The emergence of software security standards: ISO/IEC 27034-1:2011 and your organization

Prepared by

Reavis Consulting Group, LLC

May, 2013

Value and Importance of ISO/IEC 20734

Executive summary

Software has become a pervasive element of human existence and the lifeblood of the modern enterprise. The emergence of cloud computing has created the ability to use new software instantaneously, which imparts tremendous agility to the enterprise. Cloud computing also creates a new dynamic in that it allows millions of users to access a single instance of a software application, which amplifies the need for quality. But cloud computing also faces risk management challenges because of a lack of transparency from cloud service providers, especially with regard to security.

As software evolves, takes many new forms, and is subject to increasing regulatory efforts to manage risk, now is the right time for a standards-based approach to manage software security. In November 2011, the International Standards Organization (ISO) published ISO/IEC 27034-1, "Information technology – Security techniques – Application security," a vendor-neutral and technology-agnostic standard that focuses on managing software security. This standard publication is a significant milestone in industry efforts to secure software and improve risk management through greater transparency. This white paper provides details about why ISO/IEC 27034-1 is needed, presents an overview of the standard, and recommends next steps to consider toward adoption of the standard.

Reaching the current state of industry maturity has come from years of research, implementation, and empirical observations by software companies, academia, government, and other researchers that have established important best practices for securing software. Building in security as an engineering priority throughout the lifecycle of an application—from the very beginning to end—is now universally accepted as the appropriate approach. Implementing processes to assure the software development lifecycle is efficient and effective in delivering secure applications is commonly understood as necessary. The outcome of these practices is not perfect software, but better, more secure software that can be trusted to be continuously improved. Although a large body of evidence supports the benefits of a proactive approach to securing software, the industry can do a great deal to improve the chances of adopting a holistic approach to application security, which is what ISO/IEC 27034-1 prescribes.

ISO/IEC 27034-1 defines concepts, frameworks, and processes to help organizations integrate security within their software development lifecycle. ISO/IEC 27034-1's key framework encourages a holistic organizational view of software development and provides a methodology for using this framework to achieve a proportionate level of trust within a wide variety of applications the organization is responsible for producing, procuring, and operating.

ISO/IEC 27034-1 does not prescribe specific security controls or technology standards. It was designed to be compatible with existing software development lifecycles, and even references other such lifecycles in the industry. It does not mandate a specific amount of resources and is designed to scale to any sized organization. This focus on process without using prescriptive feature guidance should make integration with existing development lifecycles less burdensome. Because ISO/IEC 27034-1 reflects a heritage from the same ISO group that created the pervasive ISO/IEC 27001 and 27005 information security and risk management standards, it is very likely that it will be adopted by the industry at large.

The increasing importance of information technology and the growing threat landscape has led to increased regulatory compliance requirements for IT. Thorough and transparent processes are critical for any organization that seeks to show proactive compliance with regulations and that they availed themselves of existing best practices at any point in time. An international standard such as ISO/IEC 27034-1 is becoming the baseline of practices for producing trusted software, and can help any organization demonstrate due care within their software development lifecycle.

It is critical for organizations to consider the implications of non-secure software beyond their corporate boundaries. The ease with which software components with unknown pedigrees or with uncertain development processes can be combined to produce new applications has created a complex and highly dynamic software supply chain. This supply chain enables tremendous agility in the rapid development of applications to meet consumer demand. However, software components that are produced without secure software development guidance similar to that which is defined by ISO/IEC 27034-1 can create security risks throughout the supply chain.

Software producers have a responsibility to validate their software development practices with ISO/IEC 27034-1 and provide transparency into these practices for their supply chain and all other consumers.

Software consumers, especially large organizations, have a responsibility to understand the secure software development practices that were used to build the software products that they purchase. Toward this end, consumers should encourage transparency in the documentation of secure development lifecycle programs and should acknowledge software producers who adopt secure development standards.

CIOs and CISOs can take a leadership role in assuring their software suppliers are aware of ISO/IEC 27034-1, and they can be the standard's internal champions within their organizations' own software development and software procurement practices.

As regulatory bodies and the IT audit community gain familiarity with ISO/IEC 27034-1, they may also consider the importance of encouraging transparency toward secure software development best practices within the industry.

Experts within secure software development should understand ISO/IEC 27034-1 and map its frameworks and processes to their own practices and tools.

