Templafy

SOC 3

SERVICE ORGANIZATION CONTROL REPORT ON CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY, AND AVAILABILITY

For Templafy Services

For the period April 1, 2020 through December 31, 2020

Table of Contents

Section I: Independent service auditor's assurance report

To the Templafy Aps Board of Directors:

Scope

We have examined Templafy's (the "Service Organization" or "Templafy") accompanying assertion titled "Templafy's management assertion" (the "assertion") that the controls within Templafy's in-scope services and offerings for its Services pertaining to document creation, collaboration, productivity, and email signature ("system") were effective throughout the period April 1, 2020 to December 31, 2020, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality (applicable Trust Services Criteria), set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Templafy uses Public Cloud Service Provider Microsoft Azure. The description includes only the control objectives and related controls of Templafy and excludes the control objectives and related controls of Microsoft Azure. Our examination did not extend to controls of Microsoft Azure, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Templafy is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Templafy's service commitments and system requirements were achieved. Templafy has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Templafy is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We performed our examination in accordance with Dutch law, including Dutch Standard 3000A 'Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie (attest-opdrachten) (assurance engagements other than audits or reviews of historical financial information (attestation engagements). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

Our responsibilities in this regard are further described in the 'Service Auditor's Responsibilities' section of our assurance report. We are independent of Templafy in accordance with the 'Verordening

inzake de onafhankelijkheid van accountants bij assurance-opdrachten' (ViO, Code of Ethics for Professional Accountants, a regulation with respect to independence). Furthermore we have complied with the 'Verordening gedragsen beroepsregels accountants' (VGBA, Dutch Code of Ethics).

We believe that the assurance evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and Templafy's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Templafy's service commitments and system requirements based on the applicable trust services criteria;
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Templafy's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Service Organization's system were effective throughout the period April 1, 2020 to December 31, 2020, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Utrecht, 8th January 2021

On behalf of these,

Conclude Accountants BV

drs. J.E. ten Hoor RA
Partner

Section II: Templafy's management assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Templafy (the "Service Organization" or "Templafy") related to in-scope services and offerings for its Services pertaining to document creation, collaboration, productivity, and email signature ("system") were effective throughout the period April 1, 2020 to December 31, 2020, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality (applicable Trust Services Criteria), set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Our description of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

Templafy uses Public Cloud Service Provider Microsoft Azure. The description includes only the control objectives and related controls of Templafy and excludes the control objectives and related controls of Microsoft Azure. The description also indicates that certain Trust Services Criteria specified therein can be met only if Microsoft Azure's controls assumed in the design of Templafy's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The description does not extend to control of Microsoft Azure.

However, we perform annual due diligence procedures for third part sub-service providers and based on the procedures performed, nothing has been identified that prevents Templafy from achieving its specified service commitments.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2020 to December 31, 2020, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Templafy's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2020 to December 31, 2020, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the applicable trust services criteria.

Copenhagen, 8th January 2021

On behalf of Templafy,

Ellen Benaim
CISO

Section III: Description of the boundaries of the Templafy system

System overview and background

Templafy ApS (Templafy), headquartered in Denmark, is a business enablement Software-as-a-Service (SaaS) platform that provides document creation, collaboration, productivity and email signature tools (Templafy Services) for users of Microsoft Office and Google Suite, supporting every step of the document creation workflow. Templafy was founded in 2014 and has been fast-growing since, with employees in Denmark, the USA, The Netherlands, Germany, and Australia.

