

How to make sure a web analytics vendor complies with key security standards – a helpful guide



Maintaining high data security standards is crucial for every company, especially those dealing with personal and confidential information. Taking appropriate precautions helps protect your data from unauthorized access or breaches.

When searching for a web analytics platform, you should pay attention to its functionalities as much as to the security certificates and standards it provides. However, not everyone knows the right questions to ask about security.

That's why we've gathered a list of the essential standards, regulations, and frameworks a security-conscious analytics provider should follow. We've divided this document into three parts:

1. Organization security	3
2. Data security	7
3. Application security	11

The list will help you determine if the analytics vendor you want to sign contracts with checks all the right boxes.

Let's get started.

Organization security

This section gathers information about essential security certifications, authentication standards, and security methods a web analytics vendor should apply. It will help you check the vendor's approach to security in its internal operations.

1. Security certifications, such as ISO 27001 or SOC 2

SOC 2 and ISO 27001 are international security certifications that confirm the highest data security standards for collecting and exchanging information within an organization. They cover processes, policies, and technologies designed to protect sensitive information.

ISO 27001 focuses on developing and maintaining an Information Security Management System (ISMS). To achieve ISO 27001 compliance, companies must conduct a risk assessment, identify and implement security controls and regularly review their effectiveness.

SOC 2 is more flexible. It contains five Trust Services Principles: security, availability, processing integrity, confidentiality, and privacy. In line with specific business practices, each organization designs its own controls to comply with one or more trust principles. Outside auditors assess the extent to which a vendor complies with the trust principle(s) based on the systems and processes in place.

There are two types of SOC 2 reports. Type 1 evaluates cybersecurity controls within a company at a single point in time to determine whether all the internal regulations are sufficient and correctly designed. Type 2 examines how a company's security system performs over a period of time to check if it's really effective. Therefore, achieving this type of report takes more time and is more expensive – but it's also more thorough.

It would be best if you chose an analytics vendor with these certificates. It means you can trust them to keep your information secure. Also, implementing these certificates ensures that all processes within a vendor's company are standardized and understood by employees, ultimately streamlining business operations.

2. User access management to systems, applications, and services

User management is the capacity to manage user accounts tied to different systems, devices, applications, networks, and services. It helps organizations handle which users can view, edit and access specific pieces of data. The vendor should assign different permission levels for particular roles within an organization. For instance, the support team should be able to change the configuration of some users' accounts, but they shouldn't have access to all the accounts or all the data in the accounts.

A security-conscious web analytics vendor should be able to explain its processes for user access management in a way that is understandable for its clients.

3. User authentication methods

User authentication is a security process that prevents unauthorized access to a vendor's network or devices. It's a login procedure that requests personalized passwords to give users authorized access to an app or a system.

Here are some examples of the most common and secure authentication methods:

- **Single sign-on (SSO)** – users log into one application and gain access to other connected applications with that action.
- **Two-factor authentication (2FA)** – users enter their primary authentication credentials, such as username or password, and then a secondary piece of identifying information, such as a code from an authenticator app, a phone number, or a device that can receive a push notification or SMS code.
- **Multifactor authentication (MFA)** – requires two or more independent methods to identify a user, such as codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics, or facial recognition.
- **Token-based authentication** – enables users to enter their credentials once and receive a unique encrypted string of random characters in exchange.

Employing at least one of these methods is necessary to protect sensitive information and personal data.

4. Internal network security

Network security procedures protect the network from breaches. These rules often concern network use, accessibility, and threat protection configurations.

Here are some examples of the most recommended network security methods:

- **Firewall** – a network security device that monitors incoming and outgoing network traffic and decides if each should be allowed or blocked based on a defined set of rules.
- **An intrusion prevention system (IPS)** – scans network traffic to block attacks actively.
- **An intrusion detection system (IDS)** – detects suspicious activities and generates alerts that help investigate the issue to amend the threat.
- **A virtual private network (VPN)** – encrypts the connection from an endpoint to a network, often over the internet. Moreover, it only allows access to resources hidden in the local network.
- **Access control** – as not every user should have access to your network, you should recognize each user and device. Then, you can enforce your security policies, for example, by blocking some devices or giving them only limited access.