Non-secure applications affect us all, and we have a shared responsibility to improve the trustworthiness of software. The software industry, in all its many forms, must come together to assure that the principles of ISO/IEC 27034-1 and secure software development become as pervasive as software itself.

Why: The need for secure software development standards

It is practically impossible to overstate the importance of software to society and our global economy. Software plays a role in virtually every aspect of our lives, and the power of technology consumerization will create new uses for computer technology on both personal and global scales. Several technology firms have made bold predictions that our current 10 billion Internet-connected devices will soon reach 50 billion and even much more.[1] All of these devices depend upon software to function. Not only is the role of software increasing exponentially, but it is often hidden from view when embedded in new devices or hosted externally in cloud-based services.

At the November 2012 Cloud Security Alliance Congress, US Bank CISO Jason Witty gave a financial services view of the importance of software applications. Compromised software is a tremendous risk to the global economy. 93.6% of the total global currency, or $212 trillion, is digital, and exists in software only;[2] perhaps this metric explains why the financial services industry has traditionally been an early adopter of information security best practices. However, software is becoming similarly crucial to all industries.

Cloud computing represents a significant trend within the history of computing. Compute is essentially becoming a utility that can be instantly turned on or off and scaled up or down. Software as a service (SaaS) is clearly a dominant delivery model for future software, which is significant for multiple reasons. The economies of scale that are available through the cloud computing model will allow many cloud-based applications to provide service to millions of clients simultaneously from a single instance of software. The on-demand nature of cloud computing means that software will be deployed more rapidly than ever. Thus, the importance of software increases but the time allowed to build it with security in mind shrinks.

Software ecosystem

Understanding the implications of non-secure software and appropriate solutions requires insight into the entire ecosystem of software production and consumption. What are the different entities and their roles within this ecosystem?

As individuals, we all have multiple ecosystem roles. Many organizations have dual roles as both producers and consumers of software, and a shared responsibility exists throughout the ecosystem because failures within organizations may have an impact on external entities.

From a general perspective, the ecosystem of software production and consumption includes the following types of roles:

- **Consumers.** Everyone is a consumer of software in either a personal or business role. Educated consumers make the best decisions when faced with a variety of choices, which is also true when purchasing software. Large enterprises are typically the best educated consumers of software, and

[1] Readwrite: Cisco: 50 Billion Things on the Internet by 2020 http://readwrite.com/2011/07/17/cisco_50_billion_things_on_the_internet_by_2020

[2] CSA Congress keynote by Jason Witty https://cloudsecurityalliance.org/wp-content/uploads/2013/01/2012-CSA-CloudCongress-Witty.pdf

have the resources to hire or contract experts to evaluate software for vulnerabilities and security features.

- **Regulators, IT auditors.** This role consists of external and internal entities that assure compliance mandates are achieved within information technology systems.
- **Software delivery entities**. This role consists of the variety of organizations that deliver software:
  - **Software companies**. Producers of software that deliver their product to consumers, who are software users.
  - **Outsourced development houses**. Organizations that build software to specification for unique customers.
  - **Software toolkits**. Provide software tools and application programming interfaces (APIs) that extend functionality of software.
  - **Hardware providers**. Many devices have embedded software.
  - **Cloud providers**. Organizations that deliver software functionality as a service. NIST has defined three major delivery models:[3] software as a service (SaaS), platform as a service (PaaS, rapid application development), and infrastructure as a service (IaaS, basic operating system and storage)
  - **Internally-focused Organizations**. Many organizations develop software for their own use.
  - **Supply chain**. Any combination of this list of software delivery entities.

There are additional valuable considerations with regard to the supply chain. From sophisticated enterprise-class software to simple mobile apps, software is rarely the product of a single organization. Instead, quality, compatibility, and security vulnerabilities can be inherited from a component of the supply chain and be resident in the final product. As the Internet has grown, it has had a profound influence on the emergence of software components that are rapidly assembled into new business applications. The principles of service-oriented architecture (SOA),[4] which views software as a combination of interoperable services, has led to *mashups*, or combinations of software components that can be altered and substituted at will. These components are often *black boxes*—bundles of functionality made from unknown modules with a common interface. The upstream developer may not have access to source code, may not know the developers' secure development practices, or which country they are located in. A developer may not know anything about a component of their application except the service interface.

When the software ecosystem is not operating optimally, problems ensue. Unfortunately, a common consequence is non-secure software. The presence of vulnerabilities can have devastating impacts when software is compromised. These impacts include system downtime, data breaches, data loss, website defacements, and an ensuing loss of trust from an organization's customers and partners.