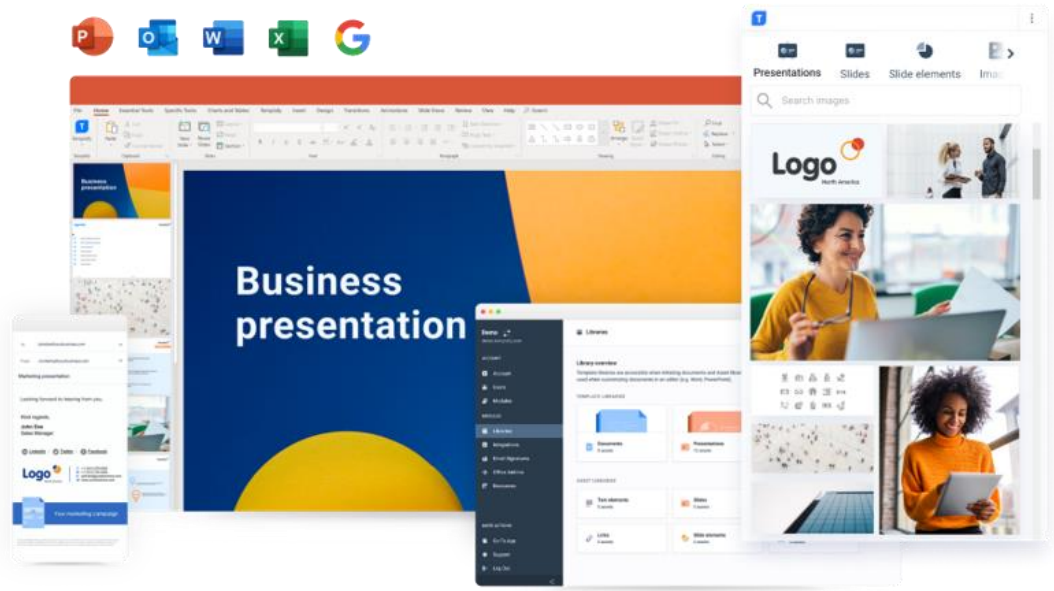
Templafy is committed to achieving and maintaining the trust of its customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across the suite of Services by design and default, including data submitted by customers to the Templafy Services. Templafy's enterprise customers span most industries globally, such as banking, financial services, professional services, industry, health, education and governmental. Both Templafy and its Services are crafted to meet their security, confidentiality and compliance requirements.

Templafy is a multi-tenant SaaS platform. Each organization that uses the Templafy Services shares a set of resources. Organizations share a common codebase, and their applications can be customized for their specific needs. The main interaction point for end-users is the Templafy web application and the Templafy add-ins. Add-ins are provided via Application Programming Interfaces (APIs) and add-in models by Microsoft and Google. Furthermore, Templafy integrates into or with Document Management Systems, CRM solutions, DAM solutions and ERP solutions via APIs.

Description of covered Services

The scope of this report covers the Templafy Services described in figure 2. Templafy provides various tools to enable businesses throughout the document creation lifecycle:

Templafy Solution



Service Name	Service Description
	Platform
One	**Real-time management and distribution** of document templates and digital assets. **Filtering and access management** with filters and AI powered tags. **Role-based access control** of user access rights throughout the platform. **Add-on's to content distribution** **Font Distributor** distributes and manages fonts across the whole organization for font control. **Offline content** distribution**.** **Integrations management** • **DAM** integration • **CRM** integration • **DMS** integration
Hive	*Templafy Hive is the **second iteration** of our platform. We moved from a monolithic architecture to a **microservices architecture** and structured our software in separate, connected units – much like a hive.* **Real-time management and distribution** of document templates and digital assets. **Filtering and access management** with filters and AI powered tags. **Role-based access control** of user access rights throughout the platform. **Add-on's to content distribution** **Font Distributor** distributes and manages fonts across the whole organization for font control. **Offline content** distribution**.** **Integrations management** **App** connector (e.g., Office applications, Office 365, Salesforce, G-Suite, Teams) **Data** connector (e.g., Salesforce, Highspot, SQL, other company data sources) **Content** connector (e.g.,, Bynder, Aprimo, other company DAM solutions) **Delivery** connector (e.g., SharePoint, Highspot, other company DMS solutions)

Modules

Library	**Direct access to the latest business document** assets like slides, graphs, text elements, images etc. through a user-friendly task pane add-in inside document creation applications. **Filtered access** to relevant assets based on user profile and office location. **Integrate and connect** with company image banks and digital asset management applications to bring all the relevant assets close to the user. *(optional)*
Dynamics	**Building, updating, and maintaining automatically personalized templates** with brand and compliance information through dynamic content fields. **Dynamically inserted metadata** and DLP information **Building, updating, and maintaining complex documents** like sales quotes, contracts and quarterly reports becomes an easy task.
Validator	**Chosen PowerPoint presentations validated against up-to-date** latest versions uploaded in Templafy. **Easy update of re-used presentations** through a simple popup appearing right in PowerPoint.
ProductivityPlus	**Pro-presentations made easy** using intuitive features designed to build complex slides while making professional formatting simple. **Import and link tables, data cells, and graphs from Excel to PowerPoint** with a simple copy-paste. Keep the linked data up to date with real-time update function.
Check	**Check function** inspects documents against up-to 40 pre-defined rules and ensures that the content, format, and layout are professional. **Fix format, layout, and content compliance issues fast** with one click before sending. Get an overview of issues in the Templafy task pane and use the Fix button to quickly amend the presentation.

