Evaluating security and privacy of SaaS service

Sami Savolainen

Master's thesis
October 2023
Master of Engineering in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Description

Savolainen, Sami

Evaluating security and privacy of SaaS service

Jyväskylä: JAMK University of Applied Sciences, October 2023, 77 pages plus appendix SaaS Security Evaluation Tool-matrix 8 pages.

Technology, Communication and Transport. Degree Programme in Information Technology. Master's Thesis

Permission for open-access publication: Yes

Language of publication: English

Abstract

Software as a Service (SaaS) applications have become famous for IT services, especially in small and medium-sized organizations (SMEs). In the SaaS model, the customer depends on the service provider for appropriate security measures and availability. Many cybersecurity and data protection requirements must be considered when purchasing a new service. The thesis aims to find key security aspects of SaaS applications and investigate the possibility of providing a checklist tool for SME organizations to evaluate these requirements manually without investing in procurement systems and cybersecurity resources.

The SaaS evaluation tool requirements are collected using a literature review, including SaaS security issues, mitigations, and security standards, to understand the needs of the framework. There are also reviewed available cloud security evaluation frameworks, like Enisa and Cloud Security Appliance (CSA).

Using the checklist tool, the test group tried out the evaluation model, and their feedback was analysed using a qualitative research method. Based on these results, it was possible to compile the challenges of the manual evolution process. It was noticed that there is no standard method in describing the security of SaaS services and understanding the terminology requires information security knowledge. In addition, the manual evaluation was perceived as laborious, and ensuring its up-to-date and comparability requires follow-up measures.

As a summary of the research, it can be stated that it is challenging to build a SaaS service information security and data protection evaluation criteria. On the other hand, it is possible to share information about information security requirements for business; the respondents found it helpful. In future development, the need for authorities is to provide a consistent framework for cloud security documentation. Another requirement is to get an easy and cost-effective IT procurement solution for SME-size businesses to automate these security evolutions.

Keywords/tags (subjects)

Cyber security, Software as a service (SAAS), cloud services, information security, data protection

Miscellaneous (Confidential information)

Work is public. Does not include any confidential information.

Kuvailulehti

Savolainen, Sami

Turvallisuuden ja tietosuojan arviointi SaaS-palvelulle

Jyväskylä: Jyväskylän ammattikorkeakoulu, Lokakuu 2023, 77 sivua, lisäksi liitteenä SaaS turvallisuuden arviointitaulukko 8 sivua

Tekniikan ja liikenteen ala. Insinööri (ylempi AMK), tietotekniikka

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: englanti

Tiivistelmä

Software as a Service (SaaS) -sovelluksista on tullut suosittu tapa IT-palveluiden käyttämiseen, erityisesti pienissä tai keskisuurissa organisaatioissa (pk-yritykset). SaaS-mallissa asiakas on riippuvainen palveluntarjoajasta asianmukaisten turvatoimien ja saatavuuden suhteen. Uutta palvelua ostettaessa tulee huomioida monet kyberturvallisuus- ja tietosuojavaatimukset. Opinnäytetyön tavoitteena oli löytää keskeisiä SaaS-sovellusten tietoturva- ja tietosuojakriteereitä ja tutkia mahdollisuutta tarjota pk-yritysten organisaatioille tarkistuslistatyökalu, jonka avulla nämä vaatimukset voidaan arvioida manuaalisesti ilman hankintajärjestelmiin ja kyberturvallisuusresursseihin panostamista.

SaaS-arviointityökalun vaatimukset kerättiin kirjallisuuskatsauksen avulla, mukaan lukien SaaS-tietoturvaongelmat, -mitigaatiot ja -standardit, jotta voidaan ymmärtää viitekehyksen tarpeet. Työssä hyödynnettiin myös saatavilla olevia pilviturvallisuuden arviointikehyksiä, kuten Enisa ja Cloud Security Appliance (CSA)

Tarkistuslistatyökalun avulla testiryhmä kokeili arviointimallia ja heidän antamaansa palautetta analysoitiin kvalitatiivisella tutkimusmenetelmällä. Näiden tulosten perusteella oli mahdollista koota manuaalisen evoluutioprosessin haasteita. Huomattiin yhteisen tavan puuttuminen SaaS-palveluiden turvallisuuden kuvaamisessa ja termistön ymmärtäminen vaatii tietoturvaosaamista. Lisäksi manuaalinen arviointi koettiin työlääksi ja sen ajantasaisuuden ja vertailukelpoisuuden varmistaminen vaatii jatkotoimenpiteitä.

Tutkimuksen yhteenvetona voidaan todeta, että on haastavaa rakentaa SaaS-palvelun tietoturvallisuuden ja tietosuojan arviointikriteeristöä. Toisaalta on mahdollista jakaa tietoa tietoturvavaatimuksista liiketoiminnalle, vastaajat kokivat sen hyödylliseksi. Kehitystoiveina nähdään tarve viranomaisten kehittämälle vertailukelpoiselle viitekehykselle pilvipalveluiden turvallisuuden arvioimiselle. Lisäksi pk-yrityksille suunnatut helpot ja kustannustehokkaat IT-hankintajärjestelmät auttaisivat automatisoimaan hankittavien palveluiden turvallisuusarviointeja.

Avainsanat

kyberturvallisuus, Software as a service (SAAS), pilvipalvelut, tietoturva, tietosuoja

Muut tiedot (salassa pidettävät liitteet)

Työ on julkinen. Ei sisällä salaisia tietoja.

Contents

Figures

1 Introduction

1.1 Background

Software as a Service (SaaS) applications have become increasingly popular for providing IT services to organizations. SaaS has many advantages, especially for Small or medium-sized organizations (SMEs) (Mäkikyrö, 2020); it reduces the need for resources and money for installing, managing, and upgrading software. According to Mäkikyrö's study, the main benefit of a SaaS solution is that it is a service, not a product; the customer is responsible only for service use and payment. The service provider updates their product and looks for errors when developing new versions. Organizations need scalable and more complex applications to run their business, and many solutions, like widespread communication, CRM, or ERP, are only available in SaaS applications.
The vendor provides SaaS services from a central location, accessible over the Internet, most typically using a web browser, and the vendor is responsible for hardware and software maintenance. Another possible delivery method is providing desktop applications to client devices like Slack or Microsoft Office 365 desktop applications.

There are limitations and questions about SaaS services:

- Integration with other applications and services
- Vendor lock-in
- Missing integration support
- Data security
- Customization
- Lack of control
- Features limitations
- Performance and downtime

These elements need to be evaluated by business needs before onboarding new services. This thesis will concentrate mainly on the data security features of SaaS solutions.

The purchasing process of a new SaaS application starts most commonly from the business unit's needs. They might need some solution to provide better service for the customer or trial new technology. Enterprise-sized and more mature organizations have more standard processes of solution provider procurement. They are invested in procurement solutions and have in-house IT and legal teams to support the purchase process.

An SMB-sized organization might have a different IT department, or evaluation and trialing of applications has started in the business unit before contacting the IT department. The business unit has used a lot of effort and time to evaluate the product and its business effects. It should have checked security and privacy questions in a standardized way. This thesis aims to provide a SaaS Evaluation Tool that allows verification solutions for security and privacy functions during the evaluation phase. Then, it is possible to save organizations and IT departments time and provide a more secure IT environment.

The size of the SaaS service business is growing fast. Fortune’s insight report (*Software as a Service [SaaS] Market Size & Growth, 2022-2029*, 2023) estimates that the market size of SaaS services will triple during the next seven years, from USD 251 billion (2022) to USD 884 billion (2029) and market has been grown 12 % from the year 2019 to 2020.

1.2 Purpose and Objectives

Avidly Oy has ordered this thesis. Avidly is an SMB-sized marketing technology provider headquartered in Helsinki, with about 350 employees in eight countries. Avidly provides marketing agency services in Finland and is the world's largest reseller and consultant of US-based marketing automation tool HubSpot. HubSpot provides SaaS-based software for inbound marketing, customer service, and sales and has a close partnership with Avidly. Thesis author Sami Savolainen is an IT manager in Avidly and manages and operates its IT environment. SaaS-based, like collaboration tools, file storage, and marketing technology solutions.

Avidly's business unit members are innovative and keen to develop their work and toolsets. The business unit uses time and effort to evaluate new applications and service providers. Avidly’s goal is to review the application's security and privacy in a standardized way. Avidly's IT department will help audit the service, but Avidly's goal is to move preliminary audit work to the business units. One main reason is to check the service's security earlier to avoid wasting time; if first evaluating the service's business effect, the IT department may abandon the application during the IT security audit. The second reason is to share knowledge of security for non-technical persons. The third reason is to provide a standardized way to evaluate applications' security and privacy.

IT departments have IT service management tools (ITSM) with service catalog that lists organizations' applications. The service catalog includes at least some basic information about the application, like use purpose, product owner, cost, privacy, and security details. Management tools provider target their solutions for IT departments, and these tools need the competence to maintain. These tools have user license limitations; the IT department will restrict or avoid allowing complete access to ITSM tools for privacy and security reasons.
This thesis aims to create a SaaS-vendor evaluation checklist for evaluating applications' security and privacy in a standardized way. Tools are for business unit members without cyber security or privacy competence.

99.8% of European enterprises are Small and medium-sized enterprises (SMEs), so the sector covers most companies. There needs to be EU-level guidance on cybersecurity practices and suitable standards for organizations' needs (Ozkan & Spruit, 2019), which impacts SMEs' potential victims of cybersecurity crimes. SMEs do not have the financial resources to purchase external assistance for technical or legal support; they are not aware of the benefits of standards. Cyber security is "the preservation of confidentiality, integrity, and availability of information in cyberspace," according to ISO/IEC 27032–guidelines (ISO, n.d.). The European Cybersecurity Organization (ECSO) was published in 2017, listing existing cyber security standards. Standards are generic without specific business areas, so these are industry-specific requirements. This thesis tries to help SME organizations for evaluating SaaS security.

1.3 Research Question

The research questions of the master's thesis are:
"What are the key security aspects of SaaS application?"

Thesis aim is to find and address the key security aspects of SaaS applications. Using this knowledge, it can be possible to reduce the risk of data breaches, malware infections, and other security incidents. It's a proactive approach to managing security risks and ensuring the overall success and trustworthiness of the SaaS offering.

Another research question is:
"Is it possible to create an evaluation tool of SaaS applications security and privacy that will help select a suitable solution for the business?"

The evaluation tool could assess variety of factors, such as data encryption, access control or compliance. It can also consider the specific needs of the business, such as the type of data that will be stored in the SaaS application and the industry regulations that the business must comply with. On the other there can be found that there once the evaluation tool has assessed the SaaS applications, it could generate a report that ranks the applications based on their security and privacy features. The report could also include recommendations for how to improve the security and privacy of the SaaS applications.

According to experience, the assumption is that there might be issues with the evaluation tool that the user can handle. However, finding answers from solution providers might be complicated, and there is no standard method to document security and privacy features.

1.4 Research Objectives

This thesis will try to solve the research questions and complete the research targets. The following research objectives have been formulated for this thesis project:

- Identification of Key Security Aspects in SaaS Product Evaluation: The foremost objective is to identify and delineate the critical security aspects that warrant consideration when evaluating Software as a Service (SaaS) products.
- Establishment of a Value Scale: This scale will assign relative weights and significance to various security and privacy criteria.
- Preliminary Testing of the Evaluation Tool: Before its utilization in the primary research study, the thesis author will conduct an initial trial of the evaluation tool. This preliminary testing phase will assess the tool's functionality, validity, and reliability.
- Selection of a Diverse Trial Group: To ensure the comprehensiveness and validity of the research findings, participants for the evaluation of SaaS applications will be chosen from a

diverse pool of users with varying backgrounds, expertise, and perspectives. This approach aims to capture a wide range of insights and experiences.

- Provision of Recommendations Based on Research Outcomes: The final research objective is to generate informed recommendations derived from the empirical findings of the evaluation process. These recommendations will serve as valuable guidance for businesses and organizations seeking to make informed decisions when selecting SaaS solutions.

In summary, this thesis is designed to fulfill these research objectives, each of which plays a crucial role in advancing the understanding of security and privacy aspects in evaluating SaaS products.

1.5 Research Method and Data

The thesis uses qualitative research methods to collect and analyze non-numerical data and understand experiences and opinions. The technique collects new ideas and gives more detailed insight (Bhandari, 2020). Qualitative research methods excel in exploring the depth and complexity of human experiences and opinions. These are ideally suited for research topics where the aim is to gain a deeper understanding of the subject matter, explore the nuances of participants' perspectives, and generate insights that go beyond numerical data. By embracing subjectivity, context, and rich narrative data, qualitative methods provide a holistic and nuanced view of the research topic.

This study's selected qualitative research method involves surveys with open-ended questions, which were administered to a carefully chosen test group. This survey aimed to gather feedback and opinions regarding the SaaS evaluation tool developed for the research. The responses provided by the test group members were subsequently analysed to derive valuable insights and conclusions.

In addition to open-ended questions, the questionnaire used in the survey also included numerical scaled questions. These scaled questions complement the qualitative data obtained from open-ended responses by providing quantifiable data points. Including numerical questions facilitates the generation of comparable answer results, allowing for a more comprehensive analysis of the research findings.

Building the SaaS evaluation tool is created using a literature review. The practical part of the thesis is a survey evaluation tool by the test group. This evaluation tool will be developed for the business unit's needs.

Feedback on the evaluation tool is collected using feedback from the test group. For research, the scope is essential to find results from participants with different backgrounds. The key idea of the evaluation tool is to provide a tool for SaaS security evaluation and non-technical persons.

1.6 Research Ethics

The construction of this thesis adheres to the ethical guidelines prescribed by JAMK University of Applied Sciences (JAMK, 2018), ensuring the utmost integrity and ethical conduct in the research process. By these guidelines, the author has diligently utilized publicly available sources to gather the information presented within this thesis. It is imperative to emphasize that this thesis does not contain confidential or proprietary information about the company under study nor any sensitive details related to the organization’s security solutions.

By the established academic and ethical practices, all references and original data included in this thesis are meticulously cited and documented, strictly following JAMK's reporting guidelines (JAMK, 2020). This meticulous referencing is a testament to the author's commitment to upholding academic integrity and ensuring transparency in utilizing external sources and empirical data.

Furthermore, it is principal to note that the information derived from interviews conducted with the model's test users has undergone a rigorous anonymization process. Before their inclusion in this thesis, all interview data have been meticulously anonymized, ensuring that the participants' identities remain undisclosed and unidentifiable. This ethical safeguard follows established ethical standards and principles governing research involving human subjects, protecting the privacy and confidentiality of the interviewees.

2 SaaS-Overview

2.1 SaaS Adoption

Cloud service providers offer three main service computing models. The difference between these services is the workload of IT management allocated to the cloud service provider. IBM (*IaaS vs. PaaS vs. SaaS | IBM*, n.d.) article describes the main differences between management models:

- SaaS: All software development and infrastructure management responsibilities are allocated to the cloud service provider. Services like Visma Severa, Slack, Microsoft M365.
- PaaS (Platform-as-a-service): Complete, fully managed cloud-hosted platform. PaaS includes hardware, software, development tools, and infrastructure using an internet connection. This platform suits customers who want to install and develop their applications in a scalable environment. Services like Amazon Elastic Beanstalk, Heroku
- IaaS (Infrastructure-as-a-service): Cloud-hosted compute, network, and storage resources on a pay-by-usage model. The suitable alternative of the on-premises data center for highly variable or seasonable workloads. Allow customers to own control of the application and platform. IaaS services are available from multiple service providers, for example, Amazon Web Services (AWS) and Rackspace.

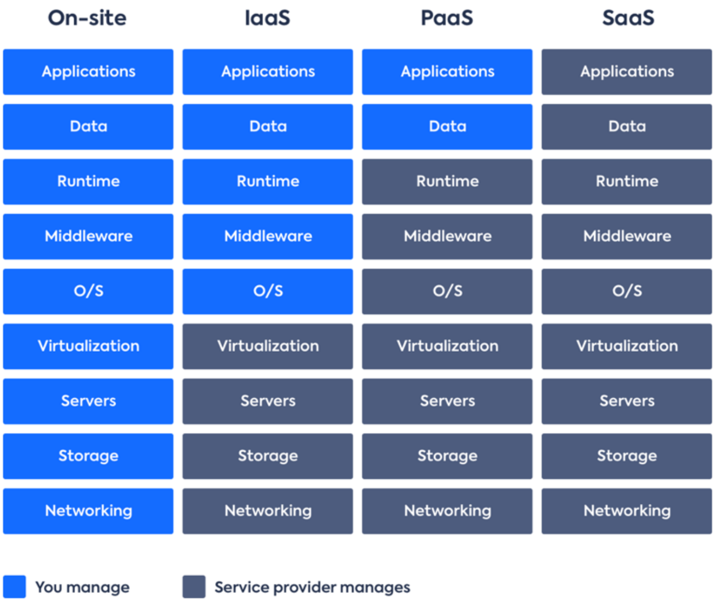


Figure 1 Level of vendor management differences between IaaS vs. PaaS vs. SaaS (G. LeanIX, 2021)

SaaS services started in 1999; then, Salesforce rolled out customer relationship management (CRM) service with web browser access. (*SaaS – Software-as-a-Service | IBM*, n.d.). SaaS services are the most popular public cloud computing service, providing daily applications like Microsoft M365 or Slack. IDC's report (Staff, 2022), the SaaS application market has grown fast over the past decade. SaaS application revenue will grow 15.3% from 2022 to 2025 and will be $302 billion by 2025. In the year 2022, the SaaS model will have a 60 % amount of cloud software markets.

According to information technology publications, SaaS services can provide operational and financial benefits for organizations. However, SaaS services can include vulnerabilities because there are some limitations, like lack of control. Oliveira et al. researched SaaS adoption using the technology-organization-environment (TOE) -model (Oliveira et al., 2019).

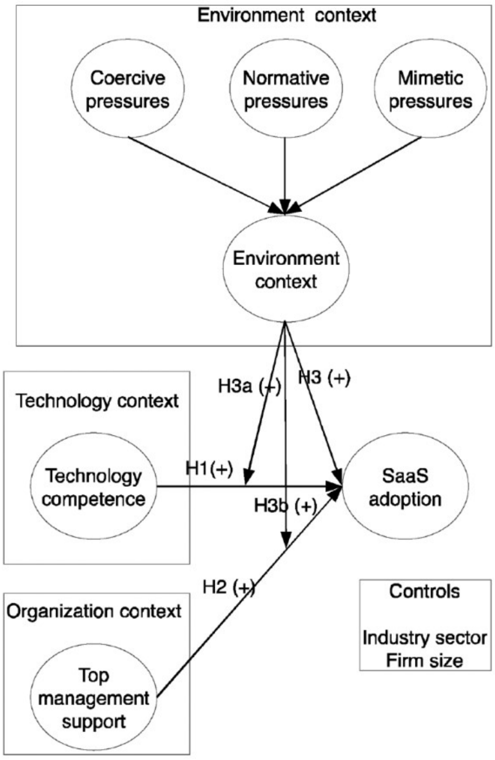


Figure 2 TOE model describes which factors affect SaaS adoption (Oliveira et al., 2019).

Oliveira’s research key finding is that companies are not ready for cloud computing; they need to learn how cloud services could help their business and get more technical knowledge to evaluate these aspects:

- What kind of capitalistic benefits will cloud shift provide their business?
- On how to manage the procurement of cloud services.
- How to arrange cloud services management

The company's decision-makers need to evaluate the required technical skills for their organization to adopt SaaS. Resources are needed to integrate SaaS into its IT infrastructure; these can be from a service provider or in-house. Communications infrastructure to the cloud should be suitable, like enough fast Internet connection.

Rahman & Subriadi researched SaaS adoption factors from individual and organizational perspectives (Rahman & Pribadi Subriadi, 2022) and found twenty-five influential factors from individuals; the most important were the ease of use, social influence, and perceived usefulness of the software. On the other hand, they found thirty-four factors from an organizational perspective, top management support, and IT readiness were the critical factors of SaaS adoption of the organization. They have tried to provide a guideline for SaaS adoption.

SaaS adoption will change the company's environment, and it is not isolated to some parts of services. The company needs to take care of integrations to the legacy IT infrastructure to avoid problems. SaaS adoption should link to the organization’s daily operations and intend top management for the integration project.

