Templafy

SOC 3

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

For Templafy Services

For the period 1 January, 2021 through 31 December, 2021

Table of Contents

Templafy

Section I:

Independent service auditor's assurance report provided by Conclude Accountants

Independent service auditor's assurance report provided by Conclude Accountants

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 1 January 1, 2021 to December 31, 2021, 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 1 January 1, 2021 to December 31, 2021, 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.

On behalf of Conclude Accountants,

Conclude Accountants BV

drs. J.E. ten Hoor RA

Partner

Utrecht | 7 January, 2022

Templafy

Section II:

Templafy's management assertion

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 1 January 1, 2021 to December 31, 2021, 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 1 January 1, 2021 to December 31, 2021, 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 1 January 1, 2021 to December 31, 2021, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the applicable trust services criteria.

On behalf of Templafy,

Ellen Benaim
CISO
Copenhagen | 7 January, 2022

Templafy

Section III:

Description of the boundaries of the Templafy system

The Templafy organization

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 (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, the UK 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 sSpan 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, Customer Relationship Management (CRM) solutions, Digital Asset Management (DAM) solutions and Enterprise Resource Planning (ERP) solutions via APIs.

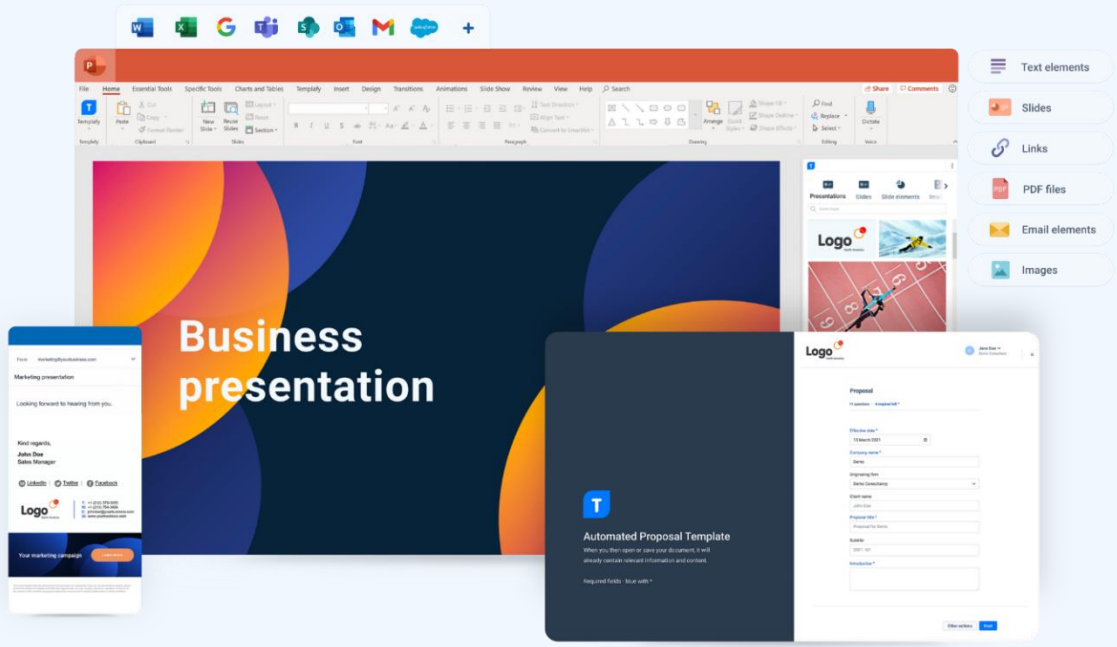

Figure 1 Templafy user experience

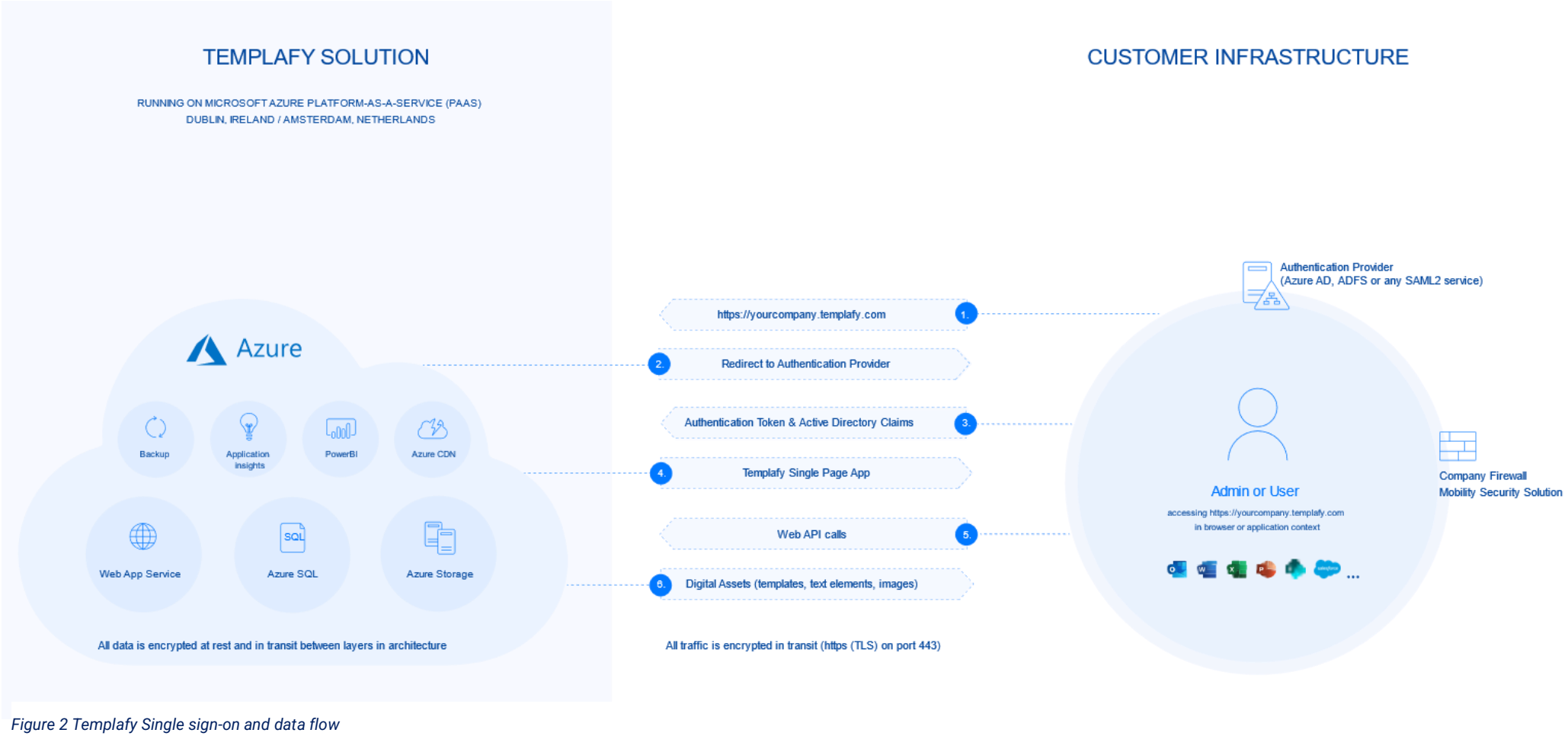

Figure 2 Templafy Single sign-on and data flow

Description of covered Services

The scope of this report covers the Templafy Services described in *Figure 3*. Templafy provides various tools to enable professionals to create better performing documents faster through connected content.

	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 (Artificial Intelligence) powered tags. Role-based access control (RBAC) of user access rights throughout the platform. Add-ons 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 the platform. Templafy moved from a monolithic architecture to a microservices architecture and structured our software in separate, connected units. 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 (RBAC) of user access rights throughout the platform. EU data protection access filter and activity log available to customer admins. Add-ons to content distribution: • Font Distributor distributes and manages fonts across the whole organization for font control. • Offline template distribution and access. • Spaces for content libraries to manage and distribute document templates and digital assets in real-time management to a specific group. Integrations management:

		• App connector (e.g., Office applications, Office 365, Salesforce, G-Suite, Teams). • Data connector (e.g., Salesforce, Highspot and other company data sources). • Content connector (e.g. Bynder, Aprimo and other company DAM solutions). • Delivery connector (e.g., SharePoint, Highspot and 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	Templates: Building, updating, and maintaining automatically personalized templates with brand and compliance information through dynamic content fields. Metadata: Dynamically inserted metadata and data loss prevention (DLP) information Compile: 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. Email signature servers hosted by Templafy or clients themselves. 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 3 Templafy Services