Email signature manager	**Unified look and feel** for all email signatures for enterprise-wide use, and support for multiple signatures per user. **Management of multiple brands and office locations** in one dynamic layout through our easy-to-use centralized platform. **Real-time roll out and updates** of email signatures and seasonal campaigns. **Email signatures for Outlook Online, Windows, Mac and Mobile.** **Add on:** **Advanced mobile signature hosting solution** for no re-routing of emails outside of company servers with self-hosting.
Engage	*Only available on Templafy Hive platform* **Document sharing** embedded into the organic workflow of every employee. **Curated collaboration workflows** optimize the approval process, contract negotiations and co-creation. **Document insights dashboard with actionable data** transforms every business document into performing one.

Figure 2: Templafy Solution

Components of the system providing services

Overview of Templafy architecture

Templafy Services are operated in a multi-tenant architecture that is designed with tenant isolation to segregate and restrict Customer Data access based on business needs. The architecture provides logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role-based access privileges. Templafy Hive is made up of self-contained systems. Each self-contained system runs in a docker container hosted in Azure Kubernetes Service (AKS) to support millions of daily users. Templafy uses Infrastructure-as-Code with a focus on security and DevSecOps techniques. Additional data segregation is maintained by providing separate environments for different functions, including for testing and production. Product functionality and system architecture are designed with security by design and default.

Infrastructure

Function	Description
Public Cloud Service Provider *Microsoft Azure*	**One** North Europe (Primary) and West Europe (Secondary) **Hive** West Europe (Primary) and North Europe (Secondary) East US (Primary) and West US (Secondary) Australia data region available Q1 2021

Software

Function	Description
Operating Systems	Kubernetes Linux Docker Windows Server
Databases	Microsoft SQL server and databases
Monitoring Systems	There are multiple monitoring systems in use, including: • Azure Monitor • Azure Defender • Azure Security Centre • Advanced Threat Protection • Azure Application Insights • Azure Container Insights

	• Azure Sentinel • WhiteHat Security • SonarCloud
Network Infrastructure	Templafy Services' network infrastructure utilizes a common set of network components, including: • Azure Load Balancer • Azure Firewall • NGINX • Azure Virtual Network
Core systems	Microsoft Azure • Azure App Services • Azure Key Vault • Azure CDN • Azure Cognitive Services • Azure Storage Accounts • Azure Network Watcher • Azure Service Bus • Azure Data Lake • Azure DNS SendGrid Azure DevOps
Supporting systems	Dashlane PagerDuty StatusPage Zendesk Rackspace Aha! Slack
Endpoint protection	Full disk encryption Anti-malware Mobile device management

People

Templafy's structure is documented in its organizational chart, which shows the separation of duties and levels of oversight. The CEO leads the company, and there are multiple C-Suites who report to the CEO. Templafy's board of directors is comprised of representatives that are independent of management. The following teams are in-scope as their job responsibilities require that they have

access to production systems, develop code to be included in the environment or supporting operational and advisory functions:

Department	Responsibilities covered (Non-exhaustive)	Office Location
Engineering	Change, development, security and availability responsibility over Templafy Services	Copenhagen Berlin Eindhoven
Technical Operations	Deliver and support to customers	Copenhagen Berlin Eindhoven New York
Information Security	Security and Privacy over Templafy Services and Templafy	Copenhagen Berlin Eindhoven
IT	Provisioning and managing employee laptops and desktops Mobile device management Network management	Copenhagen Berlin Eindhoven
Customer Success	Enable the customer usage of Templafy Services	Copenhagen Berlin Eindhoven New York
Product	Strategic direction and prioritization of Templafy Services roadmap	Copenhagen Berlin Eindhoven
People+	Onboarding/offboarding employees Employee background checks Performance management	Copenhagen Berlin Eindhoven New York