If your analytics vendor follows the best internal network security practices, your valuable data and sensitive personal information is protected against cyberattacks.

5. Audits and penetration tests

External security audits systematically evaluate IT infrastructure defenses within the organization. During this examination, security professionals measure how well security protocols within the organization comply with established safety rules. These audits should be thorough and conducted regularly to secure the collected data and digital assets.

Also, internal audits are a great practice within the organization. They evaluate a company's internal controls and allow for identifying problems and errors before discovering them in an external audit.

Penetration tests go beyond security audits by trying to breach companies' security systems. It means that an impartial expert will try to break the IT infrastructure to see if the company could withstand a similar attack in a real-life scenario.

You should ensure that the analytics vendor you choose regularly goes through external and internal audits and pen tests. It will prove that your information is safely stored.

6. Service Level Agreement (SLA)

A service-level agreement (SLA) is a contract between a service provider and its customers. It defines what services the provider will deliver and the standards it must meet. An SLA allows you to hold your service provider accountable and details the type of service you can expect.

A customer service-level agreement includes the following:

- Exact details of the service expected by the customer.
- Provisions of the service availability.
- Standards for each level of service.
- Each party's responsibilities.
- Escalation procedures.
- Terms for cancellation.

Signing an SLA will help you ensure the continuity of data collection and the safety of your analytics application.

Data security

Data security relates to the vendor's privacy compliance and security methods regarding data hosting, storage, transfers, and backup.

1. Data privacy compliance

Data privacy is typically associated with properly handling personal data or personally identifiable information (PII), such as names, addresses, or credit card numbers. However, it includes other data types, including financial data, intellectual property, and personal health information.

For businesses, privacy guidelines are more complex than for individuals, but there are a few tactics that companies should include to become privacy-compliant:

- Collect only the data needed to fulfill their business goals (delete it after accomplishing them).
- Apply security methods within their organization (as mentioned in the previous section).
- Understand data sources, the purpose for using data, and how to collect and store it properly.
- Educate employees, partners, and customers about data privacy guidelines regularly.

When choosing an analytics vendor, ensure that they follow privacy regulations when handling clients' personal data.

For more information about data protection in analytics, read these blog posts:

11 new privacy laws around the world and how they'll affect your analytics

[Read more](#)



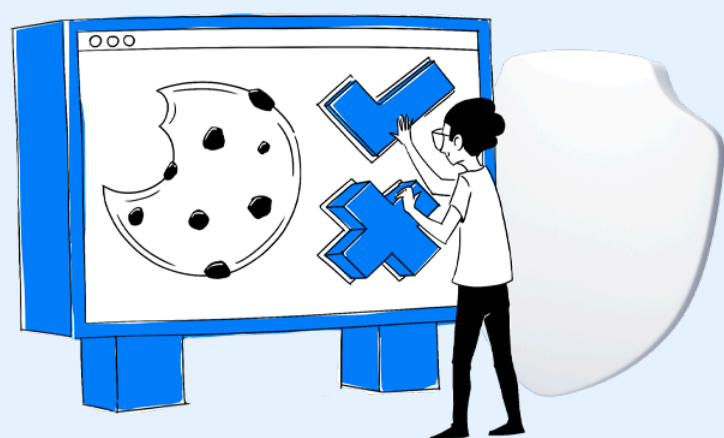
First-party data: The future of digital marketing

[Read more](#)



Everything you need to know about cookie consent in the EU

[Read more](#)



2. Data storage

Pick data hosting based on the data protection standards within your organization. The chosen method will affect the implementation and maintenance of the analytics platform. Organizations need to keep a healthy balance between efficiency and safety.

There are a few most popular methods for data hosting:

- **The public cloud** – is the most basic and cost-effective type of hosting that requires a cloud infrastructure provided by third-party cloud vendors.
- **A private cloud** – is a step above shared web hosting, in which infrastructure, including hardware and software, is dedicated to a single client.
- **On-premises** – is a physical, on-site server that a company must manage and maintain individually.

Your web analytics vendor should enable you to host data on the server and location of your choosing. To know more about data hosting methods, [read our blog post](#).



