followed to protect the integrity and confidentiality of data.
- **Incident Response Plan Inclusion**: The new product or service should be incorporated into the organization's incident response plan, ensuring that specific response strategies are in place.

3) Infrastructure and Security

- **Periodic Review of Authorizations**: The organization should periodically review authorizations and privilege accounts to ensure that access controls remain appropriate and secure.
- **Review of Manufacturer's Security Attestations**: Security attestations provided by the manufacturer should be periodically reviewed for updates to ensure that the product continues to meet the required security standards.
- **Management of Legacy and New Technologies**: The organization should have a roadmap or support plan for managing both legacy and new technologies, ensuring that security and operational risks are addressed.

4) Product Owner

- **Manufacturer Adherence to Claims**: The product owner should verify that the manufacturer continues to adhere to the security and operational claims made during the purchase phase.
- **Periodic Contract Reviews**: Contracts and service level agreements with the manufacturer should be periodically reviewed to ensure ongoing compliance and to address any changes in the organization's needs or the product's performance.
- **Risk Assessment of Changes**: Any changes to the product, including updates or configuration changes, should be risk assessed to ensure they do not introduce new vulnerabilities or compromise security.
- **Development of Continuity and Security Plans**: The product owner should ensure that business continuity plans and system security plans are developed and maintained, addressing both regulatory and legislative requirements