The environment around the company will provide particular elements of SaaS development. (Yang et al., 2015) These elements put pressure on the company, which is linked to other actors:

- formal regulators
- shared information and needs from suppliers.
- governmental agencies
- modeling the same kind of companies, including competitors

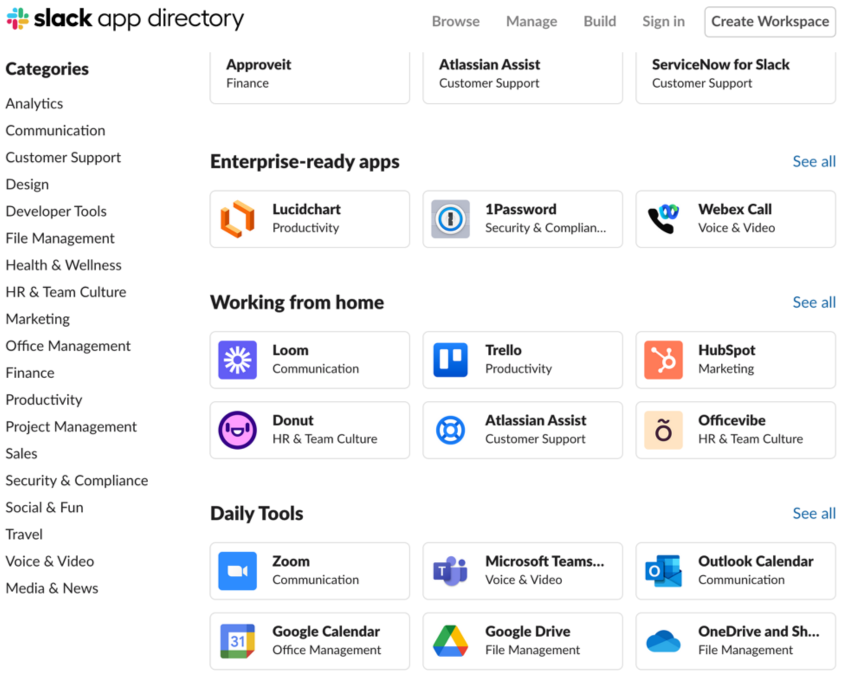
The environment varies between companies, depending, for example, its business area or customer's needs. Managers will use these models in their decision-making when organizations' SaaS readiness. Technological, organizational, and environmental factors were the research's most signifiable influencers in the SaaS adoption (Oliveira et al., 2019). Environmental directly affect SaaS adoption and rule the connection between technology. When an organization's technical knowledge is higher, the company will enable new technology more efficiently.

2.2 Third-Party Connected Apps

Many SaaS services have marketplaces for third-party application integrations. These integrations provide critical functions to business collaboration platforms for providing text chatting and third-party resource integration. Integrations allowed users to access multiple resources from the leading portal like document sharing or video calls (Chen et al., 2022).

Third-party app rights are access rights to the leading SaaS service controlled by access permission limitations, which the user will approve during the installation of the app for a workspace. The user has no option to verify, for example, the app's source code. According to the audit of (Chen et al., 2022), hundreds of apps have the potential right to post a message as a user, hijack the functionality of other valid apps, or access data in private channels without permission. These functionalities will provide security and privacy issues to the platform. (Greenberg, 2022)

Slack is US based instant messaging service, that recommends installing only approved apps from their app stores (Greenberg, 2022), and organization administrators should limit permissions to who has the right to install apps. However, there are severe issues with the pre-audit process of apps. Apps are located on the developers' server so that someone can change applications after the audit process. After the change, the harmful app is malicious; this code change can happen during the development process or by hackers in the solution providers' delivery chain. App store providers must include code reviewing in the collaboration platform's app store audit process. Users are used to trusting audited applications delivered to mobile devices using Apple's App Store and Google Play, so many assume the situation is the same with all app stores.



slack app directory

Browse Manage Build Sign in Create Workspace

Categories

Analytics
Communication
Customer Support
Design
Developer Tools
File Management
Health & Wellness
HR & Team Culture
Marketing
Office Management
Finance
Productivity
Project Management
Sales
Security & Compliance
Social & Fun
Travel
Voice & Video
Media & News

Approveit
Finance

Atlassian Assist
Customer Support

ServiceNow for Slack
Customer Support

Enterprise-ready apps See all

Lucidchart
Productivity

1Password
Security & Complian...

Webex Call
Voice & Video

Working from home See all

Loom
Communication

Trello
Productivity

HubSpot
Marketing

Donut
HR & Team Culture

Atlassian Assist
Customer Support

Officevibe
HR & Team Culture

Daily Tools See all

Zoom
Communication

Microsoft Teams...
Voice & Video

Outlook Calendar
Communication

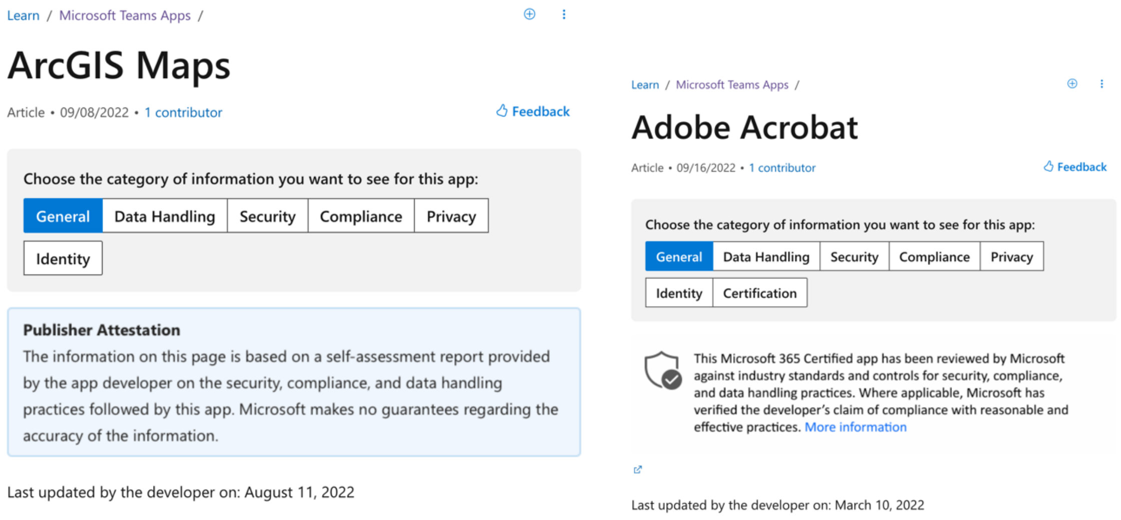
Google Calendar
Office Management

Google Drive
File Management

OneDrive and Sh...
File Management

Figure 3 Slack app directory main page (Slack, n.d.)

Microsoft has a validation guideline for Teams store (heath-hamilton, 2023) that includes guidelines and requirements of the application to be allowed to publish to their store. App developers must follow these guidelines to provide end-users a solid user experience, including App naming, compatibility, response time, and other user experience-related content. The next step of the App approval process is the compliance program. There are two types of compliance checks; the most common is Publisher attestation, where the app developer answers more than 80 risk factors identified by Microsoft Defender (Microsoft, 2023). Teams' admins can check attested apps from the Teams app security and compliance page or Teams admin panel. Microsoft also has a 365 certification program, where Microsoft verifies apps against industry-standard frameworks. The application will be marked with the Microsoft 365 Certified app -icon if it passes Microsoft's certifications certification, which helps Teams admin to workload when Microsoft pre-audits applications. Microsoft offers this certification free of charge, and Microsoft recommends that the app publisher if a publisher, has appropriate resources for delivering the documentation needed to comply with the audit.



Learn / Microsoft Teams Apps /

ArcGIS Maps

Article • 09/08/2022 • 1 contributor

Feedback

Choose the category of information you want to see for this app:

General | Data Handling | Security | Compliance | Privacy | Identity

Publisher Attestation

The information on this page is based on a self-assessment report provided by the app developer on the security, compliance, and data handling practices followed by this app. Microsoft makes no guarantees regarding the accuracy of the information.

Last updated by the developer on: August 11, 2022

Learn / Microsoft Teams Apps /

Adobe Acrobat

Article • 09/16/2022 • 1 contributor

Feedback

Choose the category of information you want to see for this app:

General | Data Handling | Security | Compliance | Privacy | Identity | Certification

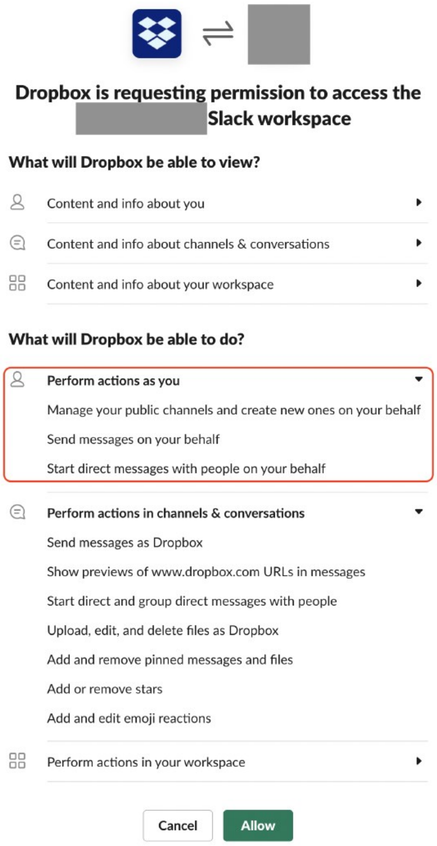
This Microsoft 365 Certified app has been reviewed by Microsoft against industry standards and controls for security, compliance, and data handling practices. Where applicable, Microsoft has verified the developer's claim of compliance with reasonable and effective practices. More information

Last updated by the developer on: March 10, 2022

Figure 4 Example of Microsoft Teams Apps Publisher Attestation and 365 Certified app includes information on the application provider's security, compliance, and data handling practices followed by the app. (elenamalova, 2022)

A single user can approve a new application for the entire organization if not restricted by the organization's application security policy and settings. Currently, the default setting of platforms like Slack allows everyone to install hosted apps independently. The company admin can change this setting, but platform providers must actively inform how significant this change is.

The user will approve access permissions to the organization's data during the app's installation process. These permissions might violate the minor access security policy so that the app will ask for more access permissions than its operational needs. The user or administrator will approve apps, and there is no option to limit access to only part of the organization. So, for example, the same application will get access to office jokes-channel and finance-departments information. Apps might get too broad permissions, like the ability to post as a user, which can allow the use of an app for phishing purposes. Applications might have access to company code repositories, and the app might get access to change the code of the software.



[redacted]

Dropbox is requesting permission to access the [redacted] Slack workspace

What will Dropbox be able to view?

- Content and info about you
- Content and info about channels & conversations
- Content and info about your workspace

What will Dropbox be able to do?

Perform actions as you

- Manage your public channels and create new ones on your behalf
- Send messages on your behalf
- Start direct messages with people on your behalf

Perform actions in channels & conversations

- Send messages as Dropbox
- Show previews of www.dropbox.com URLs in messages
- Start direct and group direct messages with people
- Upload, edit, and delete files as Dropbox
- Add and remove pinned messages and files
- Add or remove stars
- Add and edit emoji reactions

Perform actions in your workspace

Figure 5 Installing Slack apps with user scopes. (Chen et al., 2022)

Researchers recommend (Greenberg 2022) changes to the app store model to fix fundamental security issues. Solution providers should audit the apps' code in more detail and monitor code changes. The app store should enforce application permission minimization and add the possibility of restricting app access to only part of the organization's data.

The SaaS security management solution provider Adaptive Shield researched connections between SaaS and another Service provider (Adaptive Shield, 2023). These connections consist of when a user connects, for example, Microsoft 365 or Slack, to another product. IT security team needs more visibility of these connections because operations increase security risk. These connections will be authorized user access requests; requests like editing files, sending emails, or accessing the data may grant permissions. Most users need to learn whether these permissions are malicious or valid. Workplace product like Microsoft 365 does not include the risk definition of the requested operation, so the IT security team needs help creating suitable security policies.

Adaptive Shield evaluated over 200 organizations in 2022; organizations represented multiple industries, like financial services, retail, and healthcare. They found that organizations with 10,000 – 20,000 users have about 3,500 integrated SaaS apps.

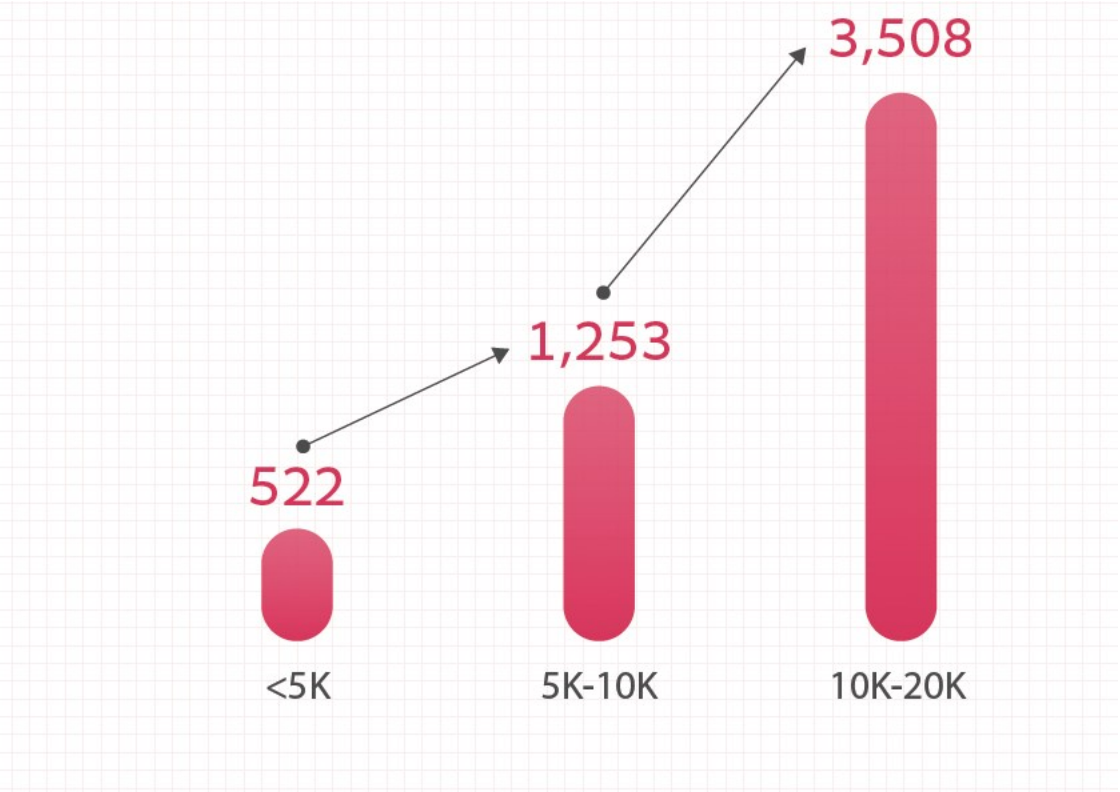


Figure 6 Average number of SaaS apps integrations into Microsoft 365 comparing company size (Adaptive Shield, 2023)

There are options to categorize SaaS integration permission by severity. Google Workspace has a built-in classification, from High to Low, and For Microsoft 365, there are third-party tools for classification. It is recommended to identify the IT security team at least all high-risk classified integrations and set up suitable policies. Some organization-specific restrictions for compliance scores might also exist, like standard ISO 27001 or GDPR needs.

3 Security

Cloud services provide many advantages, like cost-reduction, scaling, and efficiency, instead of on-premises solutions. Some tough security questions still slow customers from moving their services to the cloud. Security is the primary need for cloud services. Systems are provided over the Internet so that cloud providers will affect attacks like Denial of Service (DoS) or SQL injection (Hawedi et al., 2018). The DoS and DDoS attacks affect the service's availability and performance because of these consuming service resources, like memory, CPU resources, and network bandwidth.

SaaS service security risks can be divided into two parts because of shared responsibility. The SaaS provider is responsible for hosting the application, security of the solution, development, and maintenance. The customer organization's responsibilities are controlling its data, application management, and customization management (Elena Preci, 2022).

3.1 SaaS Service Security Issues

In SaaS environments, clients depend on providers for proper security measures, making it difficult for the user to ensure the appropriate security measures and to get assurance that the application will be available when needed. The review (Subashini & Kavitha, 2011) highlights that SaaS providers use data centers’ shared capacity, which can cause discomfort for some companies used to traditional on-premises models. Data breaches, application vulnerabilities, and availability concerns can lead to financial and legal liabilities.

There are many key security elements to consider when ensuring enterprise data security. There are elements such as data security, network security, data locality, data integrity, data segregation, data access, authentication, and authorization. These elements should integrate into the development and deployment processes of SaaS applications. The review emphasizes the importance of implementing proper security measures to mitigate risks and ensure enterprise data protection in SaaS environments.

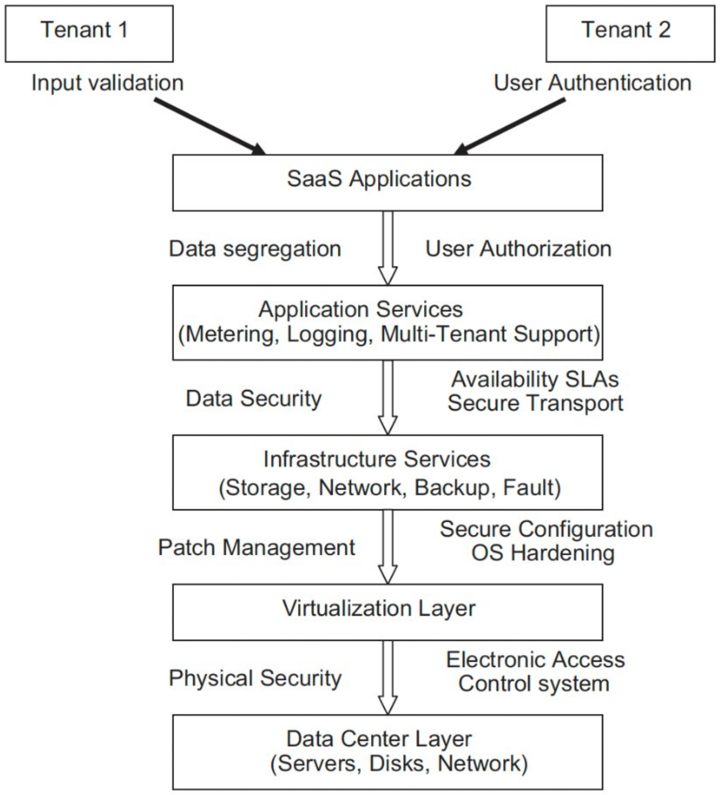


Figure 7 Security of SaaS stack (Subashini & Kavitha, 2011)

Data Security

One of the primary concerns with SaaS services is data security (L. LeanIX, n.d.). The data stored in SaaS applications may include sensitive financial numbers, customer information, and proprietary data. Any breach of this data can result in severe consequences for the organization and its clients. Therefore, SaaS providers must implement adequate measures to secure their customers' data (Subashini & Kavitha, 2011). That data includes four parts: usage data, sensitive information, personally identifiable information, and unique device identities.

Authentication and authorization

Another critical security issue associated with SaaS services is the potential for unauthorized access to data. SaaS applications are typically accessed over the Internet, which means that they are vulnerable to attacks from cybercriminals who may try to steal or manipulate data. Therefore, SaaS providers must implement strict authentication and access control mechanisms to access authorized data-only users (Subashini & Kavitha, 2011).

Network Security

It is essential to secure data flow over the network in a SaaS deployment model (Subashini & Kavitha, 2011) to prevent the leakage of sensitive information. Research recommends using solid network traffic encryption techniques such as SSL and TLS. For example, Amazon Web Services (AWS), the network layer, has robust security solutions against traditional network security issues, and storage content is available using an SSL-encrypted connection. Attackers can exploit weaknesses in network security configuration to sniff network packets that organizations can mitigate using network security assessments to test and validate the security of the SaaS vendor.

Backup

Backup is essential to securing the organization's data, and solution providers should ensure backup functionality to enable quick recovery in case of disasters. Encrypting the backup data prevents to avoid data leakage.
Assessments must be carried out on insecure storage and configuration to ensure the security of data backup and recovery services of SaaS services.

Data Availability and Data Loss

Data availability is another significant security concern for SaaS services. If a SaaS provider experiences a service disruption or outage, users may lose access to their data, which can cause significant business disruptions.

Data Loss includes accidental data deletion and leakage. The customer has a different visibility and control of their data than traditional services. Severe data loss will cause financial and legal impacts and reputation impacts. Data loss can occur for many reasons; the most common cause of data loss is the accidental deletion of data by the user (Spanning Cloud Apps, n.d.). Other reasons can be the programmatic error of the app or administrative error.

The Main SaaS service provider has suitable disaster recovery solutions, like protecting against hardware or software failures, power issues, or other disasters. However, services do not include customer data backup in cases of the most common causes of data loss, like user error, malware, or ransomware attacks. Data loss can affect the cost when processing data recovery plans, restoring data from backups, investigating the reason for the issue, and other compensations. For example, restoring companies' repositioning to their customers will take time and effort. EU GDPR can affect fines for violations.