3. Data center security measures

Data center security concerns the physical and digital support systems and measures that keep its operations, applications, and data safe from threats. It includes a secure location, physical access controls, or monitoring systems. Data centers can receive various security certifications if they follow the applicable regulations and standards, such as HIPAA, PCI DSS, SSAE 18, SOC 2 type II, or ISO 27001.

In addition to the physical security systems, IT infrastructure requires a complete zero trust analysis incorporated into any data center design. Therefore, companies need to understand the security measures and the SLAs they have in place.

By choosing data centers that follow security regulations, your analytics vendor confirms its commitment to data protection.

4. Data transfers

You should always make sure that your analytics vendor transfers data securely. Applying the proper safeguards will guarantee that data will be accessed only by authorized people and will be protected from cyberattacks.

There are various methods for secure data transfers that your web analytics vendor can employ, including encrypted connection, HTTPS protocols and other security protocols, such as SSH (secure shell), SSL (secure sockets layer), TLS (transport layer security) and VPN (virtual private network).

5. Data backup policy

Data backups are essential for good storage security and overall business resilience. However, a significant percentage of security breaches come from mismanagement of data backups. That's why your analytics vendor should have a backup policy that defines all the rules for planning, executing, and validating backups.

You should check if your web analytics vendor considers the following issues while developing data backup policies:

- Technologies for data backups, recovery, and restoration.
- The frequency of backups and individual services.
- Types of data and systems that need to be backed up.
- Network infrastructure requirements to complete data backups.
- The professional team assigned to perform backups and recoveries.
- Emergency procedures if data backups become compromised.
- Procedures for ensuring that critical data is securely stored in the event of a data breach, ransomware attack, or other cybersecurity events.

If your analytics vendor has a proven data backup policy, it allows you to safely recover all the servers, network components, databases, and infrastructure. That means you don't have to worry if unexpected errors will destroy your data collection.

Application security

Application security focuses on requirements for lifecycle management, product updates, business continuity management, and vulnerability management programs.

Application security describes security measures that prevent an app's data or code from being stolen. It may include hardware, software, and procedures that identify or minimize security vulnerabilities.

1. Application security methods

Application security features may include:

- **Authentication** – ensures that a user is who they say they are. This can be done by providing a username and password or by including the security measures mentioned in the previous section.
- **Authorization** – gives the user permission to access and use the application after a user has been authenticated. The system can validate permission by comparing the user's identity with a list of authorized users. Authorization also includes the company's password policy, a set of rules designed to enhance computer security.
- **Encryption** – means security measures that protect sensitive data from being viewed or used by a non-authorized user.
- **Logging** – can help identify who got access to the data and how if there is a security breach in an application. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- **Alerting** – informing technical support about a breach by unauthorized personnel.
- **Application security testing** – is necessary to ensure that all of these security controls work correctly.

Application security is vital for reducing security risks and the overall impact of data breaches. If your analytics vendor follows the safe methods for application security,

each cyberattack can be identified and neutralized sooner, even before any severe damage to your data is done.

2. Lifecycle management

IT system lifecycle management is a process of overseeing the application's life, from conception, through maintenance, to retirement.

There are five stages of the system management lifecycle (SMLC):

- **Identifying risks** – listing the different risks the project could face and defining their characteristics.
- **Assessing their impact** – its goal is to sort risks according to quantitative and qualitative criteria, which facilitates categorizing them (high, moderate, or low) based on their potential impact.
- **Defining risk control strategies** – describe the actions that help avoid the risk, mitigate the adverse effects if the risk cannot be avoided, and find an alternative if the identified risk could compromise a crucial part of the project.
- **Monitoring your actions** – allows for setting up a process for tracking and monitoring risks throughout the project's development, which helps identify and control new risks.
- **Reporting the results** – this concerns saving your analysis and recording your tracking to make the history available to others, which makes it possible to derive good practices for future projects from your experience.

You should ensure that your analytics vendor practices lifecycle management processes in various areas of their business. That means that no redundant procedures are performed within the organization and proper operations are a priority.

