ISO/IEC 27034

Search
● Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | DONATE!

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27034:2011-2018 — Information technology — Security techniques — **Application security** *(6½ parts)*

Introduction

ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems, in other words business and IT managers, developers and auditors, and ultimately the end-users of **I**nformation and **C**ommunications **T**echnologies. The aim is to ensure that computer applications deliver the desired or necessary level of security in support of the organisation's **I**nformation **S**ecurity **M**anagement **S**ystem, adequately addressing many ICT/cyber-security risks.

The generation and sharing of libraries of reusable, parameterised, well-engineered security functions (see ISO/IEC 27034-5) is a powerful capability with the *potential* to improve security practices in software development, globally. However, it only makes sense in the context of a comprehensive security engineering approach to software/systems development (the other parts of ISO/IEC 27034 plus other standards), requiring substantial investment and management commitment.

Scope and purpose

This multi-part standard provides guidance on specifying, designing/selecting and implementing information security controls through a set of **processes** integrated throughout an organisation's **S**ystems **D**evelopment **L**ife **C**ycle/s. It is process-oriented.

It covers software applications developed internally, by external acquisition, outsourcing/offshoring or through hybrid approaches.

It addresses all aspects from determining information security requirements, to protecting information accessed by an application as well as preventing unauthorized use and/or actions of an application.

The standard is SDLC-method-agnostic: it does not mandate one or more specific development methods, approaches or stages but is written in a general manner to be applicable to them all. In this way, it complements other systems development standards and methods without conflicting with them.

One of the key driving principles is that it is worth investing more heavily in specifying, designing, developing and

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

testing software security controls or functions if they are reusable across multiple applications, systems and situations, albeit at the risk of propagating vulnerabilities more widely than might otherwise be the case. In a nutshell, "Do it properly, once, and reuse". The approach may seem a little idealistic, but some far-sighted organisations are already successfully using it: it is more than just an academic ideal.

ISO/IEC 27034-1:2011 — Information technology — Security techniques — Application security — **Part 1: Overview and concepts** *(first edition)*

- **Abstract:** *"ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications. [Part 1] presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security. ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced." [Source: ISO/IEC 27034-1:2011]*
- As with other multipartite ISO27k standards, the first part sets the scene for the remainder, providing a general introduction and outlining the remaining parts.
- ~80 pages long with quite a bit of detail.
- States explicitly that **this is not a software application development standard, an application project management standard, nor a software development cycle standard. Its purpose is to provide general guidance on application security that will be supported, in turn, by more detailed methods and standards in those other areas.**
- Explicitly takes a *process approach* to specifying, designing, developing, testing, implementing and maintaining security functions and controls in application systems. For instance it defines application security not as the state of security of an application system (the results of the process) but as "a process an organisation can perform for applying controls and measurements to its applications in order the manage the risk of using them".
- Uses the concept of defining a Targeted Level of Trust (similar to a security plan) for an application, designing and building the application to meet it, and then validating the application against it.
- Draws on concepts such as auditing and certification of application systems similar in style to the **C**ommon **C**riteria and similar schemes primarily used for government and military systems. The text tends to emphasize deliberate threats arising from external adversaries implying the importance of confidentiality controls, arguably downplaying insider and accidental threats and the need for integrity and availability controls, but the process described ostensibly takes account of the full spectrum of security risks and controls.
- **Status:** the *first* edition of part 1 was published in **2011**. Three minor corrections plus a revised figure were published in **2014** as a technical corrigendum. The corrected standard was confirmed in 2022.*

ISO/IEC 27034-2:2015 — Information technology — Security techniques — Application security — **Part 2: organisation normative framework** *(first edition)*

- **Abstract:** part 2 *"provides a detailed description of the Organization Normative Framework and provides guidance to organizations for its implementation." [Source: ISO/IEC 27034-2:2015]*
- Part 2 explains the structure, relationships and interdependencies between processes in the **O**rganisation **N**ormative **F**ramework - a suite of application security-related policies, procedures, roles and tools.
- The standard provides guidance on designing, implementing, operating and auditing the ONF.
- The approach is formal and bureaucratic *e.g.* a committee is needed to oversee the ONF, hence it seems most likely to suit organisations who have or want a highly structured way of securing the applications they develop.
- **Status:** the *first* edition of part 2 was published in **2015** and confirmed unchanged in 2021.*

ISO/IEC 27034-3:2018 — Information technology — Security techniques — Application security — **Part 3: Application security management process** *(first edition)*

- **Abstract:** *"Provides a detailed description and implementation guidance for the Application Security Management Process." [Source: ISO/IEC 27034-3:2018]*
- Part 3 describes "the overall process for managing security on each specific application used by an organisation".
- As such, this may be the most broadly applicable and useful part of this standard.
- **Status:** the *first* edition of part 3 was published in **2018**.*

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

~~ISO/IEC 27034-4 — Information technology — Security techniques — Application security — **Part 4: Application security validation** *[cancelled]*~~

- ~~Part 4 was *intended* to describe an application security validation and certification process to assess and compare the ‘level of trust’ of an application system against its previously stated [information security] requirements. However ...~~
- **Status:** the part 4 project was stopped and resurrected several times following objections from CASCO (ISO’s **C**onformity **AS**sessment **CO**mmittee), before eventually being buried for good.
- Part 4 has been *deleted* from ISO’s catalogue.*