Data Integrity

Data integrity is crucial for any system, including SaaS services. Data integrity can be maintained through database constraints and transactions that follow the ACID properties (Subashini & Kavitha, 2011) in a single database. However, data integrity is more complex in distributed systems like SaaS applications. Many SaaS applications include multiple tenants and applications hosted by a third party, linked through XML-based Application Programming Interfaces (API). API is crucial for connecting applications and data. Insecure APIs are a growing threat; Forrester estimates API breaches are becoming increasingly common and imminent (*The Threat of Insecure Interfaces and APIs*, n.d.). API with missing access or permission control can cause access to unauthorized data.

Services move from SOAP API, typically accessed using VPNs or encrypted connections, to REST APIs. REST API is designed to access other services using a browser or app. It should have least-privilege access and server-side data validation to provide a secure API connection. The organization should define API security measures like verification of any client-supplied data. On-premises applications expose their functionality in API-based web services. The lack of integrity controls at the data level or bypassing the application logic to access the database directly could result in profound problems.

Web application security

Web application security is a complex and constantly evolving field; it is a significant concern for SaaS, as security holes in web applications can create vulnerabilities for SaaS applications. Verizon Business report (Verizon, 2023) showed that web applications are the most attacked targets using different techniques like using stolen credentials to exploit vulnerabilities or brute force. Customers must trust the SaaS provider's skills and process effectiveness. During the purchase process, verify the provider’s vulnerability management skills, such as security training and security in application design. SaaS providers must be aware of The Open Web Application Security Project's

Top 10 (*OWASP Top Ten | OWASP Foundation*, n.d.) security risks and security issues when developing and maintaining their web applications:

- *Injection attacks: Injection attacks, such as SQL injection and cross-site scripting (XSS), are a common way for attackers to exploit vulnerabilities in web applications and gain access to sensitive data.*
- *Broken authentication and session management: Weaknesses in authentication and session management can allow attackers to hijack user accounts and gain access to sensitive data.*
- *Insufficient access controls: Improper access controls can allow unauthorized users to access sensitive data or perform actions they should not be able to.*
- *Insecure communications: Unencrypted or improperly encrypted communication channels can allow attackers to intercept sensitive data.*
- *Security misconfigurations: Misconfigured security settings, such as incorrect file permissions or improperly configured firewalls, can create security vulnerabilities.*
- *Poor input validation: Failure to properly validate user input can allow attackers to execute malicious code or perform actions they should not be able to.*
- *Lack of monitoring and logging: Inadequate monitoring and logging can make detecting security incidents challenging or identifying the source of attacks.*

Overall, SaaS providers must be vigilant in addressing these and other web application security issues to ensure that their customers' data remains secure and confidential. Regular security testing, monitoring, and patching can help mitigate the risks associated with web application security.

3.2 How to mitigate SaaS security issues

SaaS services have limitations in security because services are provided over the Internet. The third part of the security issues can be the connection of service to customers' security processes and reporting. Gartner predicts that customer fault will be linked to most cloud security issues in 2025(GmbH, n.d.). So, lifecycle management (central management and monitoring of cloud products) is essential for security processes in multi-provider environments. Gartner also predicts that most organizations have issues monitoring and measuring the security risk of cloud services. The risk management strategy should be correctly aligned with the organization's cloud strategy to help decisions where usage of the public is suitable. Gartner’s third prediction tells that in 2025, 90 % of organizations will have issues with public cloud management, and sensitive data will be shared without approved rules. Organizations have cloud strategies, but cloud usage will grow faster, exposing unnecessary risks when the strategy is not current.

Risk management practices

Organizations should have risk management practices in place to help with the decisions of cloud projects. There are always risks with public cloud services, but the organization should try to mitigate the risk according to their needs and budget. Public cloud risk management can be divided into five parts (Kasey Panetta, 2019):

- *Agility: Define cloud providers' development for future needs*
- *Availability: Service availability in case of disruptions and data loss.*
- *Security: Evaluate confidentially and data control*
- *Supplier: service providers' possible changes, for example, business model*
- *Compliance: legal and regulatory requirements*

According to these risk management parts, evaluating the risk to benefits is possible when selecting a suitable cloud solution. Risk management provided by the IT department will guide business units' decisions when selecting new solutions. Accepting the cloud risk needs to be considered as a business decision.

SaaS applications Discover and Documentation

Implementing a comprehensive SaaS discovery and documentation process enables organizations to identify, manage, and optimize their SaaS portfolio (LeanIX Gmbh, 2023). Critical steps in the discovery process include:

- Internal survey: Conduct an internal survey to gather information from employees about the SaaS applications they use. This survey information will help to find shadow IT and unauthorized applications.
- Network monitoring: Utilize network monitoring tools to analyze network traffic and identify SaaS applications in use.
- Cloud Access Security Brokers (CASBs): Implement CASBs to gain visibility into cloud applications and monitor usage across the organization.
- Documentation Best Practices

When an organization has discovered SaaS applications, it should document and maintain an inventory of them. Best practices for SaaS documentation include:

- Application inventory: Create a centralized list of all SaaS applications, including application name, provider, version, and purpose.
- License information: Document the license information for each application, including the number of licenses, subscription costs, renewal dates, and terms of use.
- Data classification: Identify the types of data stored, processed, or transmitted by each application and classify the data according to its sensitivity and regulatory requirements.
- Access controls: Document the access controls in place for each application, including user roles, permissions, and authentication mechanisms.
- Integration and dependencies: Identify any integration points or dependencies between SaaS applications and other systems within the organization.

With a comprehensive SaaS discovery and documentation process, organizations can implement strategies to manage their SaaS portfolio effectively. Key strategies include:

- Establish governance: Develop and enforce policies defining the criteria for SaaS application selection, approval, and ongoing management.
- Regularly review and update documentation: Organizations should review and update the SaaS documentation to ensure that it remains accurate and add, modify, or decommission applications.
- Optimize SaaS spending: Analyse SaaS spending patterns, identify unused or underutilized licenses, and consolidate applications where possible to reduce costs.
- Enhance security and compliance: Continuously monitor and assess SaaS applications' security and compliance posture, ensuring they adhere to organizational policies and regulatory requirements.
- Encourage collaboration and communication: Foster a culture of collaboration and communication within the organization to ensure employees know approved SaaS applications and their associated benefits, fostering better adoption and usage.

SaaS discovery and documentation are essential for organizations seeking visibility and control over their cloud application landscape. Organizations can optimize their SaaS portfolio, enhance security, and ensure compliance by implementing a robust discovery process, maintaining accurate documentation, and adopting effective SaaS management strategies. As SaaS adoption grows, organizations should continue to refine and adapt their discovery and documentation processes to stay ahead of evolving challenges and opportunities.

Employee Training and Awareness

Employee training and awareness programs are crucial in minimizing SaaS security issues (Paddle, n.d.). Organizations should:

- Provide regular security awareness training to educate employees about potential risks, best practices, and their responsibilities in maintaining the security of SaaS environments.
- Conduct targeted training for employees with specific roles in managing and using SaaS applications, such as administrators and developers.
- Implement ongoing reinforcement strategies, such as security newsletters, reminders, and periodic assessments, to ensure employees remain aware of security best practices.

Third-party risk management

Evaluate internal processes and operations of new SaaS providers to mitigate security risks from a third-party provider. The solution provider typically provides standard format documentation, like ISO certification or security audit documentation. These documents provide part of the provider's security processes. The missing piece might include the provider’s internal documentation, like business continuity or backup plans. This missing documentation will dilute understanding of the SaaS provider’s risk to the organization.

Identity and Access Management (IAM) Controls

Identity and Access Management (IAM) Controls implementation is essential for preventing unauthorized access to SaaS data. Unauthorized access can be done using the organization’s compromised accounts or brute force attacks. SaaS services are located on the Internet and provide services worldwide, so geographic or IP restrictions are not expected. Improving authentication and authorization procedures of SaaS service should be evaluated by customer organizations. Single sign-on (SSO) solutions and enforced multifactor authentication (MFA) are efficient methods for authentication security.

Shadow IT

Shadow IT is a practice where some purchase or uses IT systems, software, or SaaS service that the organization's IT department does not approve. SaaS services are easy to purchase and use as shadow IT; the employee needs a new tool to improve his work and use the service instead of tools provided by the company. According to McAfee's study, 80 % of employees have used shadow IT solutions (G. LeanIX, n.d.). Individuals purchase 50 % of SaaS services now, the organization procures 35 %, and only 15 % are ordered by IT departments. There are multiple risks of shadow IT:

- Security issues: There is the possibility of data leak from undocumented application
- Noncompliance: Undocumented services are not compliant
- Configuration management: shadow IT is missing from CMDB
- Collaboration issues: Communication can be inefficient when an organization has multiple services
- Lack of visibility: The IT department cannot help with undocumented apps

Backup data in several locations

SaaS services have backup functionality as standard (Paddle, n.d.). Multi-location backups play a crucial role in safeguarding business data in SaaS environments. Storing backups in multiple locations can significantly reduce the risk of data loss due to natural disasters, hardware failures, or human errors. As the adoption of SaaS services grows, businesses must prioritize robust backup strategies, including multi-location backups, to protect their valuable data and maintain operational resilience.

Data Encryption

SaaS services use data encryption to protect sensitive data from unauthorized access. Cloud applications have no protection using traditional methods, like firewalls (Polar Security - 8 Data Security Best Practices for SaaS Applications, n.d.). Data encryption involves encoding data so that only authorized parties can read it. One way to achieve this is by using private, unique, and secret cryptographic keys to encrypt and decrypt data.

Using private keys for data encryption provides several benefits. First, private keys are more secure than passwords, as they are longer and more complex, making them harder to crack. Second, private keys can encrypt and decrypt data without needing a third-party service, reducing the risk of data breaches. Finally, private keys allow more granular control over data access because data is encrypted using different keys for different users or groups.

There are also some negative aspects of private keys that need to be taken care of before proceeding (Pilgrim, 2022). Private keys might affect service performance when encryption requires separate processing. Service owners should define the management of the private keys very accurately using a dedicated key management policy or system. The key management system will minimize the risk of losing the security keys and access to the encrypted data.

Use a Key Vault Service

Key vault services help organizations securely store and manage encryption keys, secrets, and certificates (Nimrod Iny, 2022). Key benefits include:

- Centralized key management, simplifying key rotation, and reducing the risk of key compromise.
- It enhanced access control and auditing capabilities for improved security and compliance.

Logging and Monitoring

A centralized logging and monitoring system, typically Security information and event management (SIEM), allows continuous monitoring and logging of SaaS environments. It is crucial for maintaining security and detecting potential incidents. Organizations should:

- Implement logging and monitoring solutions that provide visibility into user activity, access patterns, and potential security events.
- Regularly review logs and alerts to identify and address potential security incidents.

3.3 Security Standards

Most smaller organizations have no resources and competence to evaluate SaaS providers’ security processes. Security standards like ISO 27001 and CTA STAR can help demonstrate a provider's commitment to security and help businesses evaluate their security capabilities. Here are listed the essential security standards that can assist companies in making informed decisions about choosing a SaaS provider.

International standards provide a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Standards guide organizations to secure information assets, including sensitive data, from unauthorized access, disclosure, and modification. For example, a provider certified for ISO27001 compliance has been audited and verified to meet the standard's requirements, which includes a rigorous assessment of their security policies, procedures, and controls. By choosing an ISO27001-certified cloud provider, businesses can be confident that their sensitive data is being handled and secured consistently with internationally recognized best practices. Ultimately, these standards can help companies mitigate risks and ensure the security and confidentiality of their data.

Researchers Tang and Liu have evaluated in their paper (Tang & Liu, 2015) coverage of most adopted standards, such as ISO27001, NIST SP800, CSA CCM, and PCI DSS. They tried to create a holistic SaaS security risk management model with four significant parts: Function, Auditability, Governability, and Interoperability (FAGI). These parts are selected to cover four aspects: security functions of SaaS providers meet the organization’s security needs, security capabilities can be verified using an independent auditor, transparency of security information, and how easy it is to transfer data from one service provider to another. Of course, every SaaS program has a different function and risk profile, so all needed controls are needed for every solution. This kind of vendor governance model can be suitable for some organizations.

3.3.1 ISO 27001

The ISO 27001 standard is an internationally recognized framework that outlines the best practices for implementing an Information Security Management System (ISMS) (ISO Org, 2022). It provides a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system. The standard covers a wide range of security controls and risk management practices, making it a valuable tool for evaluating the security of a SaaS service.

Critical elements of ISO 27001 include:

- **Risk assessment:** Organizations must conduct regular assessments to identify and prioritize information security risks.
- **Risk treatment:** Organizations must implement appropriate measures to mitigate identified risks.
- **Controls:** ISO 27001 includes 114 controls across 14 domains, providing a comprehensive set of best practices to manage information security risks.
- **Continuous improvement:** Organizations must regularly review and update their ISMS to ensure its effectiveness and adapt to changes in the security landscape.

When evaluating the security of a SaaS service, the evaluator should assess whether the service meets ISO 27001 requirements:

Review the service provider's ISO 27001 certification: The service provider should be able to provide evidence of their ISO 27001 certification; this can be done by reviewing their certificate or obtaining a copy of their certification report. It is essential to understand the scope of the certification, which should include the services the provider offers to the customer, to ensure that it covers the SaaS provider's relevant services, infrastructure, and data processing activities.

Review the risk assessment and treatment process: The service provider should have a documented risk assessment process that identifies and evaluates the risk of the information security management system. The risk treatment process should outline the measures taken to mitigate those risks.

Review the security controls implemented by the service provider: The service provider should have implemented a set of security controls appropriate for the risks identified in the risk assessment. These controls should cover various areas, such as access control, incident management, and business continuity management.

Review the security incident management process: The service provider should have a documented security incident management process that outlines the steps during a security incident.

Review the service provider's compliance with legal and regulatory requirements: The service provider should have processes to ensure compliance with legal and regulatory requirements related to information security.

By following these steps, businesses can ensure that the SaaS service they consider meets ISO 27001 requirements and has appropriate security controls to protect their data and systems. ISO 27001 certification is part of a comprehensive security evaluation process. Other factors, such as the provider's track record and reputation, should also be considered when evaluating the security of a SaaS service.

3.3.2 Cloud Security Alliance

Cloud Security Alliance (CSA) STAR (STAR, n.d.) certification program offered by the Cloud Security Alliance provides a way for cloud service providers to demonstrate their security compliance to potential customers. The CSA is a non-profit organization that promotes best practices for secure cloud computing. The program includes a set of rigorous security controls to achieve certification.

There are two levels of certification in the CSA STAR Certification program:

The CSA STAR Self-Assessment is a free self-assessment questionnaire that cloud service providers can use to evaluate their security practices. The questionnaire includes a set of over 100 security controls based on the CSA's Cloud Controls Matrix (CCM). For providing needed documents to CSA’s registry, the service provider will receive a Compliance Mark, valid for one year. Service providers can use Compliance Mark to demonstrate the provider's security compliance for potential customers.

The CSA STAR Certification: This formal certification program based on the CCM requires an independent third-party auditor to evaluate the cloud service provider's security practices. The auditor will determine the provider's security controls in data protection, vulnerability, and incident management. Once certified, the cloud service provider can display the CSA STAR Certification logo to demonstrate their security compliance to potential customers.

The CSA designed the STAR Certification to provide transparency and accountability in cloud service provider security. By achieving certification, cloud service providers can demonstrate their commitment to implementing and maintaining strong security controls. The certification process can help businesses make more informed decisions when selecting a cloud service provider. The CSA STAR Certification program also offers several other resources and initiatives to help businesses ensure the security of their cloud computing environments. These include the Cloud Controls Matrix, the Consensus Assessments Initiative Questionnaire, and the Security, Trust & Assurance Registry.

In conclusion, the CSA STAR Certification program is a valuable resource for businesses evaluating cloud service providers. By providing a set of rigorous security controls and a formal certification process, the program helps ensure that cloud service providers are implementing and maintaining strong security practices. The CSA STAR certification can help businesses make more informed decisions when selecting a cloud service provider and improve overall security in the cloud computing environment.

3.3.3 NIST SP800-53

NIST SP800-53 is a set of security controls and guidelines developed by the National Institute of Standards and Technology (NIST) (NIST, 2020) to help federal agencies in the United States protect their information and information systems. The policies cover various security topics, including access control, incident response, and system and communications protection. NIST SP 800-53 is a comprehensive document with 20 control families, over 1000 controls, and many pages (Vincent van Dijk, 2022). It is only a guide that helps organizations tailor controls to their needs.

When evaluating the security of a SaaS service, NIST SP800-53 controls can ensure that the service provider has implemented appropriate security controls to protect the data and systems of their customers.

There is no formal certification for NIST SP800-53 compliance; it is a somewhat customizable security standard. NIST SP800-53 full compliance is challenging to measure, but there is an available certification for full (Federal Information Security Management Act) FISMA compliance. FISMA compliance is a much deeper certification for organizations that operate with US Federal Agencies.

For the service provider, certification can help demonstrate their commitment to security and provide a competitive advantage in the market. The certificate assures the customer that the service provider has implemented appropriate security controls and procedures to protect their data and systems. NIST framework is compatible with the ISO 27001 framework but more flexible and doesn’t have a certification path. Traficom’s Cyber meter has connectivity with NIST framework, but NIST framework is now widely used in EU area (*Viitekehyksiä parempiin tietoturvallisuuskäytäntöihin*, 2022).

4 Privacy

Using SaaS services, personal data is processed, and principles are taken care of when evaluating a suitable service provider for the organization. Selecting the right Software as a Service (SaaS) provider that adheres to GDPR principles is crucial for businesses. Organizations build their data Security using technical measurements that secure information and systems. Data protection safeguards subjects' rights when personal data is processed. Data protection defines when and under what conditions personal data can be processed (*Data Protection | Data Protection Ombudsman’s Office*, n.d.).

The General Data Protection Regulation (GDPR) is a regulation that came into effect on May 25, 2018, to protect the privacy and personal data of citizens of the European Union (EU) and the European Economic Area (EEA). It applies to all organizations that collect, process, and store personal data of EU and EEA citizens, regardless of their location. The GDPR aims to give citizens more control over their personal data and to ensure that organizations handle it appropriately.

GDPR has positively impacted the software industry by forcing companies to focus on data privacy and security (Thais Santos Araujo, 2023). This has made the software industry more transparent and accountable to its users. However, the GDPR has also created some challenges for software companies, such as the increased compliance costs and the need to adapt to new requirements.

One of the most significant impacts of the GDPR on the software industry has been the increased focus on data privacy and security. Software companies must now have robust measures to protect the personal data they collect and process. This includes implementing technical and organizational security measures and having clear and transparent data privacy policies.

The increased focus on user consent is another significant impact of the GDPR. Software companies must now obtain explicit consent from users before collecting or processing their personal data. This has required many software companies to change the way they collect and use cookies, as well as the way they market their products and services.

The GDPR has also had an impact on the way software companies transfer personal data outside the EU. Software companies that transfer personal data outside the EU must ensure that the data is transferred to a country with adequate data protection. If the country needs sufficient data protection, the software company must implement additional safeguards to protect the data.

4.1 Principles of GDPR

The GDPR is a vital regulation that protects the privacy and personal data of citizens of the EU and EEA. The GDPR has critical principles that organizations must adhere to when collecting, processing, and storing personal data. To ensure compliance with the GDPR, organizations must adopt systematic data management that includes data analysis, risk assessment, data protection, and compliance monitoring. By doing so, organizations can ensure that they comply with the GDPR and protect individuals' privacy and personal data.

The GDPR has seven fundamental principles that govern personal data collection, processing, and management. These principles are (*The EU General Data Protection Regulation | IT Governance Ireland Ireland*, n.d.):

- **Lawfulness, fairness, and transparency:** Personal data must be processed lawfully, fairly, and transparently. This principle means providing clear information about how the data will be used and ensuring that it is not processed in a way that violates the individual's rights.
- **Purpose limitation:** Data must be collected for specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data minimization:** Organizations should only collect and process the minimum amount of personal data necessary to achieve their purpose.
- **Accuracy:** Personal data must be accurate, up-to-date, and, where necessary, corrected or deleted immediately.

- **Storage limitation:** Personal data should only be stored for as long as necessary to fulfill the purposes for which it was collected.
- **Integrity and confidentiality:** Organizations must ensure that personal data is processed securely, protecting it from unauthorized access, disclosure, or destruction.
- **Accountability:** Data controllers must comply with GDPR principles and take responsibility for the personal data they process.

To ensure compliance with the GDPR, organizations must adopt a systematic approach to data management. This approach involves:

- **Data analysis:** Organizations must analyse the personal data they collect to identify the purpose for which it is collected and the data necessary to achieve that purpose.
- **Risk assessment:** Organizations must assess the risks associated with collecting, processing, and storing personal data. They must identify potential risks and take appropriate measures to mitigate them.
- **Data protection:** Organizations must implement appropriate measures to protect personal data. Data protection measures include encryption, access controls, and regular backups.
- **Compliance monitoring:** Organizations must monitor their compliance with the GDPR to identify areas where they are not compliant and take appropriate measures to rectify the situation.