Process and procedures

Templafy has implemented an Information Security Management System (ISMS) based on the International Organization of Standards (ISO) Codes of Practice for Information Security Management ISO IEC27000:2017 standard. Templafy chooses to focus on the highest quality level of controls to achieve a risk-based approach in preserving the confidentiality, integrity and availability of information. Organization-wide, Templafy is committed to continually improving the suitability, adequacy and effectiveness of the ISMS. Templafy has extensive information security policies and procedures pertaining to confidentiality, integrity and availability, such as:

- Information security
- Risk management
- Access control
- Physical and environmental security
- Personnel security
- Awareness and training
- Asset management
- Cryptography
- IT operations
- Network and information transfer
- Software development lifecycle
- Change management
- Vulnerability management
- Information security supplier management
- Incident response management
- Business continuity and disaster recovery

Data

Customer Data means electronic data and information submitted by or for the Customer to the Templafy Services as defined by the publicly available Templafy General Terms and Conditions Agreement (SaaS agreement). Templafy has an information classification procedure and has classified Customer Data as confidential, the highest level. Templafy complies with privacy standards and is governed by a data processing agreement to ensure the data receives the appropriate level of protection. Customers are covered under Templafy's data processing agreement available on the website unless a contract is otherwise entered. Templafy stores public enterprise information such as office locations and legal disclaimers, digital assets (such as office templates, email signatures, text snippets, images for image library, icons). All these digital assets that are provided by customer admins are then uploaded into the system. Contact information about employees such as name, job title, work email, work phone numbers and work location are stored to personalize the templates used.

Templafy has implemented best practices regarding encryption methods and has implemented a secure process for transmitting or receiving data across open, public networks.

- Templafy One and Hive support TLS1.2.
- Encryption at rest using AES 256-bit encryption is enabled by default throughout all Azure services in use for the Templafy Services.
- TLS1.2 is used to communicate between all the Azure services in use for the Templafy Services.

The transmission, movement, and removal of information are restricted to authorized internal users and processes. Encryption keys for built-in encryption are managed using Azure Key Vault and are subject to Templafy cryptography policy.

Templafy retains and disposes of customer data in a secure manner in accordance with customer agreements and information classification and handling procedures. Customer data is disposed of 90 days after termination of customer contract, and as soon as possible for active customers requesting specific data removal.

Customer responsibilities

Templafy instructs customers to contact the customer success team by phone or email, or to contact the information security team at support@templafy.com if they become aware of a possible security incident or breach. These instructions are communicated to customers through the SaaS agreement, available on Templafy's website, and verbally during procurement.

System Incident Disclosures

There were no system incidents during the period April 1, 2020 to December 31, 2020 requiring disclosure that either:

- Were the result of controls failing; or,
- Resulted in a significant impairment to the achievement of systems requirements or service commitments to customers.

Relevant Changes

There were no changes that are likely to affect report users' understanding of how Templafy provides the Templafy Services during the period April 1, 2020 to December 31, 2020.

Relevant aspects of the control environment, risk assessment, information and communication, monitoring

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), this section provides information about the five interrelated components of internal control at Templafy:

- Control Environment. Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

- Control Activities. The policies and procedures that help make sure that management's directives are carried out.
- Information and Communication. Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Monitoring. A process that assesses the quality of internal control performance over time.
- Risk Assessment. The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

Control environment

Organizational structure and assignment of authority and responsibility

The board of directors and executive management play an integral role in demonstrating from the top the importance of security, including integrity and ethical values throughout the organization. Information security is seen as a key strategic initiative, therefore the Chief Information Security Officer (CISO) reports directly to the chairman of the board of directors and meets regularly, at least quarterly, to discuss ongoing security efforts. The CISO is head of the information security department. The information security team implements the Information Security Management System (ISMS) and provides security guidance throughout the organization. Management communicates and oversees the requirements regarding conduct, professional integrity, and ethics by making the code of conduct available in Templafy's internal SharePoint site and through documents signed by employees.