3. Security guidelines for releasing new products, software, and updates

When planning a new release, your web analytics vendor should consider all the work needed to support customers during such a process. This includes, for example, updating the public website and training the support team.

Four steps should be followed to perform a secure product release:

1. **Reporting changes** – all changes should be carefully planned, added into the code repository, and registered, for example, in the company's internal communication spaces and the product changelog.
2. **Change review and approval** – all software code and server configuration changes require review and approval (at least two permissions are needed).
3. **Change testing** – changes to the product or software need to be preceded with tests, such as static code analysis, unit tests, integration tests, or acceptance tests. In addition, the product should be tested daily and nightly by an automatic test suite.
4. **Change deployment** – before changes are deployed to production and made available to users, the vendor's team needs to perform tests on testing and staging environments in the various configurations, such as testing on limited hardware with no data, on a pre-production environment that exactly resembles a production environment with production simulated data and on production deploy at a pre-scheduled time.

If your analytics vendor follows secure product requirements, this gives you an iron-clad guarantee that it supports customers' needs. For example, they will receive information about every change with accurate descriptions and documentation.

4. Vulnerability management programs

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting on, managing, and remediating vulnerabilities across endpoints, workloads, and systems. Typically, it is conducted by a security team that leverages a tool to detect vulnerabilities and utilize different processes to patch or remediate them.

The pre-vulnerability management process consists of five steps:

1. Determining the program's scope.
2. Defining roles and responsibilities within the process.
3. Choosing the vulnerability assessment tools.

4. Creating policy and SLAs.
5. Identifying asset sources.

It can help in staging, assessing, and measuring current resources, processes, and tools to identify gaps.

The vulnerability management cycle ensures that your analytics vendor prioritizes the essential tasks and processes critical to internal operations. You can be confident that the whole process of protecting your personal data is conducted according to the plan.

5. Business continuity management

Business continuity management (BCM) is a framework that allows companies to identify the risk of exposure to internal and external threats. Its goal is to effectively respond to threats such as natural disasters or data breaches and protect the organization's business interests. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management, and contingency planning.

According to ISO 22301, a BCM system focuses on the following:

- Understanding continuity and preparedness needs, the necessity for establishing BCM policy and objectives.
- Implementing and operating measures for managing the overall continuity risks.
- Monitoring and reviewing the BCM system's performance and effectiveness.
- Continual improvement based on objective measurements.

You should always ensure that your analytics vendor performs BCM regularly. This means that the internal processes within the organization are executed effectively.

Piwik PRO – our security standards

Piwik PRO is the first privacy-oriented alternative to Google Analytics. Created in 2013 in Europe, Piwik PRO Analytics Suite enables governments, public institutions, private companies, and enterprises to analyze and optimize the full customer journey while adhering to the strictest security policies and privacy regulations in the world. With a powerful platform comes high-touch customer care, training, and professional guidance in obtaining the most valuable insights for your business.

Operating under the best data security practices is our biggest priority, which is why Piwik PRO:

- Complies with [ISO 27001](#) and [SOC 2 Type II](#) norms.
- Goes through regular third-party audits and pen tests.
- Partners with selected ISO 27001-certified Microsoft Azure, AWS, and Elastix data centers, offering flexible hosting and data residence options.
- Helps you meet the stringent requirements of data protection laws worldwide, such as GDPR, CCPA, TTDSG, and more.
- Is suitable for industries handling sensitive customer data and allows you to adhere to HIPAA and the EBA's guidelines.

**Don't hesitate to contact us if you
want to learn more about our
approach to data security.**

Contact us

About Piwik PRO

Piwik PRO makes powerful, privacy-compliant analytics software and offers high-touch support, so customers can get the most out of their data.

Piwik PRO Analytics Suite provides flexible data collection and reports in addition to consent management, tag management and a customer data platform. Analytics professionals from leading organizations, such as the Government of the Netherlands, Crédit Agricole and Greiner, optimize customer and user journeys with Piwik PRO.

Contact

EMEA

+48 71 716 69 50

DACH

+49 2203 989 620

BENELUX

+31 858 881 458

NORTH AMERICA

+1 (888) 444 0049

<https://piwik.pro>

sales@piwik.pro