[3] NIST Special Publication 800-145 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[4] CIO.com: Long live SOA in the Cloud Era
www.cio.com/article/708850/Long_Live_SOA_in_the_Cloud_Era?taxonomyId=3016

Software as a lifecycle and SDL

Trustworthiness is a key objective of the software ecosystem. Many will consider a point-in-time vulnerability scan as an indicator of trust. However, such a scan is a single indicator, and vulnerability discovery and remediation is but one aspect of trust. Much more important than the evaluation of known vulnerabilities today is a more holistic evaluation of the people, processes, and technology that delivered the software and will continue to maintain it. Armed with this knowledge, a consumer can better predict the quality and stability of the software over the long haul. Trustworthiness begins with properly viewing software as existing within a lifecycle. Several software development lifecycles have been published, and most of them contain the same phases: Requirements, Design, Implementation, Verification, and Release.

The key principles of assuring secure software development have been gaining widespread understanding and acceptance for several years. Understanding the fact that software development operates as a lifecycle is a critical principle, regardless of the number of available development resources. If the lifecycle approach to software development is accepted, it follows that efforts to integrate security across that lifecycle must be comprehensive and encompass people, process, and technology.

The Microsoft Security Development Lifecycle (SDL)[5] is a security assurance process that focuses on software development. A holistic people, process, and technology program, SDL embeds security best practices within the software development process. As a company-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in software and culture at Microsoft.

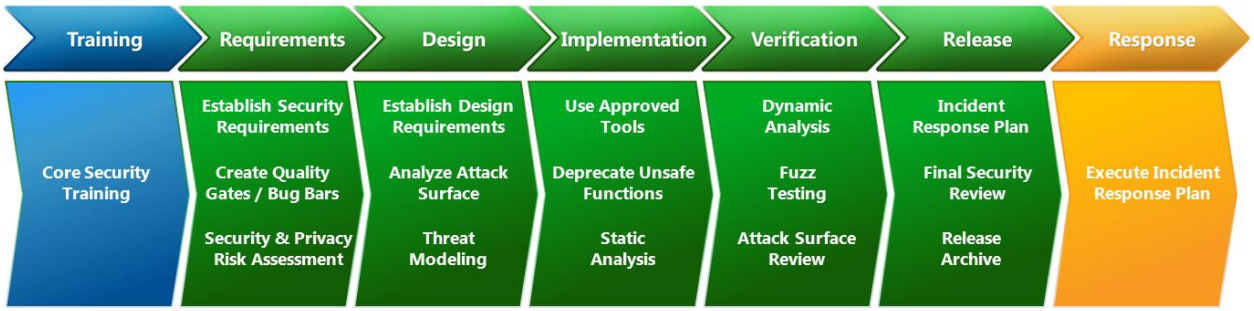

Figure 1. Microsoft Security Development Lifecycle (Simplified)

The preceding figure shows the simplified version of the Microsoft Security Development Lifecycle. Each phase contains key processes and milestone checkpoints to embed security within the typical software development phases. The SDL also includes an initial and ongoing Training phase as well as a Response phase for rapidly addressing incidents with released software.

Although initial research into secure development lifecycles was mainly applicable to large enterprises and mission-critical applications, more recent work such as Microsoft Simplified SDL has made this topic accessible to the smallest development shops. This accessibility is important, because technology

[5] Microsoft SDL Progress Report: www.microsoft.com/en-us/download/details.aspx?id=14107

consumerization makes it possible for mission-critical applications to come in the smallest packages, either by design or by happenstance. Microsoft has made the SDL process available via the Creative Commons license, which allows any organization to use it to secure its own software.

One of the key benefits realized by organizations that use any well-structured security development lifecycle is the return on investment. Identifying software bugs and potential security issues at the earliest possible phase affects fewer resources than each successive phase. Conversely, security issues that are identified in later phases, particularly after software has been released, are exponentially more expensive to remediate. There is also a greater efficiency in setting requirements jointly and early in a development lifecycle.