4.2 Data Transfers

Data transfers are a crucial aspect of many businesses today. However, transferring personal data outside the EU/EEA area can pose significant risks to the privacy and security of personal data. Therefore, it is essential to have a thorough approach to data transfers to ensure that personal data is protected.

Data Transfers Outside of the EU/EEA Area

When personal data is transferred outside the EU/EEA area, it is subject to different laws and regulations than within the EU/EEA. These laws and regulations may provide extra protection for personal data, which can risk the privacy and security of personal data. Therefore, it is essential to have appropriate safeguards to protect personal data when transferred outside the EU/EEA area.

Legal Basis for Data Transfers

Organizations must establish a legal basis for the transfer before transferring personal data outside the EU/EEA area. Ensuring that a SaaS provider has a legal basis for transferring personal data outside the EU/EEA area is crucial. The most common legal basis for data transfers is (*Rules on International Data Transfers*, n.d.):

- **Adequacy decisions:** The European Commission may determine that a non-EU/EEA country offers adequate data protection, then Data transfers to these countries can occur without additional safeguards.
- **Appropriate safeguards:** If a non-EU/EEA country does not have an adequacy decision, data transfers can still occur if proper safeguards are in place. These may include Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).
- **Standard Contractual Clauses (SCCs):** SCCs are a set of contractual clauses approved by the European Commission. Organizations can use SCCs to ensure that personal data is protected when transferred to a third country that does not provide adequate protection.
- **Binding Corporate Rules (BCRs):** BCRs are internal rules governing personal data transfer within a multinational organization. Relevant data protection authorities must approve BCRs to provide adequate protection for personal data.

4.3 Transfer Impact Assessment (TIA)

When there is no good decision or other appropriate safeguard, organizations must conduct a Transfer Impact Assessment TIA (Grynwajc, 2022) to evaluate the potential risks associated with the transfer. A TIA is a systematic and comprehensive assessment of the risks of transferring personal data. The following are the steps involved in conducting a TIA:

- **Identify Personal Data:** The organization reviews personal data transferred outside the EU/ETA area. This evaluation includes the type of data, the volume of data, and the purpose of the data transfer.
- **Analyze the Legal Framework**: The second step is to analyze the legal framework in the third country to determine if it provides adequate data protection, including analyzing the third country's laws, regulations, and enforcement mechanisms.

- **Assess the Risks**: The third step is to assess the potential risks associated with the data transfer, including unauthorized access, disclosure, or alteration of personal data.
- **Identify Appropriate Safeguards:** The fourth step is identifying appropriate safeguards to mitigate the risks identified in step three; safeguards can include implementing technical and organizational measures to ensure the security of personal data.
- **Document the TIA**: The final step is to document the TIA and the measures taken to mitigate the risks associated with the data transfer.

Conclusion

Transferring personal data outside the EU/EEA area requires a comprehensive approach to protect personal data. Organizations must establish a legal basis for the transfer and conduct a TIA to identify and mitigate potential risks associated with the transfer. By following this approach, organizations can ensure that personal data is protected and compliant with GDPR.

4.4 Privacy check when selecting a solution provider

When selecting a SaaS provider, evaluating their adherence to GDPR principles is essential. EU-funded GDPR. EU service has provided a GDPR checklist for data controllers (*GDPR Compliance Checklist*, n.d.) includes key criteria also for evaluating solution providers. This checklist includes data security, accountability governance, and privacy rights sections.

Organizations should consider these criteria during the decision process according GDPR checklist:

- **Data privacy policy**: The provider should have a clear and transparent privacy policy explaining how they collect, use, and share personal data. The policy should also explain how users can access and control their personal data.
- **Security measures**: The provider should have robust security measures to protect personal data from unauthorized access, use, disclosure, modification, or destruction. These measures should include technical and organizational measures, such as encryption, access control, and regular security audits.
- **Data transfer practices**: The provider should have transparent data transfer practices in place. If the provider transfers personal data outside of the European Union (EU), they must ensure that the data is transferred to a country that has an adequate level of data protection.

- **Compliance with applicable laws and regulations**: The provider should comply with all laws and regulations, including the GDPR.

5 SaaS vendor management tools

A SaaS vendor management tool is a software solution that helps enterprises manage and optimize their SaaS vendors. It provides a centralized platform to track all the SaaS applications, their usage, costs, and security. It also helps negotiate and renew contracts, ensure compliance, and optimize spending. The main benefits of a SaaS Vendor Management Tool for Enterprise are (Calvello, 2020):

Centralized Platform for Management

A SaaS vendor management tool provides a centralized platform for managing all the SaaS applications. This tool makes it easy for the IT department to track usage, monitor costs, and manage contracts. It also helps in identifying redundancies and optimizing spending.

Cost Optimization

SaaS vendor management tools help identify redundant applications and underutilized licenses and help optimize spending and reduce costs. The tool can also help negotiate and renew contracts with vendors, ensuring the enterprise gets the best value for its money.

Enhanced Security and Compliance

SaaS vendor management tools provide enhanced security and compliance features like helping monitor access to SaaS applications and ensure secure access. They also help ensure compliance with GDPR, HIPAA, and SOX regulations.

Better Visibility and Reporting

SaaS vendor management tools provide better visibility into SaaS usage and costs. These systems generate reports and analytics that help identify usage patterns and optimize spending. They also provide insights into application performance, enabling the IT department to identify and resolve issues quickly.

Streamlined Processes

SaaS vendor management tools streamline processes related to managing SaaS applications. They automate contract renewals, license management, and vendor onboarding tasks, save time, and reduce the workload on the IT department.

The SaaS Management Platform market is growing fast during the following years, from USD 113.82 Billion in 2020. Verified Market Research estimates the market to grow to 720 billion by 2028, so the annual growth rate is 27.5%(Verified Market Research, 2022). The most important reason for the market growth is the need to reduce license costs and waste of unused licenses. Also, IT security policies and Environmental, Social, and Governance (ESG) requirements address the needs of control systems. The SaaS Management Platforms are divided into two main segments: large enterprises and SMEs.

5.1 Enterprise-level tools

Larger organizations have resources for comprehensive governance management platform that provides a wide range of tools for managing regulatory compliance, risk management, and data privacy obligations. (Gartner, 2023). Pricing of these solutions varies on the organization's size, starting from thousand euros in months.

For example, the OneTrust platform (*Products | OneTrust*, n.d.) consists of several modules that can be combined to create a comprehensive governance management solution. These modules include:

- **Data Privacy Management**: This module provides tools for managing data privacy obligations, including data mapping, data subject requests, and consent management.
- Vendor Risk Management: This module helps organizations manage the risks associated with third-party vendors by providing tools for vendor assessments, risk scoring, and contract management.
- **Incident & Breach Response**: This module provides tools for managing security incidents and data breaches, including incident response plans and breach notification workflows.
- **ESG & Sustainability**: This module helps organizations manage their environmental, social, and governance (ESG) initiatives by providing tools for tracking sustainability metrics and reporting on ESG performance.
- **GRC Management**: This module provides a centralized platform for managing governance, risk, and compliance (GRC) activities across the organization.

OneTrust is one of the leading solutions in the governance management space (Gartner, 2023), but several alternative solutions are available that provide similar functionality. Some of the most notable alternatives include:

RSA Archer: RSA Archer is a governance, risk, and compliance platform that provides tools for managing various GRC activities, including risk assessments, policy management, and incident response.

ServiceNow GRC: ServiceNow GRC is a governance, risk, and compliance platform that provides tools for managing regulatory compliance, risk management, and audit activities.

MetricStream: MetricStream is a governance, risk, and compliance platform that provides tools for managing various GRC activities, including risk assessments, policy, and audit management.

5.2 SME-level tools

SaaS management platforms benefit small and medium-sized enterprises (SMEs) that may need more resources to manage multiple software applications individually (G2, 2023). SaaS management platforms provide various services, including application discovery, user management, license management, and cost optimization. They can help SMEs to streamline their software management processes, reduce costs, and improve productivity.

One of the main benefits of SaaS management platforms for SMEs is managing multiple applications from a single dashboard. A single dashboard view makes it easier for businesses to monitor application usage, track license renewals, and control user access across all applications. Additionally, some platforms offer automation features that can help businesses save time and reduce the risk of human error.

SaaS management platforms can be a valuable tool for SMEs to streamline their software management processes, reduce costs, and improve productivity. However, it is essential for businesses to carefully evaluate different platforms to ensure they select a solution that meets their specific needs and requirements. Many solutions exist outside the EU/ETA area, so Transfer Impact Analysis should proceed before selecting the service. The SaaS management platform's monthly pricing starts from a few Euros monthly.

Here are listed some key providers of SaaS Operations Management (G2, 2023). Organizations should be carefully the most suitable solution provider for their needs:

BetterCloud is a US-based SaaS management platform that focuses on automating workflows and improving security for cloud-based applications. It offers features like user lifecycle management, automated workflows, security policies, and auditing tools. It integrates with popular SaaS applications like G Suite, Office 365, Slack, and Zoom.

Torii is a US-based SaaS management platform that provides visibility and control over all SaaS applications used within a company. It offers features like discovery and inventory, cost optimization, security policies, and automated workflows. It integrates with over 2,000 SaaS applications, including popular ones like Salesforce, Zoom, and Slack.

Zluri is an Indian-based SaaS management platform that offers various features for managing SaaS applications. It includes features like discovery and inventory, cost optimization, license management, and automated workflows. It integrates with over 1,000 SaaS applications, including popular ones like Google Workspace, Microsoft 365, and Zoom.

6 Evaluation tool structure

A SaaS (Software as a Service) security checklist ensures that an organization's SaaS applications are secure and meet the necessary security requirements. It is essential to regularly evaluate and assess the security of SaaS applications to prevent potential data breaches, cyber-attacks, and other security incidents.

The SaaS security checklist for an organization includes data encryption, authentication, access control, security logging and incident management, and governance.

This SaaS security checklist is a tool for non-technical business users to evaluate the product's security during onboarding. It also enabled documentation history for future needs. As a general note, always consider the organization's specific security needs when assessing SaaS providers, as different organizations may have different requirements based on their size, industry, regulatory environment, and other factors.

6.1 Available models

6.1.1 Enisa

The European Union Agency for Cybersecurity (ENISA)'s Cybersecurity Certification Scheme for Cloud Services (EUCS) (SA, 2020) is a voluntary scheme that aims to improve the security of cloud services in the European Union. The scheme, published in 2021, is based on the Common Criteria (CC) for Information Technology Security Evaluation, an international standard for IT security.

The EUCS offers three levels of assurance: primary, substantial, and high- reflecting the security requirements and assurance levels associated with various cloud services and risk profiles. The level of assurance that a cloud service provider (CSP) chooses to pursue will depend on the specific needs of its customers.

The EUCS covers a wide range of security requirements, including:

- Data protection
- Access control
- Identity and authentication
- Encryption
- Incident response
- Business continuity

The scheme also includes requirements for the CSP's governance, management, and technical controls.

To become certified under the EUCS, a CSP must undergo an independent assessment by a qualified certification body. The assessment will verify that the CSP meets the requirements of the scheme.

The EUCS offers several benefits for organizations adopting cloud services:

- Simplified compliance: By providing a unified set of security requirements, the EUCS simplifies the compliance process for CSPs and reduces the burden on organizations seeking to ensure their cloud services are secure and compliant with EU regulations.
- Enhanced security: The EUCS promotes robust security measures and best practices among CSPs, enhancing security for organizations using certified cloud services.
- Improved decision-making: The transparency provided by the EUCS certification process enables organizations to make informed decisions about their CSPs, ensuring that they select providers that meet their security and compliance needs.
- Facilitated cross-border operations: The EUCS supports cross-border data transfers and operations, making it easier for organizations to expand their business across the EU while maintaining security and compliance.

The EUCS is designed to help organizations decide which cloud services to use. The scheme also provides a way for CSPs to demonstrate their commitment to security. Enisa develops EUCS and expects to finish development in 2023. Enisa opens the EUCS scheme to CSPs from all over the world.

6.1.2 Traficom (PiTukRi)

Traficom (Finnish Transport and Communications Agency) has created Criteria for Assessing the Information Security of Cloud Services (PiTuKri, abbreviated from its Finnish name, Pilvipalveluiden turvallisuuden arviointikriteeristö) to set of security requirements for cloud services by public authorities in Finland. The criteria help organizations ensure that the cloud services meet the national security requirements of Finland. (*Criteria for Assessing the Information Security of Cloud Services (PiTuKri)*, 2019) It was revised at the beginning of 2020 and included criteria from Cloud Control Matrix (CCM), ISO27001 and ISO27017 standards, and Finnish Katakri criteria.

The Pitukri criteria cover a wide range of security topics, including:

- Prerequisites
- Safety management

- Personnel safety
- Physical security
- Telecommunication security
- Identity and access management
- Information system security
- Encryption
- Operational safety
- Portability and compatibility
- Change management and system development

PiTukRi criteria are divided into three levels by Traficom: primary, enhanced and advanced. Cloud service providers (CSP) security must meet to suitable privacy class.

The Pitukri criteria are a voluntary scheme, but CSPs that want to provide cloud services to public authorities in Finland are encouraged to comply with the criteria. The criteria are also a good way for CSPs to demonstrate their commitment to security.

Pitukri criteria's benefits are:

- Help to ensure that cloud services used by public authorities in Finland meet the national security requirements.
- Provide a common framework for evaluating the security of cloud services.
- Help organizations to make informed decisions about which cloud services to use.
- Provide a way for CSPs to demonstrate their commitment to security.

The Pitukri criteria are a valuable tool for organizations looking to improve their cloud deployments' security. The criteria are also a good way for CSPs to differentiate themselves from the competition.

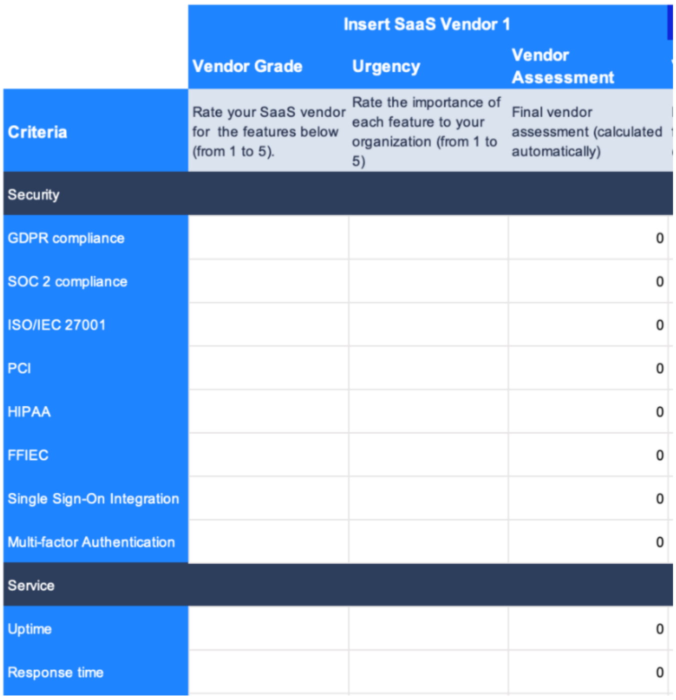
6.1.3 LeanIX

LeanIX is a German software company founded in 2012 that provides a platform for managing and optimizing enterprise IT landscapes. The platform helps organizations track their SaaS applications,

understand their dependencies, and improve their security posture. The company has over 1,000 customers in over 50 countries.
LeanIX has published the SaaS Security Checklist (L. LeanIX, n.d.), a comprehensive list of questions and considerations posed by a company looking to onboard a new SaaS software. It helps the organization assess whether the vendor meets the company's security needs.

LeanIX has divided the checklist into four sections:

- Security: Check service providers' essential security functions, like Single Sign-On and multifactor Authentication, and certifications, like ISO 27001, SOC2 compliance, and GDPR compliance
- Service: Verify the level of service, like Uptime, Response time, support functions, reporting, and dedicated contact person
- Cost: Evaluate license terms, license levels, and pricing
- Service features: Integrations, usage insights, compliance tracking



	Insert SaaS Vendor 1		
	Vendor Grade	Urgency	Vendor Assessment
Criteria	Rate your SaaS vendor for the features below (from 1 to 5).	Rate the importance of each feature to your organization (from 1 to 5)	Final vendor assessment (calculated automatically)
Security			
GDPR compliance			0
SOC 2 compliance			0
ISO/IEC 27001			0
PCI			0
HIPAA			0
FFIEC			0
Single Sign-On Integration			0
Multi-factor Authentication			0
Service			
Uptime			0
Response time			0

Figure 8 LeanIX SaaS vendor evaluation template (LeanIX Gmbh, 2023)

Vendors are graded from 1 to 5 by the feature. Also, the organization will rate the importance of each feature. A vendor evaluation template summary of the vendor assessment and combining multiple vendors using this grading is possible.

6.1.4 NCSC UK

The National Cyber Security Centre of the UK has created a lightweight approach to evaluate cloud services' security (*Lightweight Approach to Cloud Security*, n.d.). It is suitable for quickly assessing the service not used for processing sensitive data. These principles are valid for cloud and SaaS services. They have selected a light questionnaire to provide an understanding of the servicer's security: how the service protects data between client and service, protects user accounts using modern authentication, and has suitable logging and auditing functionalities. Answers to the evaluation are open forms, so it needs some technical knowledge to read the answers of SaaS providers.

NCSC recommends evaluating these four key areas when selecting a suitable provider for the organization's needs:

- Data encryption: Encryption using TLS protocol, over version 1.2, data encrypted at rest.
- Authentication and access control: API connections are protected, 2-factor authentication policy, Single sign-on, privilege separation
- Security logging and incident management: Logging and event collection, availability of logs, policies for updates and incident response, the vulnerability disclosure process
- Governance: Privacy policy, Data location, and legal jurisdiction, transparent details about security features

NCSC UK has also created a model that includes 14 Cloud Security principles (*Lightweight Approach to Cloud Security*, n.d.). They provide security goals for good cloud service and suggest the points to consider when selecting a new service. Also, NCSC provide some recommendations on how cloud provider can comply with these requirements and delivers some considerations for the purchaser when selecting a suitable service:

- *Principle 1: Data in transit protection*
- *Principle 2: Asset Protection and Resilience*

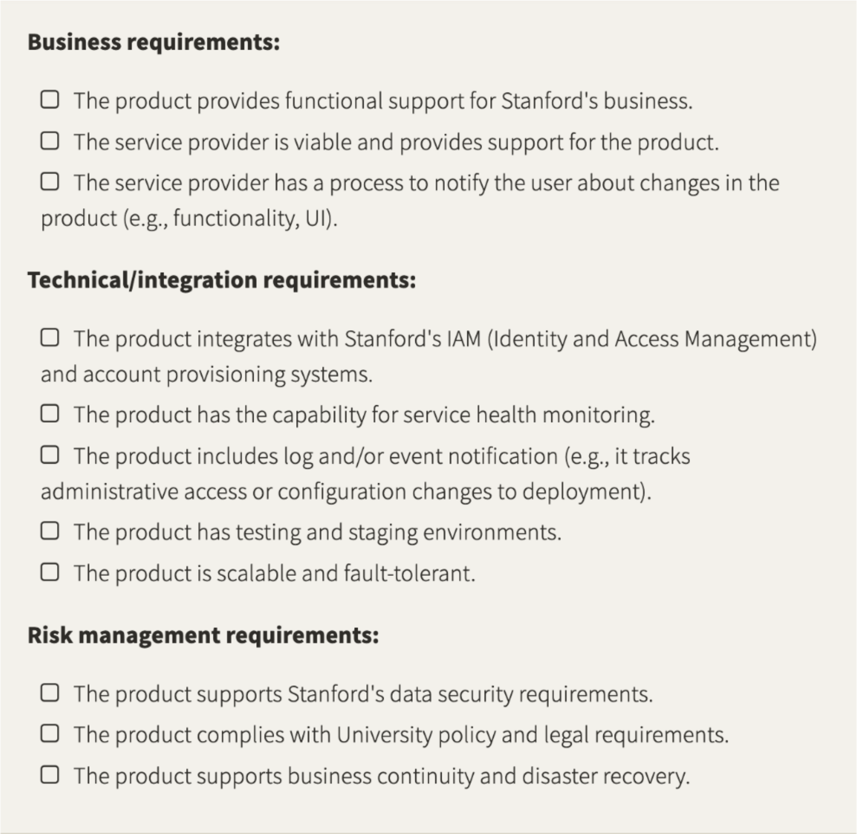
- *Principle 3: Separation between customers*
- *Principle 4: Governance framework*
- *Principle 5: Operational security*
- *Principle 6: Personnel security*
- *Principle 7: Secure development*
- *Principle 8: Supply chain security*
- *Principle 9. Secure user management*
- *Principle 10: Identity and authentication*
- *Principle 11: External interface protection*
- *Principle 12: Secure service administration*
- *Principle 13: Audit information and alerting for customers*
- *Principle 14: Secure use of the service*

6.1.5 Stanford University

Stanford University's IT department has created Minimum Security Standards (*Minimum Security Standards for Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) | University IT*, n.d.) evaluation checklists for organization users. Stanford's Minimum-Security Standards is an example of an organization-specific evaluation guide that helps users evaluate needed services as self-service before contacting the IT department to start purchasing. Service needs to complete the organization's authentication methods and data security requirements.