Personnel security and awareness

Templafy has a strong security-first mindset due to repeated emphasis and communication around numerous security topics to all the organization on a frequent basis. Templafy has put in place security awareness initiatives and a training awareness program. All employees and contractors receive information security awareness training at onboarding, and at least annually thereafter. The security awareness training covers information on relevant security best practices and includes the responsibility for every employee and contractor to communicate security concerns. Job-specific training is provided to personnel where appropriate. Awareness is raised with weekly security updates in town hall meetings, communication efforts via email, and internal communication tools. New employees are required to review and acknowledge their receipt of the Information Security Policy, Acceptable Use Policy, and Information Classification and Handling Policy during onboarding. Confidentiality and intellectual property rights classes are included in employment contracts. Once employed, employees are subject to Templafy's procedures and sanctions for violating Templafy's information security policies.

Templafy has a process for revoking system and building access and returning assigned assets. This is integrated into the onboarding and offboarding process within the Human Resource (HR) system. The task to revoke system and building access are assigned to responsible individuals and are completed in a timely manner. The information security team is responsible for ensuring the onboarding and offboarding tasks are completed correctly and within stated time intervals.

For a change of roles or position change, an automatic alert is generated from the HR system to the information security team and based on this alert, a review is conducted as to the appropriate levels of access. Subsequent action is taken based on the review.

Background checks are performed on new employees, before they start at Templafy, who will have access to the production environment or production data, as permitted by local laws. Candidates are evaluated against documented job descriptions that define the skills, responsibilities, and knowledge levels required for all critical roles in the organization. Due to local restrictions in Germany and The Netherlands, a criminal record check cannot be performed in these countries, however; a criminal conduct search is performed in its stead. The background checks performed include identity verification, employment verification, professional reference checks and criminal record check. In the United States, a criminal felony and misdemeanor search within the last seven years is carried out.

A process and submission form are in place to facilitate anonymous notification of inappropriate behavior, including non-compliance with the Information Security Policy and its supporting standards. A formal sanctions process is enforced for personnel failing to comply with the established Information Security Policy and standards, where all reports of non-compliance are investigated by the information security team, and other department representatives as required, through to resolution.

Risk assessment

Templafy has established an organization-wide risk assessment process to identify and manage information security risks across the organization. Templafy regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security, availability, and confidentiality based on the applicable trust services criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Templafy performs an annual risk assessment that covers security, continuity and operational risks. The risk management process is derived from ISO 27005 and aligned with the COSO 2013 framework. As part of this process, threats to security are identified, and risks from these threats are formally assessed. Security risks related to external parties (such as customers, contractors, sub-processors and suppliers) are identified and addressed. The assessments include threats, vulnerabilities, impact, likelihood and mitigating controls. Following the risk assessment, a risk treatment plan is implemented to mitigate risks. After the treatment plan is evaluated and residual risk rating obtained, acceptance is obtained from risk owners. Changes in security threats and risks are reviewed by the information security team, and updates to existing control activities and information security policies are performed, as necessary. The CISO, as part of the annual management review of security, considers developments in technology and the impact of applicable laws and regulations to Templafy's security policies. The chairman of the board of directors receives reports on a quarterly basis covering the main ongoing risks and the management review report on security at year-end.

Information and communication

Templafy communicates the information security program in various ways via security awareness training, town hall meetings, internal communications via email and messaging tools, policies and

procedures uploaded to the Templafy's internal SharePoint site and verbally through daily interaction with the information security team.

Customers can request meetings with security personnel during procurement and at any stage during customer use of Templafy Services. Upon request, customers can receive security documentation, including the latest penetration testing results, latest external audit reports such as ISO27001 and SOC 2. Customers can report security incidents directly to support@templafy.com. Customers may view the most recent general terms and conditions, service level agreements and data processing agreements on the Templafy website. Communication with customers and partners can include their review of blog posts and knowledgebase articles, as well as communication related to the resolution of submitted support cases on Templafy's ticketing system through the Templafy website.

The information security team establishes and communicates an organization-wide information classification and handling policy in which information is classified, defined, exemplified, and risk assessed. The policy clarifies to all Templafy employees how to handle information throughout the information lifecycle based on their classification. The lifecycle includes authorization, confidentiality, labeling, information transfer and storage protections, transportation, retention and disposal. The policy is reviewed annually or more frequently to address significant organization changes. All Templafy employees share in the responsibility for ensuring that Templafy information receives an appropriate level of protection by observing the information classification restrictions and information handling process in the policy. The information classification policy is a module in the annual security training and all users must pass a test with 90% success criteria.