Transparency

The information security industry has been undergoing an evolution for several years as to its core guiding principles. Just as the previous generation of security technology was focused upon a perimeter, "castle and moat" style of protection for internal assets, the pervading security management philosophy was that of opaqueness—a virtual perimeter surrounding the best practices, processes, and governance employed to secure the organization. This security by obscurity is being replaced by a culture of transparency. Some laws, such as the Sarbanes-Oxley Act, have actually mandated greater transparency.[6] An organization known as the Cloud Security Alliance launched a voluntary registration service for cloud providers to publish their security practices in a public venue, called the CSA Security, Trust and Assurance Registry (STAR).[7] This level of transparency makes understanding and managing risks appropriately much less difficult. As the growing interdependencies of the software supply chain have become apparent, transparency is the primary means by which consumers can assure that their software providers and software supply chain partners are maintaining an appropriate level of security.

Secure software development in the context of organizational information security assurance

As it pertains to a broad view of information security assurance within an organization, the globally recognized standard for certification of security best practices is the ISO/IEC 27001 certification, "Requirements for information security management systems."[8] With a history of nearly two decades, ISO/IEC 27001 certification provides assurance that information security management systems (ISMS) meet rigorous standards. Although not all industries have a clear need to have their information security program externally certified via ISO/IEC 27001, most enterprises are familiar with its principles and have aligned their own ISMS with its code of practice, which is separately described in ISO/IEC 27002, "Code of practice for information security management."[9]

ISO/IEC 27001 proscribes a systematic approach to information security in general, using risk management and the Plan-Do-Check-Act methodology as its quality assurance model. ISO/IEC 27001

[6] SEC: Testimony Concerning Implementation of the Sarbanes-Oxley Act of 2002 www.sec.gov/news/testimony/090903tswhd.htm
[7] CSA Security, Trust and Assurance Registry https://cloudsecurityalliance.org/star/
[8] ISO/IEC 27001:2005 www.iso.org/iso/catalogue_detail?csnumber=42103
[9] ISO/IEC 27002:2005 www.iso.org/iso/catalogue_detail?csnumber=50297

depends upon a scope of certification. For example, an organization may choose to certify a specific business unit. If an organization has significant software development activities, it would likely seek to include its development division within its scope of certification to build trust in its secure software development program.

Historically, the key challenge of certifying the security of a software developer is the lack of its own standardized code of practice analogous to ISO/IEC 27002. Application security requires its own standardized frameworks, methodologies, and processes to achieve its goals. In the past, a lack of such standards could cause auditors to miss key aspects of software development practices and focus instead on generic security practices, such as file encryption, password strength, and incident handling. These practices are important considerations, to be sure, but inadequate for a software developer. For example, assuring that a software application is appropriately performing input validation is a typical security and quality control that is specific to software development. Documenting and evaluating their security development lifecycle appropriately is a pragmatic requirement for a software company to achieve ISO/IEC 27001 certification. The introduction of an international standard for application development (discussed in the next section) is critical to a high-quality ISO/IEC 27001 certification.

Future of standards, regulations, and industry requirements

Standards have an important role in driving information technology. A few specifications from the Internet Engineering Task Force (IETF) have enabled the global Internet and an ability to communicate seamlessly around the world. Although developing standards before a technology is well understood can stifle innovation, the introduction of standards at the right time can drive compatibility, create more consumer options, and establish a baseline of quality. It is difficult to imagine a functioning digital economy without a healthy community of standards development organizations (SDOs).

As information technology has become more vital, a parallel increase in laws and regulations has occurred to mandate how these systems must be governed to protect the public interest. Arguments have been made that the Internet and cloud computing actually resemble a public utility and should be regulated as such. Regardless of your opinion of the efficacy of certain regulations affecting information technology, IT law is clearly here to stay. However, a key problem of regulations is that they typically lag behind the technology. To address this lag, regulations that relate to information systems will increasingly reference standards. Rather than writing regulations that directly prescribe IT best practices, regulators are instead focusing on high-level principles, such as the consequences and potential sanctions stemming from a lack of compliance, and referring to standards as the appropriate best practices to utilize. For example, many laws refer to NIST standards as encryption best practices rather than prescribing their specific cryptographic elements, such as key lengths. The Open Web Application Security Project (OWASP) Top Ten list of web vulnerabilities is used by the Payment Card Industry Data Security Standard (PCI/DSS), which in turn is referred to by various state data breach laws. The problem with these efforts is they are reactive and not proactive. As such it is difficult to train and audit for compliance, and applications have vulnerabilities that could have been mitigated through a proactive process-based approach.