Stanford's IT uses risk-based evaluation, from Low risk (not personal data) to moderate risk (personal data) to High risk (healthcare or finance data). Then, Stanfords's IT created step-by-step instructions for functions taken care of when using the services, like password policies and API key rules. Stanford has set mandatory security standards aligned with NCSC UK's recommendations, so from service should evaluate at minimum these functionalities:

- *Credentials and Key Management*
- *Encryption*
- *Two-Step Authentication*
- *Logging and Auditing*
- *Data Management*
- *Security, Privacy, and Legal Review (from regulated Data Security Controls)*



Business requirements:

□ The product provides functional support for Stanford's business.

□ The service provider is viable and provides support for the product.

□ The service provider has a process to notify the user about changes in the product (e.g., functionality, UI).

Technical/integration requirements:

□ The product integrates with Stanford's IAM (Identity and Access Management) and account provisioning systems.

□ The product has the capability for service health monitoring.

□ The product includes log and/or event notification (e.g., it tracks administrative access or configuration changes to deployment).

□ The product has testing and staging environments.

□ The product is scalable and fault-tolerant.

Risk management requirements:

□ The product supports Stanford's data security requirements.

□ The product complies with University policy and legal requirements.

□ The product supports business continuity and disaster recovery.

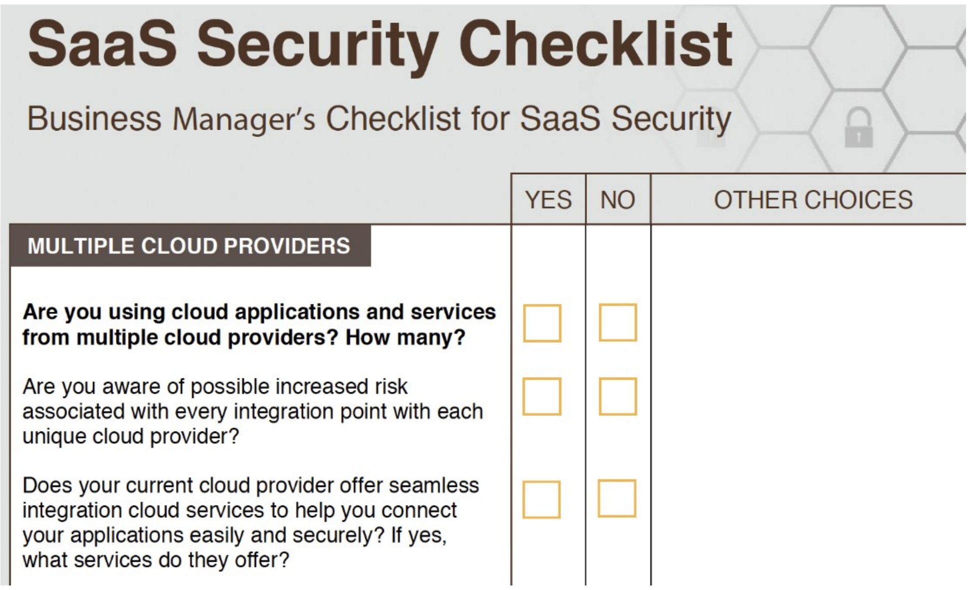
Figure 9 Stanford University’s IT departments SaaS Checklist (*Minimum Security Standards for Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) | University IT*, n.d.)

6.1.6 Oracle

Oracle is a multinational technology company that provides a wide range of software and hardware products. The company's cloud computing platform, Oracle Cloud Infrastructure (OCI), offers a variety of SaaS applications.

Oracle's SaaS Security Checklist for Business Managers is one of the resources that Oracle provides to help organizations secure their SaaS deployments (Oracle, n.d.). The list is more of an overall tool that will force business managers to evaluate their company's existing SaaS infrastructure. Oracle’s checklist includes questions like:

- *Do you use cloud-based applications and services from various service providers?*
- *Do you know the risks involved in integrating points from all providers?*
- *Can you secure access to your data across different cloud environments?*
- *How often do you meet the IT department to talk about SaaS security?*



SaaS Security Checklist

Business Manager's Checklist for SaaS Security

MULTIPLE CLOUD PROVIDERS	YES	NO	OTHER CHOICES
Are you using cloud applications and services from multiple cloud providers? How many?	□	□	
Are you aware of possible increased risk associated with every integration point with each unique cloud provider?	□	□	
Does your current cloud provider offer seamless integration cloud services to help you connect your applications easily and securely? If yes, what services do they offer?	□	□	

Figure 10 Example of Oracle's SaaS Security Checklist's questions (Oracle, n.d.)

Oracle's checklist contains around 40 questions; some are straightforward yes or no questions and some are more flexible. This checklist will make business leaders think of their SaaS security requirements for both existing and new cloud applications.

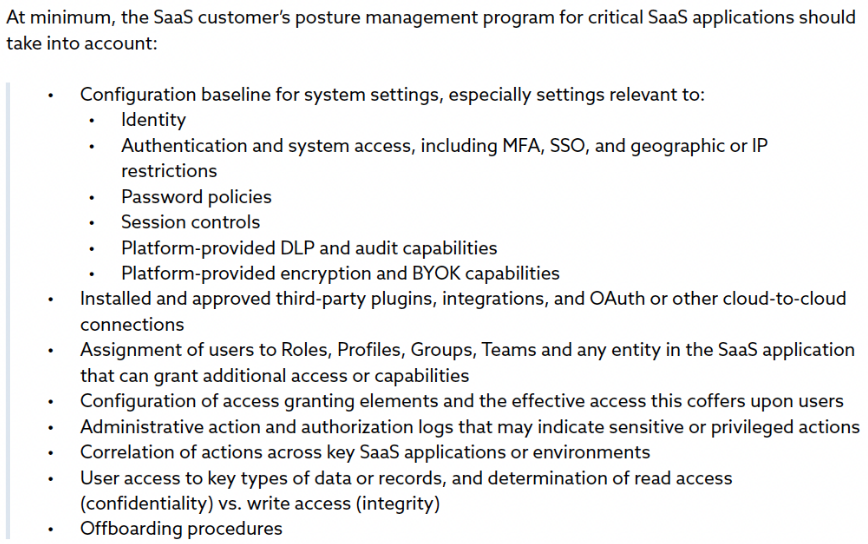
6.1.7 Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices for providing security assurance within cloud computing and providing education on the uses of cloud computing to help secure all other forms of computing. Established in 2008, the CSA acts as a neutral information source for individuals and organizations seeking knowledge, education, certification, and advocacy in cloud security.

SaaS Governance Best Practices for Cloud Customers (*SaaS Governance Best Practices for Cloud Customers*, n.d.) is a document published in 2022 by CSA that guides how to govern SaaS deployments. The SaaS Governance Best Practices document includes best practices for protecting data in SaaS tools, enumerates and considers risks compared with SaaS adoption, and provides mitigation measures for SaaS users. NIST 800-145 (Mell & Grance, 2011) document defines SaaS as "*the capability provided to the consumer through using a provider's applications running on cloud infrastructure.*"

CSA's Best Practices are built around three pillars:

- Discovery: Understanding and documenting the SaaS applications in use within an organization. It needs to know the environmental components before being competent to secure it; in SaaS environments, this is more difficult than in legacy IT environments.
- Management: Ensuring effective management and control over the use of SaaS applications. Setup process for validating SaaS vendors for suitability around industry requirements, like security frameworks.
- Security: Implementing appropriate security measures to protect data and ensure compliance with relevant standards and regulations. Cloud services have a shared responsibility model, but customers are still responsible for security issues.



At minimum, the SaaS customer's posture management program for critical SaaS applications should take into account:

- Configuration baseline for system settings, especially settings relevant to:
  - Identity
  - Authentication and system access, including MFA, SSO, and geographic or IP restrictions
  - Password policies
  - Session controls
  - Platform-provided DLP and audit capabilities
  - Platform-provided encryption and BYOK capabilities
- Installed and approved third-party plugins, integrations, and OAuth or other cloud-to-cloud connections
- Assignment of users to Roles, Profiles, Groups, Teams and any entity in the SaaS application that can grant additional access or capabilities
- Configuration of access granting elements and the effective access this coffers upon users
- Administrative action and authorization logs that may indicate sensitive or privileged actions
- Correlation of actions across key SaaS applications or environments
- User access to key types of data or records, and determination of read access (confidentiality) vs. write access (integrity)
- Offboarding procedures

Figure 11 Example of CSA's Best Practices instructions for customer's posture management (*SaaS Governance Best Practices for Cloud Customers*, 2022)

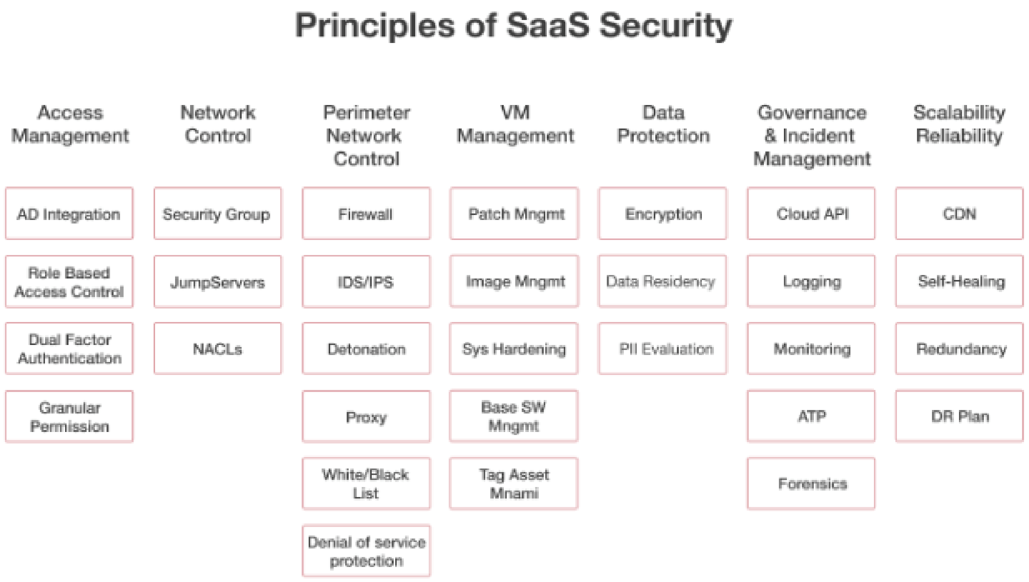
CSA's Best Practices divide the SaaS Lifecycle into three stages and recommend that the organization's IT security personnel be involved in the purchase process during the evaluation phase to ensure the solution's security.

- Evaluation: Assessing the SaaS application before adoption ensures it meets the organization's needs and compliance requirements. It typically comprises four steps: collecting the services that could suit the need, market research, pilot testing, and purchase decision.
- Adoption: The process of implementing the SaaS application within the organization. Includes phases: Evaluation, Adoption, Routine Use and Expansion and finally Termination.

- Usage: Ongoing use of the SaaS application, ensuring it remains compliant and continues to meet organizational needs.

The best practices document divides SaaS security into three main components: process, platform, and application security:

- Process security protects the integrity of procedural activities, ensuring processes' input and output are not easily compromised. These are the managerial aspects, including policies and procedures, to ensure that an organization’s processes are consistent.
- Platform security deals with the security strength of the platform and the underlying dependencies of a SaaS service. These include the SaaS infrastructure, operating systems, and potential suppliers.
- Application security deals with the security of the SaaS application itself. A SaaS application can only stay secure if it does not contain exploitable vulnerabilities and has implemented hardened configurations aligned with organizational and vendor security best practices and compliance requirements.



Principles of SaaS Security

Access Management	Network Control	Perimeter Network Control	VM Management	Data Protection	Governance & Incident Management	Scalability Reliability
AD Integration	Security Group	Firewall	Patch Mngmt	Encryption	Cloud API	CDN
Role Based Access Control	JumpServers	IDS/IPS	Image Mngmt	Data Residency	Logging	Self-Healing
Dual Factor Authentication	NACLs	Detonation	Sys Hardening	PII Evaluation	Monitoring	Redundancy
Granular Permission		Proxy	Base SW Mngmt		ATP	DR Plan
		White/Black List	Tag Asset Mnami		Forensics	
		Denial of service protection				

Figure 12 Seven main components of SaaS security (Solanki, 2022)

Moody's Corporation is a US-based global integrated risk assessment firm that serves various industries, including banking, insurance, government, real estate, and corporate finance sectors, to make better decisions. They used CSA’s SaaS security recommendations when providing their SaaS best practices (*Best Practices for SaaS Security*, 2018) for the banking sector. Regarding security in SaaS-specific models, there are seven core areas to be aware of:

- Access Management: Knowing who can access your cloud and their access privileges is crucial. The vendor must provide a consolidated system that manages user verification. It utilizes business rules that dictate user access based on their position in the organization, the system accessed, data needs, and workflow tasks, regardless of the device used.
- Network Control: Using security groups helps regulate who has access to specific instances within the network. Network Controls can include additional measures like jump servers and network access control lists (NACL) for more refined control. They offer an extra security layer for a virtual private cloud, acting like a firewall to control traffic flow into and out of one or more subnets.
- Perimeter Network Control: The conventional approach to perimeter security focuses on managing traffic moving in and out of a data centre network. Firewalls are the primary technology for this, filtering out potentially harmful or unrecognized traffic based on pre-set rules. Many organizations also use intrusion detection and prevention systems (IDS/IPS) to monitor suspicious traffic that has passed the firewall.
- Virtual Machine (VM) management: Regular updates to your virtual machine are necessary to ensure infrastructure security. Keeping abreast of the latest threats and patches requires significant resources. A SaaS provider will constantly perform these tasks on standard VM images and third-party software, minimizing the time between a breach and its rectification.
- Data Protection: A SaaS provider's strategies to prevent data breaches, primarily via diverse data encryption methods, are critical. The most effective solutions allow customers to control their encryption keys, prohibiting cloud operations staff from decrypting customer data. Data encryption is especially relevant when handling personally identifiable information (PII), which requires stringent safeguards.
- Governance and Incident Management: There should be clear protocols for recording, reporting, and resolving specific types of incidents. Procedures for investigating potential security breaches are also necessary.
- Scalability and Reliability: Cloud's primary benefit is its capacity to scale resources as required. Vertical scaling has limitations as it can only expand as large as the server, whereas horizontal scaling connects multiple servers to work as a single unit. Implementing this scale requires planning, so a cloud computing vendor must incorporate substantial horizontal redundancy into the infrastructure to ensure service continuity. Lastly, a disaster recovery (DR) plan for data and service replication in the event of a disaster is crucial.

6.2 Building of Security Evaluation Tool

Building a SaaS security evaluation tool for non-technical business users balances selecting the most critical requirements and compacting the list of requirements. Work started by gathering requirements from existing standards or evaluation models and selecting the most popular and recommended requirements.

One of the first decisions was to decide the framework of the SaaS evaluation tool. The structure should include cloud-specific requirements by risk-based decisions. It can be found that the Cloud Security Alliance (CSA)'s best practice is suitable for the Evaluation Tool's framework for multiple reasons. CSA is one of the leading organizations dedicated to providing awareness of best practices for secure cloud computing environments. The CSA's SaaS Governance Best Practices for Cloud Customers model, published in 2022, is a comprehensive framework that covers all aspects of SaaS security management, from SaaS lifecycle management to data security and privacy to compliance. The main reason to select CSA's model as a framework is that it is based on the shared responsibility model of cloud security, which recognizes that both the SaaS provider and the customer have a role in protecting SaaS environments. CSA is model-comprehensive and covers all aspects of SaaS security management. It is vendor-neutral, meaning it can be used with any SaaS provider, and some business-oriented organizations do not provide it.

The model provides a step-by-step guide to implementing SaaS governance best practices and includes tools and resources to help organizations get started. CSA's SaaS Governance Best Practices model can help organizations to improve their SaaS security, provide tools to identify and assess SaaS risks and help organizations to select and onboard SaaS providers securely.

On the other hand, part of the CSA's Best practices is also technical and needs cyber security skills to follow SCA's guidance. For that reason, suitable SaaS Governance Best Practices for Cloud Customers are selected from the model's seven categories, described in Chapter 6.1.7. The main sections are Access Management, Data protection, Governance, and incident management.

There is selected self-assessment as a model of the evaluation tool. The article "Audit and self-assessment in quality management: Comparison and compatibility" (Karapetrovic & Willborn, 2001) compares self-assessment and audit methods. These are two essential tools that organizations can use to evaluate some areas. However, there are some critical differences between the two approaches. Self-assessment is when an organization’s internal employees or an external consultant evaluates the service against a set of criteria. Organizations use self-assessments to assess compliance with regulations, identify improvement areas, or better understand service performance.

An audit is when an independent party, like internal auditors, external auditors, or government regulators, evaluates a service against criteria. Audits are typically more formal and rigorous than self-assessments, and they can be used to verify compliance with regulations, ensure the accuracy of financial records, or assess the effectiveness of an organization's risk management system.

Self-assessment can a suitable security method for evaluation tools because a small organization has, in many cases, limited resources. Large organizations with complex operations or significant risks should consider the audit process when selecting suitable solution providers. Also, it is essential to note that self-assessment and audit can be complementary approaches. Organizations can start using self-assessment to identify areas for improvement. An audit is suitable for an organization to verify that improvements have been implemented effectively.

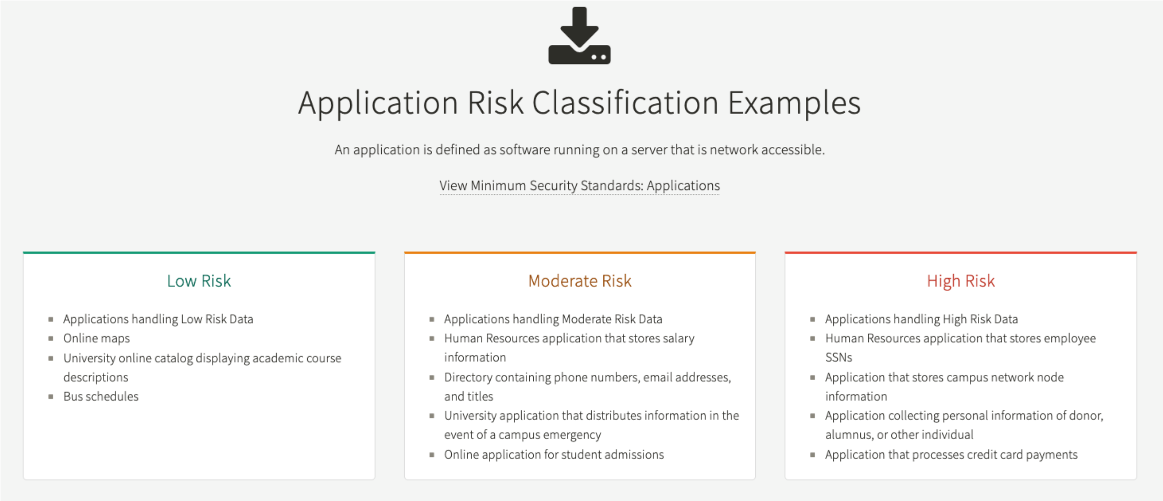
Researcher Monev published an article (Monev, 2021) where he proposes a method for improving the usefulness of the self-assessment method for evaluating the cyber security of cloud providers. Monev has examined many commercial risk-management solution providers. He found that solution providers must align the commercial solutions with standardized information security risk management practices, such as the ISO 27005 standard or NIST 800-30 guide. The article recommends improving the risk assessment process with a self-assessment method developed for organizations' risk management needs using standard models like ISO 27005. This self-assessment template can be filled out by the organization or sent to the solution provider. This will-defined model can also develop solution providers' risk management and documentation processes.

The thesis author collects evaluation tools from available standards or evaluation models. For example, a requirement of Access management: Two-factor authentication is an essential requirement in CSA’s, NCSC UK’s, LeanIX, and Stanford's models. The description section defines why this requirement is essential and selected for the tool: “*Two-factor authentication helps to secure access to the data and accounts. It lowers the risk of credential theft. There should be a policy to force settings on all users.*”

The instruction section instructs how to verify that the Requirement can be validated. For example, validating Requirement Two-factor authentication is instructed by: “Verify is two-factor authentication available and is there a possibility to set up mandatory for all users.” Instruction means that the evaluation tool user should verify the solution provider's security page or setting to validate whether there is a possibility to enable two-factor authentication or if that setting is possible to force to all user accounts.