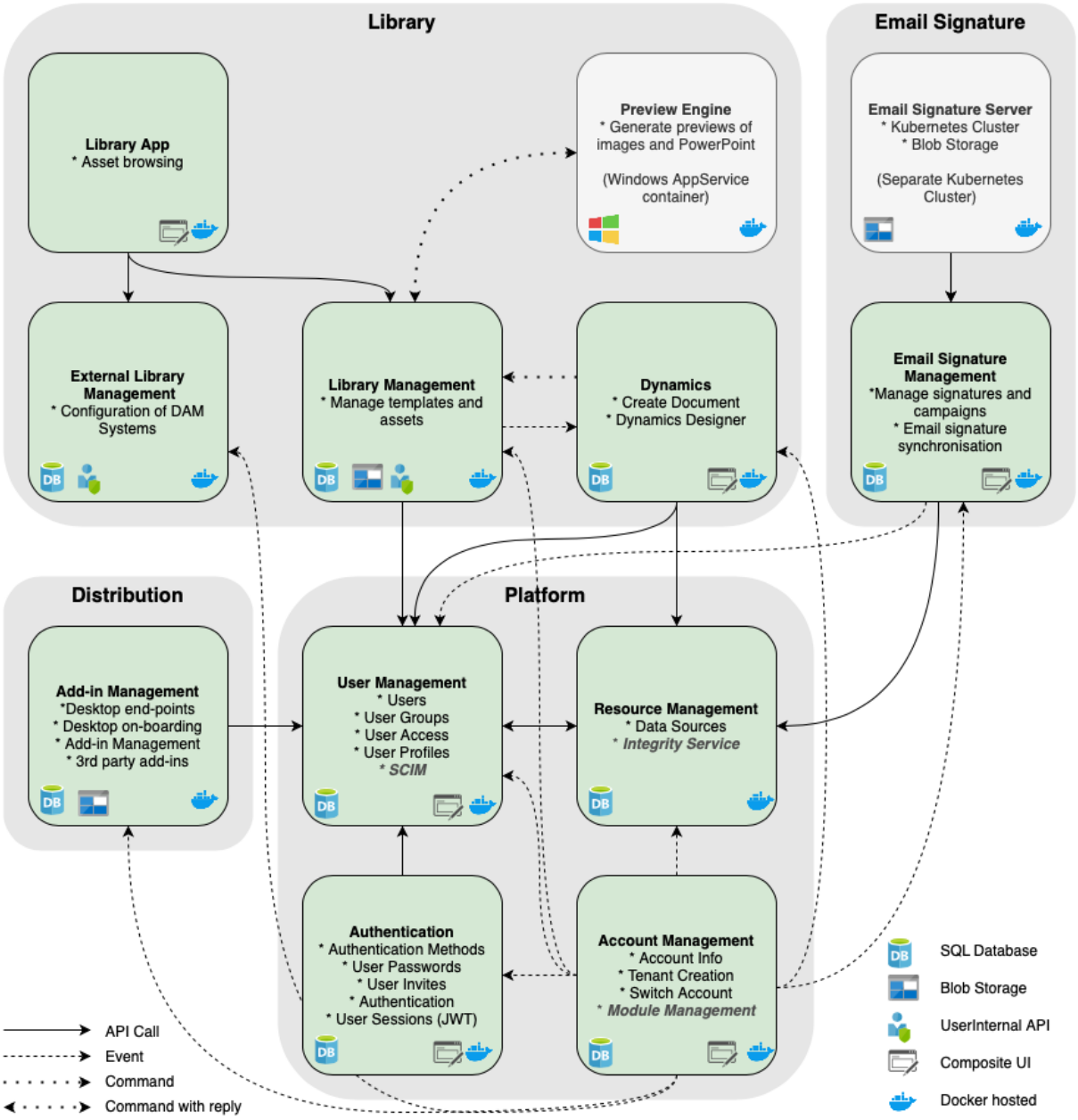

Figure 4 Self-contained system architecture

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 East (Primary) and Australia Southeast (Secondary)

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 • Network Security Group
Core systems	Microsoft Azure • Azure App Services • Azure Kubernetes Service • Azure Key Vault • Azure CDN • Azure Cognitive Services • Azure Storage Accounts • Azure Network Watcher • Azure Service Bus • Azure Data Lake • Azure DNS Amazon Simple Email Service (SES) SendGrid Azure DevOps
Supporting systems	Dashlane PagerDuty StatusPage Zendesk Aha! Slack

Endpoint protection	Microsoft Endpoint Manager BitLocker FileVault

Figure 5 Infrastructure components

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	Provision and manage 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

Figure 6 Templafy departments

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 agreements

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 retains and disposes of customer data in a secure manner in accordance with customer agreements and information classification and handling procedures. Customer data is disposed90 days after termination of customer contract, and as soon as possible for active customers requesting specific data removal.