In addition to proactively complying with laws that affect information technology, most organizations are very concerned about the legal consequences of a security incident that may be causally related to how an IT system or application is operated. An organization is in the strongest position when it has adopted commercially reasonable security practices—that is, actions that are well known to the industry and do not introduce inordinate costs to the IT system or application. As standardization of secure software development continues apace, adopting these standards helps an organization establish that it has employed commercially reasonable security practices within the production of its software. IT auditors and regulators are rightfully reluctant to create their own standards for evaluation of an IT system or application. Any lack of clarity increases the complexity of the audit and their findings are more likely to be challenged. It is much simpler and more likely to be seen as more fair if both parties are in practical agreement about the audit criteria. A published standard such as ISO/IEC 27034-1 provides objective evaluation criteria that can be known well in advance and simplify the mandate for auditors and regulators in the realm of application security.

What is ISO/IEC 20734?

ISO/IEC 27034[10] is a six-part standard created by Subcommittee SC27 of the Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC SC27 is the same group that has developed several other widely used information security standards, including ISO/IEC 27001 (Requirements for information security management systems), 27002 (Code of practice for information security management), and 27005 (Information security risk management).[11] ISO/IEC SC27 is globally recognized as the key standards development organization for information security management practices, and its work is commonly cited and referenced by laws, regulations, and other standards around the world. Any standard formally released by ISO/IEC SC 27 should be carefully scrutinized by the industry to understand its implications and appropriate usage.

ISO/IEC 27034 is officially titled “Information technology — Security techniques — Application security.” Its purpose is to help organizations integrate security throughout the lifecycle of their software applications. The first part of six, ISO/IEC 27034-1 was officially released in 2011 and provides an overview of application security concepts as well as the framework and processes that are needed to operate a comprehensive application security program. ISO/IEC 27034-1 is the only part released so far, and can be used separately from the other parts. It is the focus of this section.

What is application security?

In a major section of the standard, ISO/IEC 27034-1 seeks to provide a consensus understanding of application security. It articulates the definitions, concepts, and principles involved in both information security generally and application security specifically. The key takeaways from the definitional section of the standard are as follows:

- **A holistic view of application security**. A valuable contribution of ISO/IEC 27034-1 in the area of definitions is to encourage a holistic view of application security. Securing software should be

[10] ISO/IEC 27034:2011 www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378
[11] ISO/IEC 27005:2011 www.iso.org/iso/catalogue_detail?csnumber=56742

viewed in a broad context that includes software development considerations but also the business and regulatory context as well as other external factors that can affect overall security of the application. For example, a software module might be free of coding errors that may create vulnerabilities, but may otherwise expose sensitive information through a lack of knowledge of which databases are critical to the business function.

- **Application security requirements**. An understanding of risk and the ability to employ this knowledge via risk assessments is crucial to the ability to properly define the appropriate security requirements for any application. An organization's ISMS systematically governs information security risk for the enterprise, including that of the application security program.

Key concepts of ISO/IEC 27034-1

The strategic contribution that 27034-1 makes to the industry's body of knowledge of application security is the introduction of the following two key frameworks for application security and their associated processes. Implementation of these flexible frameworks is intended to help organizations integrate security seamlessly throughout their applications' lifecycles. This part of the standard aligns well with the industry's existing body of work that relates to application security.

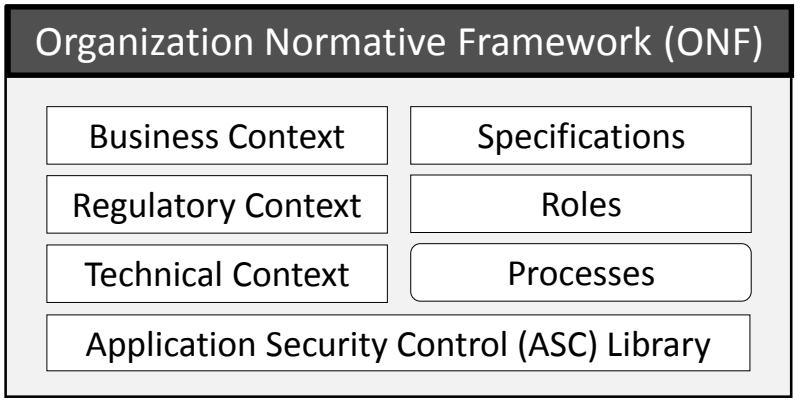

Figure 2. ONF and the Application Normative Framework (ANF)[12]

- **Organizational Normative Framework (ONF)**. The ONF is a framework of so-called containers for all components of application security best practices catalogued and leveraged by the organization. These containers include:
  - Business context, including all application security policies, standards, and best practices adopted by the organization.
  - Regulatory context, including all standards, laws, or regulations that affect application security.
  - Technological context, including required and available technologies that are applicable to application security.
  - Application specifications repository, which documents the organization's IT functional requirements and the solutions that are appropriate to address these requirements.
  - Roles, responsibilities, and qualifications, which document the different actors within an organization that are related in some way to the IT applications. This container will include a wide range of job titles and duties aside from the developer.