Tool users should document their findings in the Notes or Links section, for example, copying the description from solutions providers' documentation or a link to solution providers' documentation. This method helps other departments, like IT or procurement, verify evaluation results afterward.

There are different requirement levels; others are easier to complete than others. Also, the usage of the application differs. Organizations use other applications for lighter purposes, like image processing without processing personal or financial information. Risk classification levels for web applications are typically categorized to help organizations understand and manage potential threats. These levels provide a structure for identifying, evaluating, and prioritizing risks, thereby guiding the application of security measures. There are different risk classification models; for example, Stanford University (*Risk Classifications | University IT*, n.d.) has shared Applications risk classification into three categories—low-risk application processes anonymized data, like maps, public information, or similar. Applications that process personal data, like contact details or low-level human resources information, are Moderate risk applications. The high-risk applications process high-risk-level data, like healthcare or finance data. The SaaS Evaluation tool is not suitable for the evaluation of applications. The exact definition and mitigation strategies for these risk levels may vary between different organizations and depend on the specific nature of the web applications, regulatory environment, and the broader risk management framework in place. Understanding the risk classification levels of web applications is essential for developing a robust cybersecurity strategy, and organizations often rely on frameworks like OWASP Top 10 to guide their assessments and mitigation strategies.



Application Risk Classification Examples

An application is defined as software running on a server that is network accessible.

View Minimum Security Standards: Applications

Low Risk

- Applications handling Low Risk Data
- Online maps
- University online catalog displaying academic course descriptions
- Bus schedules

Moderate Risk

- Applications handling Moderate Risk Data
- Human Resources application that stores salary information
- Directory containing phone numbers, email addresses, and titles
- University application that distributes information in the event of a campus emergency
- Online application for student admissions

High Risk

- Applications handling High Risk Data
- Human Resources application that stores employee SSNs
- Application that stores campus network node information
- Application collecting personal information of donor, alumnus, or other individual
- Application that processes credit card payments

Figure 13 Stanford's Application Risk Classification Examples (*Risk Classifications | University IT*, n.d.)

SaaS Evaluation Tools includes four categories:

- The basic requirements every service should comply with include the most recommended security requirements, like Two-factor authentications and Data encryption.
- The second category includes basic Data protection requirements, like the Data Processing Agreement (DPA) and vendor's data subprocessors.
- The third category included requirements requiring more resources from service providers to comply. The applications in the third category process moderate risk-level information. This category includes a requirement of compliance, like ISO 27001 certification of Service level agreement (SLA) measurement.
- The fourth and last category is related to a situation before purchasing or onboarding a new SaaS service. This category includes steps from ownership terms, like license and professional service fees. Also, it is critical to evaluate whether the new service is compatible with the organization's current applications catalogue and whether IT or procurement departments know the new service.

The tools calculate the SaaS service's security score. When the tool user confirms that the service complies with the requirement, a user checks the result to the tool. The requirements value is from 1 or 3; the user should modify these evaluates according to the organization's needs—basic and data protection requirements as one point. The value of intermediate controls in the tool is three points, because of compliance requirements make these harder to achieve. These weightings might vary by the organization's needs. Before onboarding the service, a reviewer should evaluate requirements in the last category to complete the evaluation process.

6.3 Basic Requirements

The SaaS Security Evaluation tool has included 22 different requirements, and the first four requirements include its basic needs. The complete SaaS Evaluation Tool will be found in **Attachment 1** of this thesis.

6.3.1 Two-factor Authentication

Two-factor authentication (2FA) is an essential requirement that helps secure access to data and accounts. It improves the security of SaaS services by adding protection beyond passwords. Passwords are often weak and easily guessed, and abusers can compromise passwords through phishing attacks or data breaches. 2FA helps protect against these attacks by requiring users to provide something they have in addition to their password. 2FA makes it much more difficult for attackers to gain unauthorized access to SaaS accounts. Setting up 2FA needs actions from the user; for that reason, the solution provider should have a policy to force settings on all users. This thesis chapter 3.2. describes 2FA in a more detailed way. All reviewed cloud security models recommend enabling Two-factor authentication. The reviewer should verify the availability of two-factor authentication from the service and verify the possibility of setting up mandatory for all users.

6.3.2 Single sign-on

Single sign-on (SSO) allows authentication to the service without remembering and managing extra passwords using the organization's existing credentials. By reducing the number of passwords that users need to remember, reducing the risk of password compromise, and improving user productivity, SSO can help protect users and organizations from various threats. This thesis chapter 3.2 describes SSO in a more detailed way. SSO is a recommended security improvement method by CSA, NSSC UK, LeanIX, and Stanford’s evaluation models.

The reviewer should verify that there is support for Single Sign-On using his organization’s identity provider. Also, verify whether there is a method for provisioning user accounts automatically using an integration service.

6.3.3 Data Encryption

Transport Layer Security (TLS) 1.2 or higher should protect data in transit between clients and cloud services. TLS is a cryptographic protocol that encrypts data in transit, making it unreadable to unauthorized parties. By encrypting data in transit, organizations can help protect their data from unauthorized access, breaches, and regulatory violations. Additionally, service providers should encrypt data when it is stored on disk. Encryption can be done using various encryption methods, such as AES-256 or Blowfish. By encrypting data on a disk, organizations can help protect their data from unauthorized access, even if it is physically stolen or lost. TLS encryption is recommended, for example, by NCSC UK's listing on this thesis in chapter 6.1.4 or the network security part in chapter 3.1. A reviewer should ensure that the provider has robust security measures, including transit data over the Internet using encryption TLS 1.2 or higher, data encryption at rest and in transit, secure data centres, and regular security audits.

6.3.4 Authentication to Services and APIs

Authentication is verifying a user's or device's identity before granting access to a system or resource. Authentication service verifies the identity of the client application before allowing it to connect to the SaaS API. Authentication is an important security measure for Representational State Transfer (REST) APIs because it helps prevent unauthorized API access. By requiring client applications to authenticate before they can connect to the API, the REST API provider can help to protect its data and resources from unauthorized access. Some authentication methods can be used to secure SaaS API connections, including OAuth 2.0 and API keys. A review should verify if the service has an API connection function and, if available, should be verified if internal and external APIs are protected by authentication. NSCS UK recommends this requirement and is more detailed described in the thesis chapter 3.1.

6.4 Data Protection Requirements

The General Data Protection Regulation (GDPR) stands as a comprehensive data protection and privacy legislation in both the European Union (EU) and the European Economic Area (EEA). It also controls the transfer of personal information beyond these areas. Before purchasing a SaaS service that manages individuals' data, verifying that the service adheres to GDPR guidelines is essential.

The thesis lists a more detailed privacy check in chapter 4.4. There are five requirements in the data protection section.

6.4.1 Data Processing Agreement (DPA)

A data processing Agreement (DPA) describes how a service processes and secures personal data and should have defined the rights and obligations of each party regarding the protection of personal data. The privacy policy outlines how the service provider collects, uses, stores, and protects user data. The reviewer should check that SaaS providers comply with GDPR or other relevant data protection regulations. Privacy information will be found on solution providers' webpages, from privacy, GDPR, or trust pages. The thesis lists a more detailed privacy check in chapter 4.4.

6.4.2 Data Location

Data location within a web service environment is a multifaceted consideration, tightly connected with the core principles and requirements of GDPR. From jurisdictional compliance to security, transparency, and the effective exercise of data subject rights, knowing and controlling where data resides is a foundational aspect of GDPR compliance. Any lapse in managing data location could lead to consequences in the GDPR context. The reviewer should ensure the location of data storage and processing by the service provider. Suppose the SaaS provider operates or stores data outside the EU area. In that case, the provider needs to demonstrate that they have equal protection as GDPR requires, for example, using Transfer Impact Assessment (TIA). The thesis has a TIA chapter 4.3.

6.4.3 Vendor Subprocessing

It is crucial to understand the SaaS provider's subprocessors and verify that they are also in compliance with GDPR. This information is usually in the provider's Data Processing Addendum (DPA). The reviewer should verify SaaS providers and their possible subprocessors and verify that these subprocessors are also in compliance with GDPR. Vendor sub-processing is more detailed and described in the thesis chapter 4.4.

6.4.4 Vulnerability Disclosure Process

A defined Vulnerability disclosure process (VDP) encourages security researchers, ethical hackers, and users to report vulnerabilities they discover in the web service. This collaborative approach helps identify security flaws that might go unnoticed, leading to more timely remediation. The service should proactively enhance its security measures and maintain a robust and secure platform for its users. The reviewer should verify whether a vulnerability disclosure process is available and documented in the SaaS service. VDP is recommended by NCSC UK and mentioned in the thesis chapter 6.1.4.

6.4.5 Support Services

The service provider should have suitable support services. A good support service can help customers identify and resolve problems quickly and easily. Suitable support services are essential for delivering a satisfying user experience, maintaining compliance and security, enabling customization and scalability, and driving continuous improvement and growth. The reviewer should evaluate the service provider's support functions, like email, chat, or community. Also, are there different Support levels or Dedicated customer success managers? LeanIX's SaaS review tool recommends reviewing the support service mentioned in this thesis in chapter 6.1.3.

6.5 Intermediate Requirements

Intermediate requirements, where service processes more risky information than contact data.

6.5.1 Compliance

Evaluating compliance is a critical step in selecting a SaaS provider, providing insights into their security practices, reliability, and alignment with legal and industry standards, ultimately aiding in making an informed decision. For example, ISO 27001 is a compliance standard and framework that ensures a range of security practices and controls are performed by the service provider.
The reviewer should evaluate whether the SaaS vendor complies with relevant industry standards such as ISO 27001, SOC 2, or PCI-DSS. Reviewing the support service is recommended by most evaluation methods, as mentioned in this thesis in chapter 3.3.

6.5.2 Privilege Separation

Segregated duties mean that no single user has too many privileges. This is an essential function of a SaaS tool because:

- Prevents unauthorized access: SaaS providers can help prevent unauthorized access to sensitive data or systems by only granting users the privileges they need to do their jobs.
- Reduces the impact of a security breach: If a security breach does occur, the damage can be limited if only authorized users have access to the affected data or systems.
- Improves accountability: When privileges are separated, tracking who has access to what and when is easier.
- Complies with regulations: Many regulations require organizations to implement separation of privileges.

The solution provider can provide a privilege separation function by creating different roles with different levels of rights and by requiring multiple users to approve specific actions. The reviewer should verify the service possibility of providing different user roles and privileges. Privilege separation is recommended by NCSC UK and mentioned in the thesis chapter 6.1.4.

6.5.3 Service Level

Documented Service level agreement (SLA) that clearly defines the expected levels of reliability and performance. It is a vital function of SaaS providers for several reasons: it defines the level of service a customer can expect, including uptime, response time, and support availability. It also specifies the responsibilities of the SaaS provider and critical components for risk management. The reviewer should check if the service has a documented Service Level Agreement (SLA). SLA separation is recommended by NCSC UK and mentioned in the thesis chapter 6.1.4.

6.5.4 Data Backup

Backup is essential to securing the organization's data, and solution providers should ensure backup functionality to enable quick recovery in case of disasters. Encrypting the backup data prevents to avoid data leakage. The reviewer should evaluate the service's backup functions and verify if there is available documentation of the frequency of data backup. Also, verify if there is an option to restore customer data quickly in case of data loss. Data backup is described in more detail in the thesis chapter 3.2.

6.5.5 GDPR Tool

The GDPR tools allow data subjects, like users and contacts, to access their data, request corrections or rectifications, request deletion, restrict data processing, and obtain data portability. These tools should be included in the SaaS service provider to provide these GDPR requirements effectively. GDPR tool is described in more detail in the thesis chapter 4.4.

6.5.6 Security Audits

Regular security audits are an essential part of the security strategy for SaaS vendors. They help assess the robustness of vendors’ security practices, ensure compliance with legal and industry standards, and build confidence in their ability to protect sensitive data and systems.

During the reviewing process, evaluators should verify the documentation of SaaS vendors performing regular audits of their security controls and whether these reports are available for the customers. A security audit is described in more detail in the thesis chapter 4.4.

6.5.7 Security Description

The security description provides an overview of the providers' measures and practices to protect user data and ensure the service's confidentiality, integrity, and availability. It summarises security protocols, access controls, encryption methods, and risk management procedures, assuring customers that their information is safeguarded against unauthorized access and cyber threats. The reviewer should verify whether the SaaS provider publishes a security description on their website. The description can also be a security whitepaper or a report from an auditor. Security description recommended by NCSC UK and mentioned in the thesis chapter 6.1.4.

6.5.8 Security Logging and Event Collection

Security logs assist both customers and the service provider in identifying any security breaches. These logs should cover critical aspects like authentication attempts, configuration modifications, and information about accessed resources. Cloud service should grant customers access to these security logs, enabling easy export of customers' auditing systems. There are different parameters to evaluate logging quality, like the type of logged events, retaining period, or encryption of the logs.

The evaluator should verify that the service provider collects security logs and that records are available to the customer. Evaluation of security logging is recommended by NCSC UK and mentioned in the thesis chapter 6.1.4.

6.5.9 Security Incident Response policy and applying Updates

Incident response policy defines how solution provider has prepared themself for cybersecurity incidents—a well-defined procedure for implementing security updates on their internal systems and promptly addressing identified security concerns. Evaluating the provider's past performance is an informative measure of their ability to handle future security issues.

During an evaluation, evaluation should check whether the SaaS provider published the available incident response process and policy for applying security updates in response to publicly reported issues. Evaluation of incident response policy and applying updates is recommended by NCSC UK and mentioned in the thesis chapter 6.1.4.

6.6 Before onboarding of new SaaS service

Before onboarding a new SaaS application, it is vital to carefully manage administrative duties, such as addressing ownership terms (including license terms, professional services fees, and pricing) and considering business requirements and risk management. The organization’s IT or procurement department will assist with the purchase process. Taking care of administrative duties is not merely a procedural formality but a strategic necessity. It ensures that the organization understands its commitment, that the chosen SaaS solution aligns with business goals, and that potential risks are identified and managed. Also, these steps help build a successful partnership between the organization and the SaaS provider.

6.6.1 Ownership Terms

Verifying license terms, professional services fees, and pricing is essential when selecting a SaaS provider. These operations before purchase help with financial planning, contractual clarity, service evaluation, and overall business success. The evaluator should verify the service's license terms, possible Professional Services Fee, and Pricing decision during the selection process. Evaluation of ownership terms is recommended by LeanIX and mentioned in the thesis chapter 6.1.3.

6.6.2 Business Requirements

The solution should integrate with existing products of the organization's portfolio. The service provider should be financially stable with a sustainable business model, reducing the risk of sudden closure. Additionally, the provider should be able to collaborate with other services or tools that support activities within their specific market segment. Evaluation of ownership terms is recommended by Stanford University and mentioned in the thesis chapter 6.1.5.

6.6.3 Contacting the IT Department

It is essential that the IT department verifies the SaaS service during the selection process and ensures that the chosen solution aligns with technical requirements, security standards, and overall business objectives, leading to successful integration and optimal utilization of the SaaS service. Stanford University recommends contacting the IT department before purchasing the SaaS service, as mentioned in the thesis chapter 6.1.5.

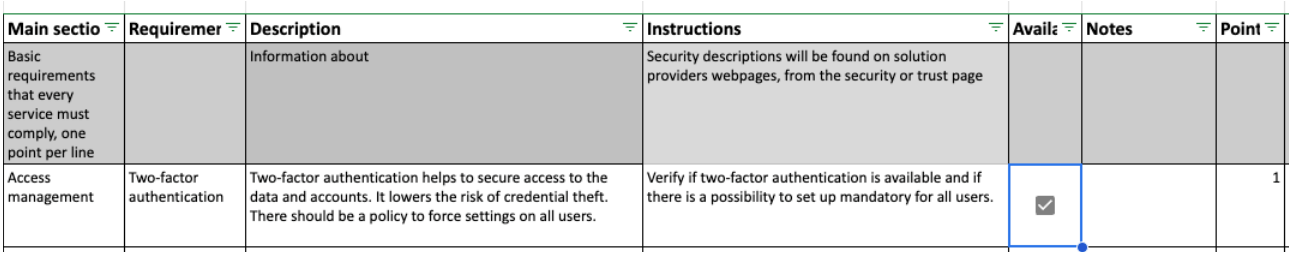
6.6.4 Vendor lock-in Technical/integration requirements

Before terminating a contract with a SaaS provider, it is essential to have a data retrieval plan. This plan can include the timeline and format for data return when switching vendors.

Verify that a method is available to export or transfer data from the service when terminating the service. Stanford University recommends evaluating termination situations before purchasing the SaaS service, as mentioned in the thesis chapter 6.1.5.

7 Testing of SaaS Security Evaluation Tool

The SaaS Security evaluation tool was drafted using Google Workspace’s Sheets online spreadsheet editor. We created multiple tool versions during development, selecting the most suitable requirements and weightings. These weightings might vary by the organization’s needs. Before publishing the tool to the test group, it was trialed by the thesis author in several size SaaS vendors. The evaluation aimed to ensure that the questionnaire and instructions were suitable for deployment and estimate the affords needed in the evaluation process. In the next section are examples of the evaluation of HubSpot marketing automation SaaS software.



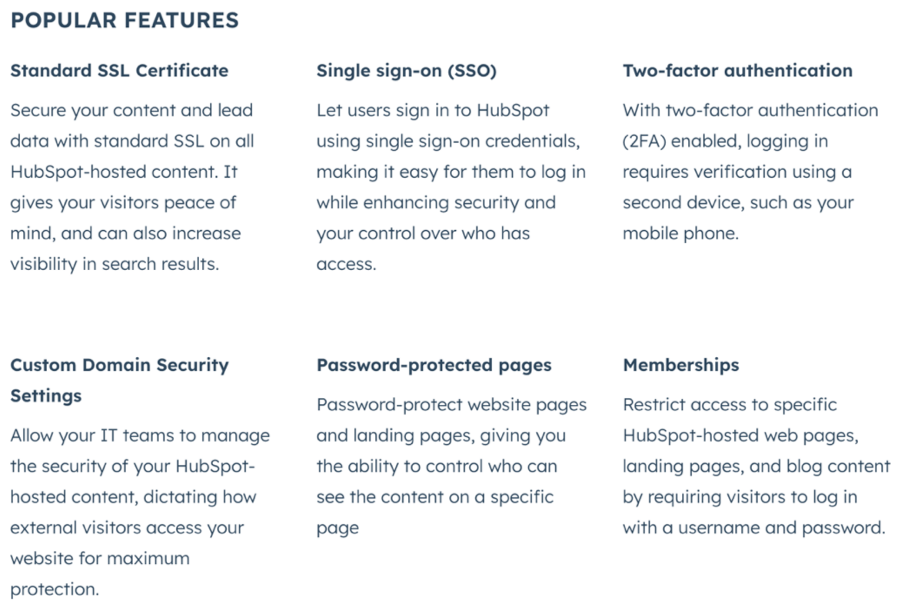
Main sectio	Requiremer	Description	Instructions	Availa	Notes	Point
Basic requirements that every service must comply, one point per line		Information about	Security descriptions will be found on solution providers webpages, from the security or trust page			
Access management	Two-factor authentication	Two-factor authentication helps to secure access to the data and accounts. It lowers the risk of credential theft. There should be a policy to force settings on all users.	Verify if two-factor authentication is available and if there is a possibility to set up mandatory for all users.	☑		1

Figure 14 Example of SaaS Security Evaluation tool spreadsheet

7.1 Security Evaluation of HubSpot

HubSpot is a US-based CRM platform that provides a suite of software products for marketing, sales, and customer service for over 120,000 customers. It was selected for trialing a SaaS security evaluation tool for evaluating large enterprise-level products.

HubSpot's security program is designed to safeguard customer data and maintain customer trust. Their security and privacy documentation has been collected on a few main pages, which are located under the Security, Privacy, and Control main page (HubSpot, 2023). It were simple to find answers to the basic requirements of access management and data protection. For example, two-factor authentication, Single sign-on (SSO), and the status of SSL encryption are listed there.



POPULAR FEATURES

Standard SSL Certificate

Secure your content and lead data with standard SSL on all HubSpot-hosted content. It gives your visitors peace of mind, and can also increase visibility in search results.

Single sign-on (SSO)

Let users sign in to HubSpot using single sign-on credentials, making it easy for them to log in while enhancing security and your control over who has access.

Two-factor authentication

With two-factor authentication (2FA) enabled, logging in requires verification using a second device, such as your mobile phone.

Custom Domain Security Settings

Allow your IT teams to manage the security of your HubSpot-hosted content, dictating how external visitors access your website for maximum protection.