Customer data elements

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. Digital assets are stored in individual blob storages per customer. Validation checks are done upon upload; file validation and restriction to certain file types occurs. Content length limit is in place for all requests. Input validation on front-end with property size check (e.g., string length, valid email address) before the back-end APIs are called. Back-end checks ensure full validation on domain layer and database layer.

Contact information about employees such as name, job title, work email, work phone numbers and work location are stored to personalize the templates used. User profile information is stored in a logically segregated SQL database. Users are authenticated based on customer admin selected authentication method. Customer admins determine which user profile data elements are processed by Templafy and modifiable by customer end-users. Templafy supports just-in-time (JIT) provisioning, single-sign on (SSO), multi-factor authentication (MFA), and on-boarding against customer Active Directories (AD).

Templafy data flow

Users access Templafy in the web application or application add-in (e.g., Word, PowerPoint). Add-ins are provided via Application Programming Interfaces (APIs) and add-in models by Microsoft and Google. Templafy also integrates into or with DMS, CRM solutions, DAM solutions and ERP solutions via APIs. APIs are subject to vulnerability scans and penetration testing.

A user starts the document generation flow by selecting a template file in the web application or application add-in. User profile information is retrieved from the SQL database and added to the template to personalize it as directed for the user.

Templates may have gating questions' answers injected into it as configured by customer admins, which the user can answer through a form interface. Templafy connects the template, any user profile information, data source information and the answers to the gating questions in a background job. The data filled template is permanently deleted after twenty-four hours from the unique temporary blob storage which is required to perform the injection. The end-user receives a read-only shared access signature (SAS) download link valid for a few minutes, where the final template is generated onto the local machine. The SAS link facilitates secure communication when data is stored in the blob storage.

The connection to Templafy ends here. The user can then use the data filled template to build further to the document or presentation, which is not stored back to Templafy. The file is shared on the customer's own local or cloud DMS. All requests throughout the document generation process are encrypted in transit and valid authentication of the user is required.

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.
- 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 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.

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.

Chairman of the Board of Directors

The Chairman of the Board of Directors oversees information security overall, sets strategic direction and assigns priority to support the information security objectives in Templafy. They allocate investment in alignment with the organization strategy and risk profile. They review Templafy's information security program's adequacy and effectiveness on a frequent basis. They have oversight of strategic security risks and provide prioritization and advisory.

CISO

The Chairman of the Board of Directors and Management Team have appointed a Chief Information Security Officer (CISO). The CISO is overall responsible for designing, implementing and monitoring a strategic, comprehensive Templafy-wide information security strategy aligned to the overall organization strategy. The CISO is a member of the Management Team and reports directly to the Chairman of the Board of Directors. The CISO reports to the Board at least annually. The CISO appoints and manages the Information Security department.

Management team

The Management team endorses and supports the development and implementation of a comprehensive information security program and its components. They review the status and impacts of security initiatives and act appropriately on management reports concerning information security performance metrics, security incidents and risks, investment requests, policy exceptions etc. The Information Security department's budget is approved in line with the budget process set by the Management team.

Information Security department

The Information Security department acts as a design and operational function, and the members work with various business units and other operational entities to implement a consistent and Templafy-wide information security program. The Information Security department are responsible for defining technical and non-technical information security standards, procedures and guidelines and supporting Templafy leaders and employees in the definition and implementation of controls, processes and supporting tools to comply with the information security policies and manage information security risks.

Leaders

Leaders must ensure their employees are informed of their obligations to fulfill the Information Security Policy where relevant to their roles and lead by example in respective departments.

Leaders must actively support the associated information security objectives and initiatives by providing the direction, resources, support and reviews necessary to ensure that information assets are appropriately protected within their area of responsibility. Leaders must monitor compliance and remind users of their obligations and escalate non-conformities as required.

Figure 7 Governance

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

Awareness training

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.

Onboarding and offboarding

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 People+ 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. Periodic access reviews are conducted as described in the logical security section.

Background checks

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.

Disciplinary process

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, privacy, 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.

Control activities

Software development lifecycle

Templafy's software development practices across each of the engineering teams are aligned with the Secure Development Lifecycle (SDLC) methodology and follow Scrum and Agile approaches. Detailed policies and processes for the development of the Templafy Services have been designed with optimal security and quality in mind. The principles of security by design and default are implemented and rooted in training, coaching, pair programming, code review comments, coding tools and branch policies in Azure DevOps. Templafy has implemented segregated environments for development, test and production as a means to support segregation of duties and prevent unauthorized changes to production. In addition, production data is not used or copied to non-production environments. Test scripts and synthetic data are created for use in the development and stage environments.