[12] Microsoft SDC 2013, Pickel, ISO/IEC 27034 – What, Why, and How. www.securitydevelopmentconference.com/

- The organization's application security control (ASC) library, which contains the approved controls that are necessary to protect an application based on the identified threats, the context, and the targeted level of trust.
- Processes related to application security.

A mapping between an organization's lifecycle model(s) and a reference model is included in the framework.

- **Application Normative Framework (ANF)**. The ANF can be thought of as a derivative of the ONF that is created for a specific application. The ANF maintains the applicable portions of the ONF that are needed to enable that specific application to achieve the required level of security—the targeted level of trust. Because a typical organization will have several applications to secure, there will be a one-to-many relationship between one ONF and many ANFs.

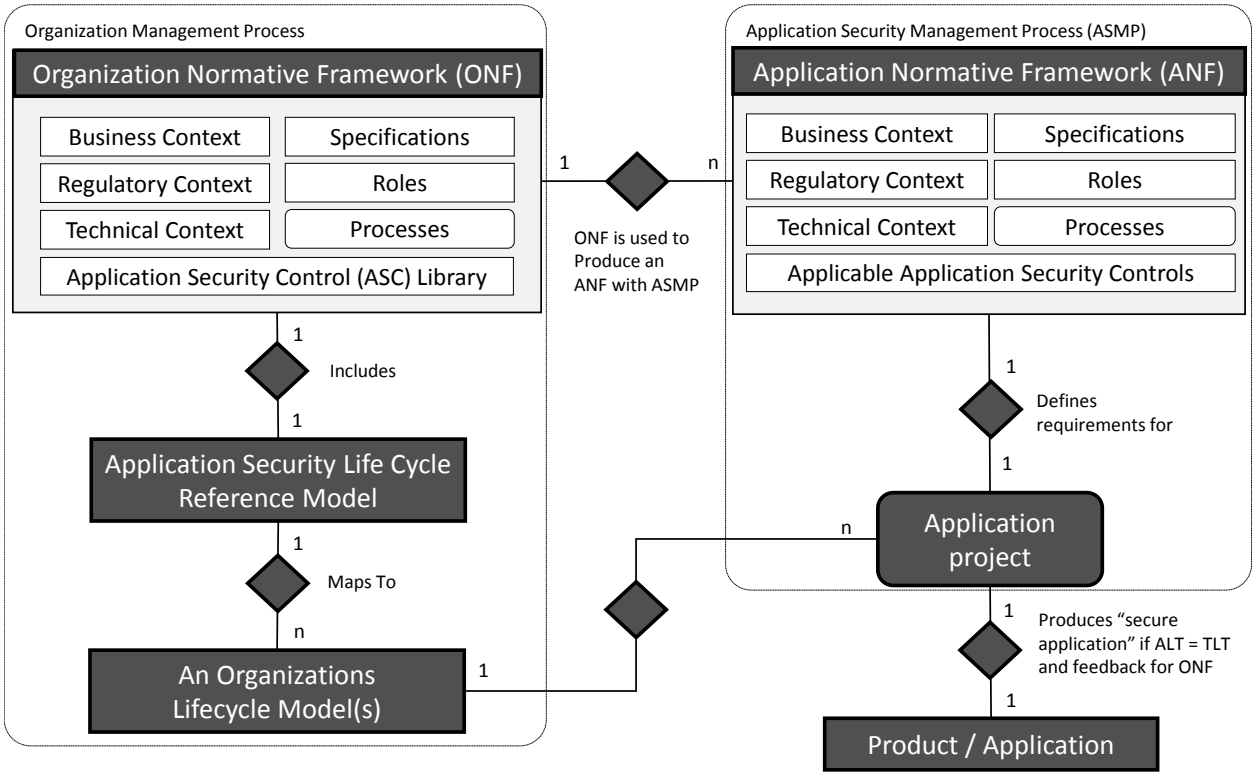

Figure 2. ONF and the Application Normative Framework (ANF)[13]