ISO/IEC 27034-5:2017 — Information technology — Security techniques — Application security — **Part 5: Protocols and application security controls data structure** *(first edition)*

- **Abstract:** part 5 *”outlines and explains the minimal set of essential attributes of ASCs and details the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM).” [Source: ISO/IEC 27034-5:2017]*
- Part 5 facilitates the implementation of the ISO/IEC 27034 application security framework and the communication and exchange of ASCs by defining a formal structure for ASCs and certain other components of the framework.
  - It defines the **A**pplication **S**ecurity **C**ontrols data structure, providing requirements, descriptions, graphical representations and XML schema for the data model.
    - The XML schema, based on ISO/TS 15000 “*Electronic business eXtensible Markup Language ebXML*”, is designated as the standard interchange format for ASCs.
  - It explains a minimal set of essential attributes of ASCs and the Application Security Life Cycle Reference Model.
- **Part 5 enables the establishment of libraries of reusable application security functions that may be shared both within and between organisations.**
- **Status:** the *first* edition of part 5 was published in **2017** and confirmed in 2023.*

ISO/IEC TS 27034-5-1:2018 — Information technology — Security techniques — Application security — **Part 5-1: Protocols and application security controls data structure, XML schemas** *(first edition)*

- **Abstract:** part 5 dash 1 *“defines XML Schemas that implement the minimal set of information requirements and essential attributes of ASCs and the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM) from ISO/IEC 27034-5.” [Source: ISO/IEC 27034-5-1:2018]*
- **Status:** the *first* edition of part 5-1 was published a **T**echnical **S**pecification in **2018** and confirmed unchanged in 2021.*

ISO/IEC 27034-6:2016 — Information technology — Security techniques — Application security — **Part 6: Case studies** *(first edition)*

- **Abstract:** part 6 *“provides usage examples of ASCs for specific applications. NOTE Herein specified ASCs are provided for explanation purposes only and the audience is encouraged to create their own ASCs to assure the application security.” [Source: ISO/IEC 27034-6:2016]*
- Part 6 provides examples of how **A**pplication **S**ecurity **C**ontrols might be developed and documented.
- It concerns the handling of information security in the course of software development.
- **Status:** the *first* edition of part 6 was published in **2016** and confirmed unchanged in 2022.*

ISO/IEC 27034-7:2018 — Information technology — Security techniques — Application security — **Part 7: Assurance prediction framework** *(first edition)*

- **Abstract:** part 7 *”describes the minimum requirements when the required activities specified by an Application Security Control (ASC) are replaced with a Prediction Application Security Rationale (PASR).*

The ASC mapped to a PASR define the Expected Level of Trust for a subsequent application. In the context of an Expected Level of Trust, there is always an original application where the project team performed the activities of the indicated ASC to achieve an Actual Level of Trust. The use of Prediction Application Security Rationales (PASRs), defined by [ISO/IEC 27034-7], is applicable to project teams which have a defined Application Normative Framework (ANF) and an original application with an Actual Level of Trust. Predictions relative to aggregation of multiple components or the history of the developer in relation to other applications is outside the scope of [ISO/IEC 27034-7]." [Source: ISO/IEC 27034-7:2018]

- Part 7 specifies a framework to deliver the assurance necessary to place trust in a computer program's security arrangements, for example:
  - When one program (such as an application) relies on another (*e.g.* a database management system, utility, operating system or companion program) to perform critical security functions (such as user authentication, logical access control or cryptography), or
  - When an organisation updates or patches a trusted program.
- Encourages organisations to consider, determine/specify and document the trust or criticality (the "security predictability") as the basis for their rational decisions plus those of their software suppliers concerning the way software is designed, developed, tested, delivered, managed, operated and maintained.
- Specifies minimum requirements when the required activities specified by an **A**pplication **S**ecurity **C**ontrol are replaced with a **P**rediction **A**pplication **S**ecurity **R**ationale.
  - The ASC mapped to a PASR defines the *Expected* Level of Trust for a subsequent application.
  - The use of PASRs is applicable to project teams which have a defined **A**pplication **N**ormative **F**ramework and an original application with an *Actual* Level of Trust.
- **Status:** the *first* edition of part 7 was published in **2018** and confirmed unchanged in 2023.*
- **Personal comment:** the language in part 7 is decidedly formal and stilted (*e.g. "An application security claim is a claim that the application team implemented certain security controls and those controls mitigate specific security risks to an acceptable level. A security prediction is the transfer of confidence in the original claim to a claim that the same security controls are also present in a subsequent version of the application and mitigate, to the same acceptable level, the same specific security risks."* - got that?). It's about as far from from ISO's version of plain English as it is possible to go.

Personal comments

* In 2023, it was *proposed* to update the entire ISO/IEC 27034 suite of standards. The structure and focus of the multi-part standard could be modified, making it more relevant and useful for SMEs, and better aligned with other software engineering standards.

All parts of the standard should conform with JTC 1/SC 17's standards on software engineering, plus relevant ISO27k standards, and the terminology should align with the ISO 31000 series.

Rewriting all the present parts in plain English would be enormously challenging for SC 27 but could substantially extend the utility and value of these standards. Maybe.

The update commenced in October 2024. It will take *years* to complete.

< Previous standard ^ Up a level ^ Next standard >