Password-protected pages

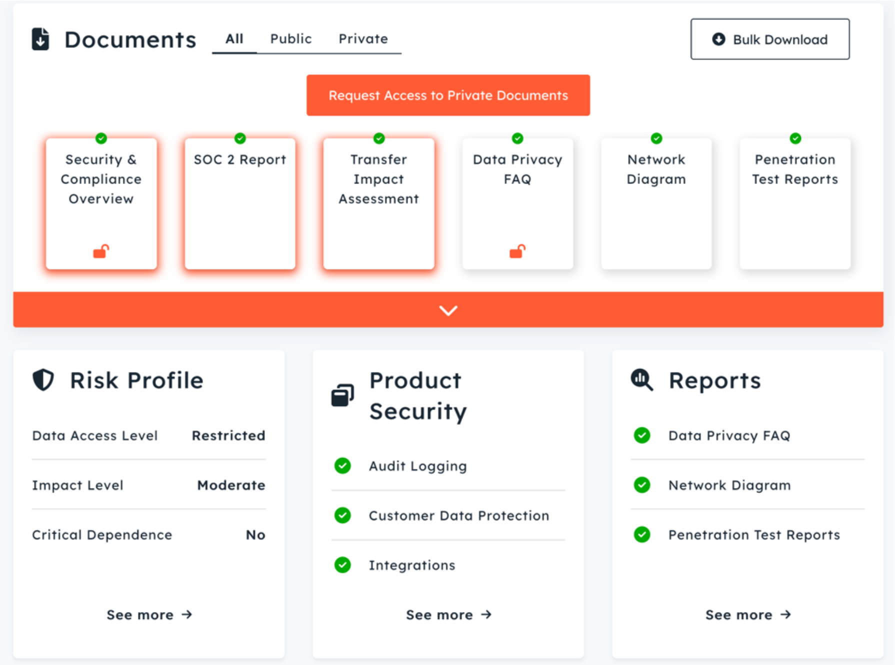
Password-protect website pages and landing pages, giving you the ability to control who can see the content on a specific page

Memberships

Restrict access to specific HubSpot-hosted web pages, landing pages, and blog content by requiring visitors to log in with a username and password.

Figure 15 Example of HubSpot's Security, Privacy, and Control web page (HubSpot, 2023)

A more technical Trust centre is available to evaluate the intermediate requirements, where it is possible to ask permission for the latest SOC 2 audit report. HubSpot has developed its security processes since the start of 2006 and complies with essential US compliance certifications, like SOC 3, Privacy Shield, and the California Consumer Privacy Act (CCPA).



Documents All Public Private

Bulk Download

Request Access to Private Documents

Security & Compliance Overview

SOC 2 Report

Transfer Impact Assessment

Data Privacy FAQ

Network Diagram

Penetration Test Reports

Risk Profile

Data Access Level	Restricted
Impact Level	Moderate
Critical Dependence	No

See more →

Product Security

✓ Audit Logging

✓ Customer Data Protection

✓ Integrations

See more →

Reports

✓ Data Privacy FAQ

✓ Network Diagram

✓ Penetration Test Reports

See more →

Figure 16 Example of HubSpot's Trust Center web page (*HubSpot | Trust Center*, n.d.)

Overall, HubSpot has a robust security program designed to protect customer data. The company regularly reviews and updates its security program to ensure it meets the highest security standards. HubSpot complies with all requirements of the evaluation tool, except there needs to be a description of their Service Agreement Level (SLA). The security evaluation report of the HubSpot service will be found attached to the thesis.

8 Feedback from Security Evaluation Tool

The feedback on the Security Evaluation tool is collected from the testing group. Trying a tool with a trial group and collecting their opinions is vital to enhancing the product's usability and functionality and managing users' preferences.

- Assessing Usability: Trial users can provide insights into the tool's ease of use, intuitiveness, and user-friendliness. This feedback is essential in making necessary adjustments to enhance the user experience.
- Validating Functionality: Testing the tool with actual users helps validate whether it meets its intended purpose and performs the desired functions. It can reveal gaps or areas where the tool needs to align with user expectations.
- Collecting User Preferences and Suggestions: Test users can provide valuable feedback and suggestions for additional features or improvements, leading to a more refined and user-centric product.

The testing group has been collected from volunteers of Avidly’s employees using announcements in Avidly’s messaging channel. There are persons from different backgrounds, like countries, technical skills, and business units.

8.1 Feedback Form

The Security Evaluation Tool has been shared with the test group as a Google Sheet template; all participants receive a copy of the evaluation sheet. They are instructed to use the tool to evaluate a service that can be familiar to them or a new service that would be useful for their business need. The feedback on the evaluation tools has been collected using the Google Forms questionnaire form with five questions with four questions with a linear scale (from 1 to 5 grading) and one open feedback question. The form covers essential aspects of the evaluation process, gathering quantitative and qualitative feedback to provide a comprehensive view of the users' experience with the security evaluation tool.

Feedback form of Security Evaluation Tool

Thank you for participating in providing feedback on the SaaS Security Evaluation Tool. Your insights are essential to estimating the value of the tool and getting knowledge difficulties for estimating the service's security and privacy. Please take a few moments to complete this feedback form. The answers are anonymous.

Feedback form questions:

Your name:

How do you rate your knowledge of cyber security area? (1=Beginner, 5= Professional)

How easy was finding answers to the tool's requirements from the solution provider's web page or service? (1 = Very Difficult, 5 = Very Easy)

Which sections were most challenging or easy to find answers to?
Open answer.

Does the tool help you give an overview of which criteria must be considered when selecting a new SaaS service? (1 =Not helped at all, 5 = Very helpful)

How satisfied are you with the tool overall? (1 = Not Satisfied at all) , 5 = Very Satisfied)

What did you like most about the tool? What areas need improvement?
Open answer.

Please provide any additional comments or suggestions that may help us improve the tool.

[Submit Button]

8.2 Analysing the feedback

The feedback form with instructions was collected during September 2023 by sending approximately 350 invitations using Slack, WhatsApp, and email messages to a possible test group that includes Avidly employees, cyber security master students, and IT professional contacts. There were challenges in getting enough answers to the feedback form, which received only 15 valid responses, so the response rate was only 4.3%. The number of answers could be higher and will affect the quality of the results collected using the feedback form. The thesis author directly connected some persons who would be potential responders; the most common explanation for not answering now was the busy work season after the holiday season; another reason was that the subject felt too technical from their knowledge. Also, the selected qualitative research method was more laborious to complete than just numerical values. According to the article Presenting and Evaluating Qualitative Research (Anderson, 2010), this method limitation heavily depends on the researcher’s skills, and creating and analyzing the research needs more work. Also, the researchers’ personal opinions can affect the results.

Although there were only a limited number of answers, collecting valuable feedback from the survey group was possible. Responders estimate their knowledge of cyber security is from beginner to professional. Four responders were from the beginner level, and three professional level; the rest of the answers were between these values. According to these answers, getting feedback from persons with different technical backgrounds was essential because one of the research questions was to investigate the possibility of providing a SaaS evaluation tool suitable for non-technical persons.

8.2.1 Finding answers to the requirements

The test group tested the SaaS Security Evaluation tool in practice for their freely selected service or verified the delivered pre-filled assessment of HubSpot service’s security and privacy. After they tried the tool, they were instructed to estimate how easy or difficult it is to find security or privacy documentation from the solutions provider’s web page or service.

According to their feedback, people with limited competence in cyber security knowledge needed help understanding terminology, like GDPR or ISO certification. Also, according to their feedback, it wasn't easy to find security information from the solution provider’s site, for example, using the website search function. Many services have separate security or privacy portals that might not be indexed with the main web pages or use different terminology. Also, there might be locked functions on the security web portals that provide access after contacting customer service or signing the NDA contract. The group rated how easy it was to find the answers between 1-2 of 5 in this group with limited cyber knowledge.

Persons who rated themselves as cyber-security professionals said the easiest part to find was GDPR or privacy information. The quality of privacy documentation has been an active topic since the publishing of the EU’s GRPR regulation, and privacy documentation is presented in standardized ways in many websites' privacy portals, which have been recently built up. The cyber professionals reported that finding documentation about the service provider’s security practices, such as a description of incident management or support or technical processes, is practically impossible. Another challenging part was to find information about the service's technical security procedures, like encryption or backup processes. Another tricky part was getting information on event log keeping. Rating of how easy was finding the answers was between 2-3 of 5 in this group. These answers correspond to the research findings that no predefined model exists to document web services' security and privacy levels. Also, the terminology of the cyber field can be complicated, and clarification needs more help functions to the evaluation tool.

8.2.2 Feedback of the Evaluation Tool

The question asked from the test group: "Does the tool help you give an overview of which criteria need to be considered when selecting a new SaaS service?" This answer was provided using a numerical scale from 1 (Not helped at all) to 5 (Very helpful). The average value of the answers was 4.0, so most people feel that delivering a list of security and privacy requirements with a description provided them with helpful information and may help them select more secure services.

Another question was: "How satisfied are you with the tool overall?" The answer was provided using a numerical scale from 1 (Not satisfied at all) to 5 (Very satisfied). The average value of the answers was 4.0. According to this feedback, the test group was satisfied with the evaluation tool. The next question provides a more profound understanding of what they like most about the tool. There was an open form for the answers; many answered that the tool was comprehensive and provided valuable information. They also provided positive feedback on a collected compact pack of questions that can be used as a list of things one must remember to check out. Also, users were pleased to see the advice of relying on the Existing certifications (e.g., ISO 27001).

There were valuable recommendations as to how the tool could be improved. Users recommended separating part of the requirement because now there are multiple questions under one requirement. This makes it harder to select yes or no when only some criteria were fulfilled. Another improvement idea was adding hints on each topic, like: "Where should I find the correct information that I'm looking for?" and keywords for searching needed information from the web page. There was also feedback on areas that should be included in the evaluation tool; contractual terms were recommended to add new criteria, like contractual terms, responsibility, and reimbursement when anything goes severely south, e.g., data breach and SLA for how the service itself and the security within the service are provided.

In the final section of the questionnaire, test group members had the option to provide free additional comments or suggestions that may help to improve the tool. More than half of the test group members provide this feedback. One of the most exciting feedback items was a recommendation to include a requirement to evaluate the access rights required by the SaaS provider to the customer's systems and how well they have been modelled with the least privilege in mind. Providing a solution for that need will need more investigation. One cyber professional mentioned that fact: unfortunately, all the necessary information is unavailable readily or at all (for certain providers), and the unclarity may make it difficult to evaluate which service provider to choose. Also, one feature requested was to provide an evaluation as a program instead of a static spreadsheet: a tool that would only need to give the website's name, which would automatically collect the information and provide a scoring of the service. This kind of commercial solution is already available, and providing this kind of solution needs more resources. According to the feedback from the test group, there is a possibility to provide a solution for delivering overall security and privacy requirements when selecting a new service. However, self-evaluation needs more competence in cyber terminology, so the provided solution is only suitable for users with technical competence.

9 Conclusions

This study aimed to find critical security and privacy aspects of SaaS applications and investigate if it is possible to create an evaluation tool for their security and privacy to help select a suitable solution for the business needs. During the research process, it was found that there is no one standardized framework for documenting or complying with cloud service’s security level like Traficom’s Finnish Cyber Security Label Field (Cybersecurity Label, n.d.) for connected smart devices. There are standards like ISO 27001 and Cloud Security alliances’ certification programs available that help end customers verify the service’s security, but these are all only part of the service provider’s security documentation. Evaluating a cloud service’s security level still requires technical and cyber security areas, which are laborious if done manually.

The European Union Agency for Cybersecurity (ENISA) initiated the EUCS – Cloud Services Scheme (SA, 2020) to look into the certification of the cybersecurity of cloud services EU's framework to document all requirements. This framework is based on international standards and frameworks, and it aims to provide certification that cloud companies can leverage to demonstrate the soundness of their privacy and security measures. While writing the thesis, this publication process is still in progress, and the certification has overcome technical and political obstacles; for example, EU countries have started to develop their own frameworks (Broadbent, 2023). On the other hand, during the writing process, cooperation between the EU and the United States in regulating data transfers between countries has become more apparent with the EU-US Data Privacy Framework (EU, 2023) in July 2023; this allows validating correctness of data transfers with lighter process. Also, in the year 2022 published Cloud Security Alliance's (CSA) SaaS Governance Best Practices for Cloud Customers (*SaaS Governance Best Practices for Cloud Customers*, 2022) model is the first SaaS-specific framework for security and privacy management, the first solutions using that framework has been published and this probably standardized way of security management and documentation of SaaS services.

According to feedback from the test group, cyber security expertise is needed for evaluating the service's security; different requirements terms are complicated to describe. On the other hand, they provided positive feedback about the SaaS Evaluation Tool because they provided overall information on all aspects taken care of when selecting a new service and may help understand the importance of security when choosing a new service for their business needs.

According to this thesis, there are many challenges to take care of to conclude the usability of manual evaluation of the SaaS services. Manual evaluation of a new service can be very time-consuming; information can be divided into multiple locations or acquired by contacting the service provider's support services to receive hidden documentation. One way to minimize consumed time is to ask the service provider to collect the needed information for the evaluation form by themselves. Still, the organization must verify the suitability of the provided data. As earlier mentioned, there is no standard method of documentation. Also, cybersecurity and privacy regulations expertise is needed to produce accurate evaluations. Organizations may only sometimes have this expertise in-house, necessitating external consultants, which can be costly. According to feedback from the test group, self-evaluating the service by a non-technical business unit user is not an easy solution, and they will contact IT or similar departments during the evolution or accusation process.

Updating the documentation can be laborious when an organization has multiple SaaS services in active use. When an organization grows or adopts more SaaS applications, the scalability of manual evaluations becomes a problem. Maintaining the same level of thoroughness and accuracy is complex as the number of applications increases. There is a need to have periodic reviews for the documentation because privacy and security regulations are continuously evolving, and maintaining these changes and understanding their implications on SaaS services can be challenging. An organization needs resources to follow these changes to evaluate the effects of their environment and whether their services need to be re-evaluated. Also, service providers develop their services continuously, and significant changes need to be reviewed and updated in the documentation.

There is a possibility of subjectivity and Inconsistency of the evaluation results because these can be subjective and vary from one evaluator to another. It is challenging to create comparable evaluation forms with enough detailed instructions. Persons might interpret requirements in different levels and weights differently. In summary, manually evaluating and documenting security and privacy aspects can create significant administrative overhead and be expensive due to the labour hours required, the potential need for external consultants, and other associated costs.

These challenges underscore the importance of automating security and privacy evaluations and supplementing manual evaluations with automated tools to ensure comprehensive and consistent assessments. The key learning of this thesis is that there is no easy way of developing evaluation requirements for service security and privacy. Still, there is a possibility to provide knowledge of cyber security to the business unit users with this model. In future development, the need for authorities is to provide a consistent framework for cloud security documentation. Another requirement is to get an easy and cost-effective IT procurement solution for SME-size businesses to automate these security evolutions.

References

Adaptive Shield. 2023. 2023 SaaS-to-SaaS Access Report. Accessed on 3 March 2023. Retrieved from https://www.adaptive-shield.com/saas-to-saas-3rd-party-app-risk-report-2023

Anderson, C. 2010. Presenting and Evaluating Qualitative Research. American Journal of Pharmaceutical Education, 74(8). Accessed on 10 March 2023. Retrieved from https://doi.org/10.5688/aj7408141

Bhandari, P. 19 June 2020. What Is Qualitative Research? | Methods & Examples. Scribbr. Accessed on 1 March 2023. Retrieved from https://www.scribbr.com/methodology/qualitative-research/

Broadbent, M. 2023. The European Cybersecurity Certification Scheme for Cloud Services Certification Scheme for Cloud Services. Accessed on 6 October 2023. Retrieved from https://www.csis.org/analysis/european-cybersecurity-certification-scheme-cloud-services

Calvello, M. 20 May 2020. The Complete Guide to SaaS Vendor Management in 2021. Accessed on 27 April 2023. Retrieved from https://track.g2.com/resources/saas-vendor-management

Chen, Y., Gao, Y., Ceccio, N., Chatterjee, R., Fawaz, K., & Fernandes, E. 2022. Experimental Security Analysis of the App Model in Business Collaboration Platforms. 2011–2028. Accessed on 3 March 2023. Retrieved from https://www.usenix.org/conference/usenixsecurity22/presentation/chen-yunang-experimental

CSA. 10 October 2022. SaaS Governance Best Practices for Cloud Customer. Accessed on 4 August 2023. Retrieved from https://cloudsecurityalliance.org/artifacts/saas-governance-best-practices-for-cloud-customers/

Data Protection Ombudsman's Office. n.d. Data protection. Accessed on 4 April 2023. Retrieved from https://tietosuoja.fi/en/data-protection

Elenamalova. 8 September 2022. Application Information for ArcGIS Maps by Esri—Microsoft 365 App Certification. Accessed on 3 May 2023. Retrieved from https://learn.microsoft.com/en-us/microsoft-365-app-certification/teams/esri-arcgis-maps

EU. 10 July 2023. Questions & Answers: EU-US Data Privacy Framework - European Commission. Accessed on 8 October 2023. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

EU. n.d. Rules on international data transfers. Accessed on 27 April 2023. Retrieved from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

Fortune. February 2023. Software as a Service [SaaS] Market Size & Growth, 2022-2029. Accessed on 31 March 2023. Retrieved from https://www.fortunebusinessinsights.com/software-as-a-service-saas-market-102222

G2. 2023. Best SaaS Operations Management Software in 2023. Accessed on 28 April 2023. Retrieved from https://www.g2.com/categories/saas-operations-management

Gartner. 2023. IT Risk Management (ITRM) Reviews 2023 | Gartner Peer Insights. Accessed on 28 April 2023. Retrieved from https://www.gartner.com/market/it-risk-management-solutions

GDPR.Eu. n.d. GDPR compliance checklist. Accessed on 22 September 2023. Retrieved from https://gdpr.eu/checklist/

Greenberg, A. 23 September 2022. Slack's and Teams' Lax App Security Raises Alarms. Wired. Accessed on 3 March 2023. Retrieved from https://www.wired.com/story/slack-microsoft-teams-app-security/

Grynwajc, S.16 May 2022. International Data Transfers: When and How to Perform a Transfer Impact Assessment. Law Office of S. Grynwajc, PLLC. Accessed on 27 April 2023. Retrieved from https://www.transatlantic-lawyer.com/international-data-transfers-when-and-how-to-perform-a-transfer-impact-assessment/

Hawedi, M., Talhi, C., & Boucheneb, H. 2018. Security as a Service for Public Cloud Tenants (SaaS). Procedia Computer Science, 130, 1025–1030. Accessed on 3 March 2023. Retrieved from https://doi.org/10.1016/j.procs.2018.04.143

HubSpot. n.d. HubSpot Security Program. Accessed on 18 August 2023. Retrieved from https://legal.hubspot.com/security

HubSpot. n.d. HubSpot Trust Center. Accessed on 18 August 2023. Retrieved from https://trust.hubspot.com/

IBM. n.d. IaaS vs. PaaS vs. SaaS. Accessed on 1 March 2023. Retrieved from https://www.ibm.com/topics/iaas-paas-saas

IBM. n.d. SaaS – software-as-a-service. Accessed on 2 March 2023. Retrieved from https://www.ibm.com/topics/saas

ISC2. n.d. The Threat of Insecure Interfaces and APIs. Accessed on 10 March 2023. Retrieved from https://www.isc2.org:443/Articles/the-threat-of-insecure-interfaces-and-apis

ISO Org. n.d. ISO/IEC 27032:2012. Accessed on 9 March 2023. Retrieved from https://www.iso.org/standard/44375.html

ISO Org. October 2022. ISO/IEC 27001 Standard – Information Security Management Systems. Accessed on 4 May 2023. Retrieved from https://www.iso.org/standard/27001

IT Governance Ireland. n.d. The EU General Data Protection Regulation. Accessed on 27 April 2023. Retrieved from https://www.itgovernance.eu/en-ie/eu-general-data-protection-regulation-gdpr-ie

JAMK. 2018. Ethical Principles for JAMK University of Applied Sciences. Accessed on 3 January 2023. Retrieved from https://www.jamk.fi/fi/file/ethical-principles

JAMK. 9 January 2020. Project Reporting Instructions. Accessed on 3 January 2023. Retrieved from https://oppimateriaalit.jamk.fi/projectreportinginstructions/

Karapetrovic, S., & Willborn, W. 2001. Audit and self-assessment in quality management: Comparison and compatibility. Managerial Auditing Journal, 16, 366–377. Accessed on 11 August 2023. Retrieved from https://doi.org/10.1108/02686900110395505

LeanIX n.d. Evaluate SaaS Applications—Criteria & Matrix. Accessed on 16 February 2023. Retrieved from https://www.leanix.net/en/wiki/saas/saas-evaluation