ISO/IEC 27034-1 defines an application security management process (ASMP) to manage and maintain each ANF. The ASMP is performed in five steps:

1. Specifying the application requirements and environment
2. Assessing application security risks
3. Creating and maintaining the Application Normative Framework

[13] Microsoft SDC 2013, Pickel, ISO/IEC 27034 – What, Why, and How. www.securitydevelopmentconference.com/

4. Provisioning and operating the application
5. Auditing the security of the application

ISO/IEC 27034-1 defines an ONF management process to manage the ONF. This bidirectional process is meant to create a continuous improvement loop, so that every application being secured with an organization gains the full benefit from total organization knowledge, tools, and capabilities. Similarly, innovations that result from securing a single application are returned to the ONF to strengthen the shared knowledge within the organization and address application security in the future.

The frameworks and processes described by ISO/IEC 27034-1 are intended to be sufficiently generic to apply to any type of organization. The standard specifically avoids recommending specific security controls within a development lifecycle, and it does not prescribe any specific technology. ISO/IEC 27034-1 can be used to assess both the quality and the completeness of your application security program.

How does ISO/IEC 27034-1 align with ISO/IEC 27001 and other frameworks?

Although ISO/IEC 27034-1 is not dependent upon ISO/IEC 27001 and can be used independently, it does nicely complement ISO/IEC 27001. As mentioned earlier, the challenge of certifying an application security program with ISO/IEC 27001 is the lack of a code of practice specific to application security. In this sense, ISO/IEC 27034-1 is analogous to ISO/IEC 27002 in that it provides an application security code of practice that can use the systematic Plan-Do-Check-Act quality assurance methodology. It is expected that ISO/IEC 27034-1 will become a key tool used to assess any software development company seeking ISO/IEC 27001 certification, if the software development lifecycle is in the scope of the certification.

Because ISO/IEC 27034-1 is intended to help guide and measure application security programs rather than replace them, it is perhaps not surprising that in Annex A of the standard publication the first case study presented is a detailed mapping of Microsoft SDL to ISO/IEC 27034-1. The standard's authors tagged specific elements of Microsoft SDL as belonging to specific containers within the Organization Normative Framework as depicted in the following figure. Because of the work already done to map Microsoft SDL with ISO/IEC 27034-1, usage of Microsoft SDL for an application security program lends itself to being evaluated by ISO/IEC 27034-1 principles.

Selected mappings between ISO/IEC 27034-1 and Microsoft SDL	
Organization Normative Framework	Security Development Lifecycle
Business context	Product Group
Regulatory context	Legal and Corporate Affairs
Technological context	Product Group and SDL
Specifications	Product Group
Roles	Product Group and Human Resources
Organization ASC library	Training / Requirements / Design / Implementation / Verification / Release
Processes	Final Security Review

Figure 3. Mapping ISO/IEC 27034-1 ONF and Microsoft SDL

The following list includes other information security and governance standards that reference application security and that are likely candidates to integrate with ISO/IEC 27034-1 in some way:

- **NISTIR 7628**. NIST Guidelines for Smart Grid Cyber Security. This standard prescribes secure software development best practices that can be measured via ISO/IEC 27034-1.[14]
- **SAFEcode**. A vendor-neutral organization that promotes the advancement of effective software assurance methods. SAFEcode has published several documents with guidance for secure agile software development, supply chain software security, and critiques of several other industry initiatives that can be mapped to ISO/IEC 27034-1.[15] SAFEcode's security integrity controls can be included in the ONF's application security control (ASC) library.
- **COBIT**. A business framework for the governance and management of enterprise IT developed by ISACA and highly popular with the IT audit community.[16] COBIT contains application security control objectives that can be further clarified and expanded upon by 27034-1.
- **Cloud Security Alliance Cloud Controls Matrix**. Security controls for cloud computing.[17] Key controls reference application security and prescribe adherence to generally accepted standards in the area.
- **Payment Card Industry/Data Security Standard (PCI/DSS)**. A pervasive and highly prescriptive standard for the credit card industry.[18] The existing guidance for payment application security relates closely to ISO/IEC 27034-1. By using ISO/IEC 27034-1 frameworks and an ASMP, it is possible to develop consistent, repeatable processes for assuring that applications handle payment card information appropriately.

