Agile software development under ISO 27001

Leon du Toit

2022-11-22

Abstract

The ISO 27001 standard lists a host of requirements for implementing IT security in an organisation. Conforming to requirements of the standard can raise the cost and friction involved in releasing new services and features in an agile manner. This paper will explore which tools and processes can be used to mitigate the potential clash between the goals of standard compliance, and sustaining an agile development culture. The paper is organised as a case study at the University of Oslo's Center for IT, where the Services for Sensitive Data is in the process of adopting ISO 27001. *Keywords: Agile, DevOps, DevSecOps, SecDevOps, ISO 27001*

Introduction

Agile software development (Beck (2022)) is described as valuing:

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

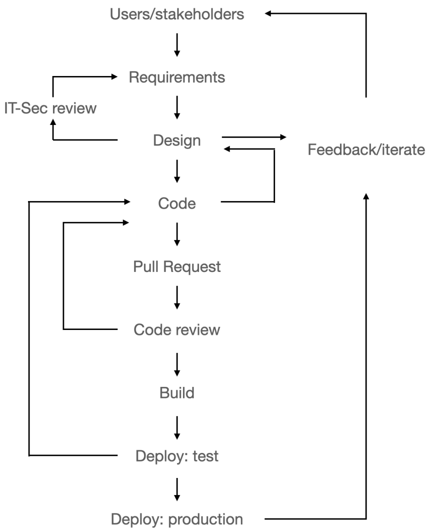
So while the latter items are valuable, Agile sees the former items as *more valuable*. The University of Oslo's (UiO) Services for Sentitive Data (TSD), a special purpose eInfrastructure, is developed and operated by UiO's Center for IT's Section for Research Services. Agile software development is a well-established practice within the section, and is used to continuously develop new features and services for TSD.

At the same time the Section for Research Servics is working to certify TSD for ISO 27001 ("Information Technology - Security Techniques - Information Security Management Systems - Requirements (ISO/IEC 27001:2013 Including Cor 1:2014 and Cor 2:2015)" (2017)). ISO 27001 stipulates that an organisation should adopt an Information Security Management System (ISMS) in order to manage risks, to ensure that its information security policies are met. The organistion shall identify, and analyse risks and their potential impact, and implement risk-mitigating controls. All of this needs to be documented, and updated over time. In practice this influences software development processes, and has the potential to uproot an agile development culture, by reversing the order of importance in the Agile values articulated above.

The rest of this report will explain how ISO 27001 certification can adversely affect TSD's agile development culture, and explore how SecDevOps can offer a solution to this conundrum.

Agile software development at TSD

Figure 1 below show lol



The impact of ISO 27001 on software development

This section reviews the controls listed in Annex A of the ISO 27001 which will have an impact on software development practices in TSD. For each control, the expected impact on TSD's software development process is described.

- A.12.1.2 Change management
- A.12.5.1 Installation of software on operational systems
- A.12.6.1 Management of technical vulnerabilities
- A.14.1.1 Information security requirements analysis and specification
- A.14.2.1 Secure development policy
- A.14.2.2 System change control procedures
- A.14.2.3 Technical review of applications after operating platform changes

- A.14.2.4 Restrictions on changes to software packages
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.8 System security testing
- A.14.2.9 System acceptance testing
- A.15.1.3 Information and communication technology supply chain

Problem statement

SecDevOps as a solution

Processes and tools

References

Beck, Kent. 2022. “The Agile Manifesto.” Agile Alliance. 2022. https://www.agilealliance.org.

“Information Technology - Security Techniques - Information Security Management Systems - Requirements (ISO/IEC 27001:2013 Including Cor 1:2014 and Cor 2:2015).” 2017. Standard. International Organization for Standardization.