Monitoring

Vulnerability management

The Templafy Services and supporting infrastructure are monitored for availability and performance and will alert on-call engineering team members via a real-time alerting system if reliability, availability, or performance thresholds are not met. This triggers the incident management process as described in the incident management section.

Penetration testing is conducted to measure the security posture of the Templafy Services. Templafy outsources penetration testing to third-party suppliers who use an accepted industry standard penetration testing methodology. Templafy carries out two penetration tests a year. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network. Customer-led penetration testing can be conducted upon request to the information security team and is subject to conditions prior to carrying out the tests.

Vulnerability scanning is performed on a continuous basis by Templafy in accordance with the vulnerability management policy. Technologies used are:

- WhiteHat Security scanning for 24/7 web application dynamic application security testing (DAST),
- SonarCloud for static application security testing (SAST) before each release,

- Azure Security Center and Azure Monitor for daily infrastructure, network and application vulnerability scanning. Retests and on-demand scans are performed on an as-needed basis.

Testing results

Individual vulnerabilities identified during penetration and vulnerability testing are logged to the appropriate change management software and managed through the vulnerability management process. Scan and test results are assessed by the security and engineering teams, risks for each vulnerability are identified, and remediation are approved and prioritized until resolution in a timely manner. Vulnerability reports include a client summary, which is available to Templafy's customers upon request.

Complementary user entity controls

Templafy Services are designed with the assumption that certain controls will be implemented by user entities.

#	Complementary user entity control
1	User entities are responsible for understanding and complying with their contractual obligations to Templafy.
2	User entities are responsible for monitoring and enforcing organizational compliance with Templafy's terms and agreements.
3	User entities are responsible for keeping the primary, service, security, billing and administrative contact information on file with Templafy updated.
4	User entities are responsible for immediately notifying Templafy of any actual or suspected information security breaches, including compromised user accounts.
5	User entities are responsible for deploying releases of the Templafy Desktop MSI package without undue delay.
6	User entities are responsible for providing accurate and complete information and documentation regarding their own authentication method for authentication set up.
7	User entities are responsible for protecting established user IDs, passwords, and other credentials within their organizations, including appropriate safeguards for devices running Templafy applications.
8	User entities are responsible for maintaining their own signing certificate for SSO authentication methods and ensuring Templafy's technical operation teams receive updated certificate no later than three weeks before expiration.
9	User entities are responsible for reviewing their own access to Templafy periodically to validate the appropriateness of access levels.
10	User entities are responsible for removing terminated user accounts from the system either manually or through SCIM in a timely manner.
11	User entities are responsible for ensuring the appropriateness of designated administrators and maintaining a low administrator count according to the principle of least privilege.
12	User entities are responsible for informing Templafy of changes to their infrastructure (e.g., network ports and proxy settings) or application environment (Office platform, OS platform, Desktop/Application Virtualization) in order to ensure the continued functioning and support of Templafy.

Complementary subservice organization controls

Templafy uses subservice organizations for data center hosting and infrastructure services in support of its document creation, collaboration and email signature system. Templafy runs on Microsoft Azure Platform-as-a-Service, which provides many enhanced features for security, availability and scalability out of the box. There are clear lines of responsibility, but often, there are also shared roles when it comes to responsibility regarding security in the cloud. Templafy conducts due diligence towards Microsoft Azure annually to monitor the outsourced operations. This is achieved by reviewing Microsoft's SOC 2 and other compliance reports, as well as having the necessary agreements in place.

Control activity expected to be implemented by subservice organization	Subservice organization	Applicable trust services
Physical access to the data center facility is restricted to authorized personnel.	Microsoft Azure	CC6.4, CC6.5
All production media is securely decommissioned and physically destroyed prior to leaving the data center.	Microsoft Azure	CC6.5
External vulnerability assessments are performed on a periodic basis, identified issues are investigated and tracked to resolution in a timely manner.	Microsoft Azure	CC7.1
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	Microsoft Azure	A1.3
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Microsoft Azure	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2