LeanIX. 2021. IaaS vs. PaaS vs. SaaS - Differences, Examples and Diagram. Accessed on 1 March 2023. Retrieved from https://www.leanix.net/en/wiki/saas/iaas-vs-paas-vs-saas

LeanIX. 2023. SaaS Security Checklist & Assessment Questionnaire. Accessed on 5 March 2023. Retrieved from https://www.leanix.net/en/wiki/saas/saas-security-checklist-and-assessment-questionnaire

LeanIX. n.d. What is Shadow IT? Discover and Manage It - The Definitive Guide. Accessed on 10 March 2023. Retrieved from https://www.leanix.net/en/wiki/saas/shadow-it

Mäkikyrö, V. 2020. SaaS-palvelun hyödyt lisensoituun ohjelmistoon verrattuna. Candidate thesis. Information Systems Science. University of Jyväskylä. Accessed on 31 March 2023. Retrieved from https://jyx.jyu.fi/handle/123456789/69825

Mell, P., & Grance, T. 2011. The NIST Definition of Cloud Computing (NIST Special Publication (SP) 800-145). National Institute of Standards and Technology. Accessed on 4 April 2023. Retrieved from https://doi.org/10.6028/NIST.SP.800-145

Microsoft. 9 March 2023. Overview of app certification by Microsoft —Microsoft Teams. Article. Accessed on 3 May 2023. Retrieved from https://learn.microsoft.com/en-us/microsoftteams/overview-of-app-certification

Microsoft. n.d. Microsoft Teams store validation guidelines—Teams. Accessed on 3 March 2023. Retrieved from https://learn.microsoft.com/en-us/microsoftteams/platform/concepts/deploy-and-publish/appsource/prepare/teams-store-validation-guidelines

Monev, V. 2021. The "Self-Assessment" Method within a Mature Third-Party Risk Management Process in the Context of Information Security. 2021 International Conference on Information Technologies (InfoTech), 1–7. Accessed on 11 August 2023. Retrieved from https://doi.org/10.1109/InfoTech52438.2021.9548373

Moodys. Best Practices for SaaS Security. April, 2018. Accessed on 4 April 2023. Retrieved from https://www.moodysanalytics.com/articles/2018/best-practices-for-saas-security

NCSC-FI. 29 May 2019. Criteria for Assessing the Information Security of Cloud Services (PiTuKri). Accessed on 3 May 2023. Retrieved from https://www.kyberturvallisuuskeskus.fi/en/publications/criteria-assessing-information-security-cloud-services-pitukri

NCSC. n.d. Lightweight approach to cloud security. Accessed on 2 May 2023. Retrieved from https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/lightweight-approach-to-cloud-security

Netum. 11 January 2022. Viitekehyksiä parempiin tietoturvallisuuskäytäntöihin: Osa 4 - NIST Cybersecurity Framework. [Frameworks for better information security practices: Part 4 - NIST Cybersecurity Framework]. Accessed on 22 September 2023. Retrieved from https://www.netum.fi/2022/01/11/viitekehyksia-parempiin-tietoturvallisuuskaytantoihin-osa-4-nist-cybersecurity-framework/

Nimrod, I. 27 July 2022. 8 Data Security Best Practices for SaaS Applications. Polar Security. Accessed on 2 May 2023. Retrieved from https://www.polar.security/post/8-data-security-best-practices-for-saas-applications

NIST, J. T. F. 2020. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. Polar Security. Accessed on 4 May 2023. Retrieved from https://doi.org/10.6028/NIST.SP.800-53r5

Oliveira, T., Martins, R., Sarker, S., Thomas, M., & Popovič, A. 2019. Understanding SaaS adoption: The moderating impact of the environment context. International Journal of Information Management, 49, 1–12. Accessed on 1 May 2023. Retrieved from https://doi.org/10.1016/j.ijinfomgt.2019.02.009

OneTrust. n.d. Products. Accessed on 28 April 2023. Retrieved from https://www.onetrust.com/products/

Oracle. n.d. Business Manager's Checklist for SaaS Security. Accessed on 26 July 2023. Retrieved from https://www.oracle.com/a/ocom/docs/oracle-saas-security-checklist.pdf

OWASP Foundation. n.d. OWASP Top 10. OWASP Foundation. Accessed on 2 May 2023. Retrieved from https://owasp.org/www-project-top-ten/

Ozkan, B. Y., & Spruit, M. 2019. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. International Journal of Standardization Research (IJSR), 17(2), 41–72. Accessed on 3 May 2023. Retrieved from https://doi.org/10.4018/IJSR.20190701.oa1

Paddle. n.d. SaaS security: How to protect user data as a SaaS. Accessed on 5 May 2023. Retrieved from https://www.paddle.com/resources/saas-security

Panetta, K. 10 October 2019. Is The Cloud Secure. Gartner. Accessed on 9 March 2023. Retrieved from https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Pilgrim, S. 29 April 2022. 3 Benefits and Limitations of Private and Public Keys Need To Know Cryptocurrency Investors Need To Know To Secure Their Crypto—Security Pilgrim. Accessed on 22 September 2023. Retrieved from https://securitypilgrim.com/3-benefits-limitations-of-keys/

Preci ,E. 26 July 2022. SaaS Security Risk and Challenges. ISACA. Accessed on 3 May 2023. Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2022/saas-security-risk-and-challenges

Rahman, Abd., & Pribadi Subriadi, A. 2022. Software as a Service (SaaS) Adoption Factors: Individual and Organizational Perspective. 2022 2nd International Conference on Information Technology and Education (ICIT&E), 31–36. Accessed on 8 October 2023. Retrieved from https://doi.org/10.1109/ICITE54466.2022.9759891

SA. 22 December 2020. EUCS – Cloud Services Scheme. ENISA. Report/Study. Accessed on 6 October 2023. Retrieved from https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Slack. (n.d.). Where work happens. Slack. Accessed on 6 March 2023. Retrieved from https://slack.com/apps

Solanki, J. 30 June 2022. SaaS Security: CISO's Guide to Principles, Challenges, and Best Practices. Simform - Product Engineering Company. Accessed on 28 April 2023. Retrieved from https://www.simform.com/blog/saas-security/

Spanning Cloud Apps. (n.d.). Data A SaaSsins: Threats That Can Cause Data Loss. Spanning. Accessed on 10 March 2023. Retrieved from https://spanning.com/blog/threats-that-can-cause-data-loss/

Staff, I. 30 March 2022. Latest IDC Report with Global SaaS Market Analysis. InCountry. Accessed on 2 March 2023. Retrieved from https://incountry.com/blog/latest-idc-report-with-global-saas-market-analysis/

STAR. (n.d.). CSA. Accessed on 4 May 2023. Retrieved from https://cloudsecurityalliance.org/star/

Subashini, S., & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11. Accessed on 28 April 2023. Retrieved from https://doi.org/10.1016/j.jnca.2010.07.006

Tang, C., & Liu, J. 2015. Selecting a trusted cloud service provider for your SaaS program. Computers & Security, 50, 60–73. Accessed on 4 May 2023. Retrieved from https://doi.org/10.1016/j.cose.2015.02.001

Thais, S. 4 February 2023. GDPR impact on business – The library of essays of Proakatemia. Accessed on 22 September 2023. Retrieved from https://esseepankki.proakatemia.fi/en/gdpr-impact-on-business/

University IT. n.d. Minimum Security Standards for Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) | Stanford University IT University IT. Accessed on 2 May 2023. Retrieved from https://uit.stanford.edu/guide/securitystandards/saas_paas

University IT. n.d. Risk Classifications. Stanford University IT. Accessed on 10 August 2023. Retrieved from https://uit.stanford.edu/guide/riskclassifications#application-classification-examples

Verified Market Research. March, 2022. SaaS Management Platform Market Size, Share, Opportunities & Forecast. Verified Market Research. Accessed on 28 April 2023. Retrieved from https://www.verifiedmarketresearch.com/product/saas-management-platform-market/

Verizon. 2023. 2022 Data Breach Investigations Report. Verizon Business. Accessed on 2 May 2023. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Vincent van Dijk. 19 September 2022. 17 Things You Need to Know about NIST SP 800-53. Article. Accessed on 4 May 2023. Retrieved from https://www.securityscientist.net/blog/x-things-you-need-to-know-about-nist-sp-800-53/

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. 2015. Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. Computers in Human Behavior, 45, 254–264. Accessed on 2 March 2023. Retrieved from https://doi.org/10.1016/j.chb.2014.12.022

Appendix 1. SaaS Security Evaluation Tool-matrix

Saas security evaluation tool

Instructions for evaluating a SaaS (Software as a Service) tool:

· Identify the needs: Start by defining the team's specific requirements and objectives for the solution. Understand what functionalities the team needs and how the tool will fit into the organization’s workflow.
· Research Potential SaaS Tools: Explore various SaaS tools available in the market that match team needs. Consider features, user reviews, and pricing to narrow the options.
· Check Security and Compliance: Ensure the SaaS tool complies with data protection regulations and maintains robust security measures. Look for privacy policies and data encryption practices to safeguard the organization’s information.
· Evaluate Usability: Request a demo or free trial of the tool to assess its user-friendliness. Ensure it has an intuitive interface and is easy to navigate for the team.
· Scalability and Integration: Consider the tool's scalability significantly if the team's needs might grow. Check if it integrates well with the organization’s existing systems and applications.
· Performance and Reliability: Research the tool's performance and reliability. Look for uptime guarantees and customer reviews regarding downtime or latency issues.
· Customer Support: Investigate the level of customer support provided by the vendor. Check if they offer different support channels and response times to address the team’s queries and issues.
· Cost and Value: Analyse the pricing plans and billing structure of the SaaS tool. Ensure it fits within the team’s budget and provides value for money based on its features and benefits.
· Trial Period: Use free trials to test the tool with the team whenever possible.
· Get Feedback from the Team: Involve team members in the evaluation process. Gather their input and opinions to ensure the tool meets their preferences and requirements.
· Check Vendor Reputation: Research the reputation and track record of the SaaS provider. Look for customer testimonials and feedback to gauge their credibility and reliability.
· Read the Fine Print: Review the terms of service and contract before committing to the tool. Pay attention to cancellation policies, data ownership, and any hidden fees.
· Consult the IT department: The IT department can help with the decision process and
· By following these instructions, you can make an informed decision when selecting a SaaS tool that best fits your team’s needs and maximizes productivity for your team.

Instructions for the SaaS security evaluation tool:

Fill service's details to the table below.
The instruction section instructs how to verify that the Requirement can be validated. For example, validating Requirement Two-factor authentication is instructed by: “Verify is two-factor authentication available and is there a possibility to set up mandatory for all users.” Instruction means that the evaluation tool user should verify the solution provider's security page or setting

to validate whether there is a possibility to enable two-factor authentication or if that setting is possible to force to all user accounts.

Mark check

Tool user should document their findings by clicking the checkmark in the **Available section** and **Notes section**, for example, copying the description from solutions providers' documentation or a link to solution providers' documentation. This method helps other departments, like IT or procurement, verify evaluation results afterward.

SaaS Evaluation Tools includes four categories. There are different requirement levels; others are easier to complete than others. Also, the usage of the application differs.

The basic requirements every service should comply with include the most recommended security requirements, like Two-factor authentications and Data encryption.

The second category includes basic Data protection requirements, like the Data Processing Agreement (DPA) and vendor's data subprocessors.

The third category included requirements requiring more resources from service providers to comply. The applications in the third category process moderate risk-level information. This category includes a requirement of compliance, like ISO 27001 certification of Service level agreement (SLA) measurement.

The fourth and last category is related to a situation before purchasing or onboarding a new SaaS service.

The tool calculates the SaaS service's security score using values from 1 to 3, depending on the control's worth, and the tool provides a summary of the result.

Before onboarding the service, a reviewer should evaluate requirements in the last category to complete the evaluation process.

Service name:	
Domain:	
Description of the tool:	
Evaluator:	
Date:	

Security evaluation score		0	Points
Weak			
0-9: weak, 10-24: reasonable, 25+: exceptional			
max 33 points			

Level	Main section	Requirement	Description	Instructions	Available	Notes	Points
	Basic requirements that every service must comply, one point per line		Information about the requirement	Security descriptions will be found on solution providers webpages, from the security or trust page			
Basic	Access management	Two-factor authentication	Two-factor authentication helps to secure access to the data and accounts. It lowers the risk of credential theft. There should be a policy to force settings on all users.	Verify if two-factor authentication is available and if there is a possibility to set up mandatory for all users.	?		0
Basic	Access management	Single sign-on	Single sign-on allows authentication to the service without needing to remember and manage extra passwords using the organization's existing credentials.	Check if there is support for Single Sign-On using my organization's identity provider. If available, verify whether there is a method for provisioning user accounts automatically utilizing an integration service.	?		0
Basic	Data Protection	Data encryption	Data should be protected as it transits over the internet between the client and the cloud service, using TLS 1.2 or higher. By encrypting data when it is stored on disk, services can help to protect their data from unauthorized access, data breaches, and regulatory violations.	Ensure that the provider has robust security measures in place: including transit data over the internet using encryption TLS 1.2 or higher, data encryption at rest and in transit, secure data centres, and regular security audits.	?		0
Basic	Access management	Authentication to services and APIs	Internet-facing access to the service that can return protected information, for example, using API, must be protected by authentication.	Verify if the service has an API connection function. If available, verify, are internal and external APIs protected by authentication.	?		0
	Data Protection	Data protection regulation	The General Data Protection Regulation (GDPR) stands as a comprehensive data protection and privacy legislation in both the European Union (EU) and the European Economic Area (EEA). It also controls the transfer of personal information beyond these areas. Before purchasing a SaaS service that man-	Verify that SaaS providers comply with GDPR or other relevant data protection regulations. Privacy information will be found on solution providers webpages, from privacy, GDPR, or trust page	?		

			ages individuals' data, verifying that the service adheres to GDPR guidelines is essential.				
Basic	Data Protection	Data Processing Agreement (DPA)	A data processing Agreement (DPA) describes how service processes and secures personal data and should have defined the rights and obligations of each party regarding the protection of personal data. The privacy policy outlines how the service provider collects, uses, stores, and protects user data.	Verify that the SaaS provider has a clear Data Processing Agreement and a privacy policy.	?		0
Basic	Data Protection	Data Location	Ensure the location of data storage and processing by the service provider. GDPR mandates that any personal data from the European Union should be handled and stored correctly. If the SaaS provider operates or stores data outside the EU area, it needs that provider to demonstrate that they have equal protection as GDPR requires.	Verify the Data location in the service; if data is processed outside the EU/ETA area, Transfer Impact Assessment (TIA) is needed.	?		0
Basic	Data Protection	Vendor Subprocessing	It is crucial to understand the SaaS provider's subprocessors and verify that they are also in compliance with GDPR. This information is usually in the provider's Data Processing Addendum (DPA).	Verify SaaS providers and their possible subprocessors and verify that these subprocessors are also in compliance with GDPR.	?		0
Basic	Governance & Incident management	Vulnerability disclosure process	The vulnerability disclosure policy outlines how customers and security researchers can report vulnerabilities. This reporting process allows these identified weaknesses to be promptly addressed and remedied by the service provider. The service should proactively enhance its security measures and maintain a robust and secure platform for its users.	Verify there is a vulnerability disclosure process available and documented.	?		0
Basic	Data Protection	Support services	The service provider should have suitable support services. A good support service can help customers identify and resolve problems quickly and easily.	Evaluate the service provider's support functions. Are suitable support services available, like email, chat, or community? Are there available different Support	?		0

				levels or Dedicated customer success managers?			
	Intermediate requirements, where service processes more risky information than contact data, three points per line			Security descriptions will be found on solution providers webpages, from the security or trust page			
Intermediate	Governance & Incident management	Compliance	Documenting compliance is essential for SaaS providers because it can help them demonstrate compliance, build customer trust, and improve security. For example, ISO 27001 is a compliance standard and framework that ensures a range of security practices and controls are performed by the service provider.	Does the SaaS vendor comply with relevant industry standards such as ISO 27001, SOC 2, or PCI-DSS?	?		0
Intermediate	Access management	Privilege separation	Segregated duties mean that no single user has too many privileges. The solution provider can fix this by creating different roles with different levels of rights and by requiring multiple users to approve certain actions. Here are some specific examples of how these principles could be applied to a service: -A user with the admin role might be able to create, delete, and modify user accounts. -A user with the editor role might be able to create and modify content but not delete user accounts.	Verify the service possibility to provide different user roles and privileges. For example, administrative users can change all configurations, and standard users cannot.	?		0
Intermediate	Data Protection	Service level	Documented Service level agreement (SLA) that clearly defines the expected levels of reliability and performance. Here are some specific examples of what the SLA might include: -The percentage of time that the service is expected to be available. -The maximum response time for requests.	Check if the service has documented Service Level Agreement (SLA). SLA will include metrics like Uptime and response time. There might be automated monthly reporting of the service's health.	?		0

			-The maximum latency for data transfers. By including these metrics in the SLA, the user can ensure that the service provider is held accountable for meeting their expectations.				
Intermediate	Data Protection	Data backup	Backup is essential to securing the organization's data, and solution providers should ensure backup functionality to enable quick recovery in case of disasters. Encrypting the backup data prevents to avoid data leakage.	Evaluate the service's backup functions, and verify if there is available documentation of the frequency of data backup. Also, verify if there is an option to restore customer data quickly in case of data loss.	?		0
Intermediate	Data Protection	GDPR tool	The GDPR tools allow data subjects, like users and contacts, to access their personal data, request corrections or rectifications, request deletion, restrict data processing, and obtain data portability. These tools should be included in the SaaS service provider to provide these GDPR requirements effectively.	Verify there is an available GDPR tool to check collected personal data in the service.	?		0
Intermediate	Governance & Incident management	Security Audits	Regular security audits are an essential part of the security strategy for SaaS vendors. They help identify and mitigate risks, ensure compliance, build customer trust, and demonstrate a commitment to safeguarding data and maintaining a secure service environment.	Verify whether there is available documentation of SaaS vendors performing regular audits of their security controls and are these reports available for the customers.	?		0
Intermediate	Governance & Incident management	Security description	The security description provides an overview of the providers' measures and practices to protect user data and ensure the service's confidentiality, integrity, and availability. It summarises security protocols, access controls, encryption methods, and risk management procedures, assuring customers that their information is safeguarded against unauthorized access and cyber threats.	Verify whether the SaaS provider publishes a security description on their website. The description can also be a security whitepaper or a report from an auditor.	?		0
Intermediate	Governance & Incident	Security logging	Security logs assist both customers and the service provider identify any security	Verify whether the service provider collects security logs and	?		0

	management	and event collection	breaches. These logs should cover critical aspects like authentication attempts, configuration modifications, and information about accessed resources. Cloud service should grant customers access to these security logs, enabling easy export of customers' auditing systems.	whether records are available to the customer.			
Intermediate	Governance & Incident management	Incident response policy and applying updates	Incident response policy defines how solution provider has prepared themself for cybersecurity incidents—a well-defined procedure for implementing security updates on their internal systems and promptly addressing identified security concerns. Evaluating the provider's past performance is an informative measure of their ability to handle future security issues.	Verify whether the SaaS provider publishes the incident response process available. Also, verify if there is a policy for applying security updates in response to publicly reported issues in your service.	?		0
	Before on selecting the SaaS service, verify these requirements. Consult your organization's IT or procurement department.						
Before onboarding	Governance & Incident management	Ownership terms	Verifying license terms, professional services fees and pricing is essential when selecting a SaaS provider. These operations before purchase help with financial planning, contractual clarity, service evaluation, and overall business success.	Verify service's license terms, Professional Services Fee, and Pricing decision during the selection process. This helps to select a provider that meets your functionally and financially requirements.	?		
Before onboarding	Governance & Incident management	Business requirements	The solution should integrate with existing products in your organization's portfolio. The service provider should be financially stable with a sustainable business model, reducing the risk of sudden closure. Additionally, the provider should be able to collaborate with other services or tools that support activities within their specific market segment.	Verify that the SaaS solution is compatible with your organization's existing products, for example, integrations. Verify vendor's roadmap of product development. Also, verify that the solution provider is financially stable to avoid the risk of sudden closure of the service.	?		

Before onboarding	Governance & Incident management	Contacting the IT department	It is essential that the IT department verifies the SaaS service during the selection process and ensures that the chosen solution aligns with technical requirements, security standards, and overall business objectives, leading to successful integration and optimal utilization of the SaaS service.	Contact the company's IT department before selecting or using a SaaS provider. They will review your findings and assist you with purchasing the solution.	?		
Before onboarding	Governance & Incident management	Vendor lock-in Technical/integration requirements	Before terminating a contract with a SaaS provider, it is essential to have a data retrieval plan. Determine the timeline and format for data return if you switch vendors. Familiarize yourself with data backup and restore technology	Verify there is a method available to export or transfer data from the service when terminating the service.	?		