A look ahead

As mentioned earlier, ISO/IEC 27034-1 is part one of a six-part standard. The remaining five parts will provide additional depth to the concepts in ISO/IEC 27034-1, but are not yet published. It is not yet known when they will be published and what type of reception they will have in the marketplace.

[14] NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
[15] SAFEcode publication library www.safecode.org/publications.php
[16] ISACA COBIT www.isaca.org/COBIT/Pages/default.aspx
[17] Cloud Security Alliance Cloud Controls Matrix https://cloudsecurityalliance.org/research/ccm/
[18] PCI SSC Data Security Standards Overview https://www.pcisecuritystandards.org/security_standards/

However, high-level management-oriented security standards that originated from ISO/IEC SC27 have an excellent track record for market adoption. We believe ISO/IEC 27034-1 comes from the same tradition of 27001, 27002, and 27005, and will also be a popular standard.

Because ISO/IEC 27034-1 is a concise document and has high-level best practices, we believe it is very accessible to enterprises, IT auditors, regulatory bodies, software producers, and others to incorporate as necessary into their existing initiatives that relate to application security. We also believe that future wildcard events, from security incidents caused by non-secure software to grassroots advocacy for software quality, will create new pressures for organizations to demonstrate their alignment to ISO/IEC 27034-1.

Call to action

Robust application security is a shared responsibility. Mission-critical software applications and services in your organization could have widely varied origins and possibly surprising pedigrees. In addition, some software is being delivered in a model that resembles a public utility, which creates new dependencies that must be accounted for.

Everyone has an interest in raising the bar for application security on a global basis, in addition to the very specific responsibility each of us has for our own software supply chain. There is also a pressing need for an easier way to assess organizational risk posed by poor software engineering practices. ISO/IEC 27034-1 is a standard for application security that is broadly applicable on a global basis and will likely be leveraged widely to quantify trustworthiness of software applications. In our opinion, the following recommendations are timely to act upon:

- **Organizational alignment with ISO/IEC 27034-1**. As described in ISO/IEC 27034-1, the business context of application security is a major consideration within the ONF. Senior management and key business unit owners need to provide executive support for application security best practices. There is precedence in other industries for this conversation, such as manufacturing quality and ISO/IEC 9000/9001. No matter the specific risk appetite within an organization, the business stakeholders need to see software quality and the consequences of non-secure applications as a factor in their risk-based decision making.
- **Align ISMS and risk management frameworks with SDL and key ISO/IEC 27034-1 principles.** Organizations that are directly involved in developing applications should adopt and implement ISO/IEC 27034-1 more fully within the context of their ISMS and risk management program. If you have an application security program, you should use 27034-1 to assess its completeness and alignment with best practices.
- **Encourage transparency within the software ecosystem**. Organizations that are more appropriately considered to be enterprise consumers should align with ISO/IEC 27034-1 as a part of their software vendor management program. It is critical to see the supply chain issues with the delivery of software and assure that vendors can attest to the pedigree of all software for which they are responsible and the application security programs that created it. Consumers should encourage transparency in the documentation of secure development lifecycle programs and should also

acknowledge software producers who meet these requirements. Software companies should see their own transparency as "table stakes" in the new era of software development.

- **C level thought leadership within information systems**. CIOs and CISOs have a responsibility to take a leadership role in assuring their software suppliers are aware of ISO/IEC 27034-1. They should also be the internal champions of ISO/IEC 27034-1 within their own software development and software procurement communities. And within these communities they should emphasize that ISO/IEC 27034-1 is not about producing security overkill, but using risk-based methodologies to achieve a targeted level of trust.
- **Compliance awareness**. Regulatory bodies and the IT audit community have a responsibility to learn about ISO/IEC 27034-1 and determine its long-term applicability to existing compliance mandates and their assurance activities. These groups should also support the transparency theme of governance and development practices within software companies.
- **Secure software expert engagement**. The community of experts that is focused on application security needs to engage with ISO/IEC 27034-1, to map it within existing tools, processes, and frameworks. Doing so will make their own solutions and future versions of ISO/IEC 27034-1 better positioned to meet the needs of the software ecosystem.

Non-secure applications impact us all, and we have a shared responsibility to improve the trustworthiness of software. We should encourage the entire industry—competitors, partners, and customers—to work together to assure that the principles of ISO/IEC 27034-1 and secure software development become as pervasive as software itself.