Change management

Changes are prioritized in collaboration with product owners and engineering teams. Information security and availability considerations are core components in application development and testing. Project management frameworks are used to manage application development and testing, and roles and responsibilities are identified throughout the system development lifecycle.

Azure DevOps is used to plan, schedule, approve, apply, distribute and track changes to the production environment with designated responsibilities and enforced through branch policies. It controls the integrity and reliability of the environment while maintaining a continuous delivery model without downtime.

All application code changes are tested, peer-reviewed and approved prior to implementation into production. The production and non-production environments are deployed in their own Azure Active Directory and their own Azure Subscriptions, thus completely separated, and changes are tested according to the nature of the change in an environment separate from production prior to deployment into a production release. Tests include functionality unit testing, integration testing, smoke tests, manual regression testing and load testing. Extensive security testing is conducted (see vulnerability management section).

All change requests are logged, whether approved or rejected, on a standardized central system. The approval of all change requests and the results thereof are documented. Access to migrate change to production requires formal approval and is restricted to authorized personnel. Code management tools enforce branch protection policies to help ensure users cannot bypass standard change controls.

The Product Owner and the engineering team discuss the status and progress of all outstanding changes within the current sprint during daily stand-ups. Release notes are documented and communicated to internal and external users via the knowledge center for changes related to feature and security changes.

Templafy maintains a continuous delivery model of the Services. Patch management is incorporated into the SDLC to ensure necessary updates, fixes and other changes are timely implemented to the Services. Patches are released like any other change in Templafy's SDLC and follow the same change management procedures. Patch implementation timescales are defined to ensure timely patching in accordance with severity. Different automatic release plans are made available to customers to choose from newest software features for testing purposes or stable and most reliable versions.

Baseline configuration hardening

Templafy's security configuration standards are applied through automated deployment mechanisms to help ensure consistent application. Templafy uses secure OS configurations deployed via Kubernetes. Templafy leverages hardened Azure Public Compute Images for servers. Templafy continuously monitors all resources deployed in the Azure environment in conformity to Azure best practices, CIS, ISO27001 and SOC 2 compliance requirements and applies applicable recommendations after review by the security guild.

Encryption

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.
- File and disk level encryption on blob storages.
- Disk level encryption on SQL database.

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.

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

Penetration testing is conducted to measure the security posture of the Templafy Services. Templafy outsources penetration testing to vetted 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

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.

Alerts and results

Anomalous user behavior is captured through user behavior analytic (UEBA) tooling. Centralized data loss prevention (DLP) solution is implemented as protection against data leakage. The information security team is responsible for continuous monitoring and reacting upon alerts from numerous rules from these technologies, feeding into centralized reporting dashboard.

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 is approved and prioritized until resolution in a timely manner. Vulnerability reports include a client summary, which is available to Templafy's customers upon request.

Log management

All Azure resources have audit logging enabled for the Templafy Services. This includes SQL and storage accounts. All activity in the production environment performed by users and administrators are tracked. Logs are protected from modification and are kept for a minimum of one year.

For Templafy Services, activity logs for administrator accounts are available in the admin portal of Templafy Hive.

For its internal infrastructure, Templafy collects, correlates, and analyzes data across users, devices, applications, and infrastructure using Azure Sentinel (SIEM). The information security team proactively threat-hunts for security incidents and reacts to threats that trigger pre-defined and configured alerts. Incidents are handled using the incident management process as described in the incident management section. All systems are configured with the same time and date to ensure traceability if an incident occurs.

Logical security

A formal, documented user account and access provisioning process is in place to assign and revoke access rights to systems and applications. Access is allocated on a least privilege basis, which means by default, account access is denied until a business need is proven, and any additional privileges require approval. Templafy uses Azure AD for centralized authentication and authorization to restrict access to the systems and services within the Templafy environment. Each user account is unique and is identifiable to an individual user.

Periodic reviews of individual accounts and security group memberships are performed by authorized individuals in the information security team or system owners, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review. Upon change of responsibilities, access rights are reviewed and addressed accordingly. Upon termination, access rights are revoked within 24 hours. Policies and standards have been established and implemented to enforce appropriate user account password length, complexity and history. Multi-factor authentication is required for critical systems and enforced where made possible by the system or application.

Access to customer data through the Templafy solution by Templafy employees will be granted only for customer support and success services offered in the best interest of the customer, or when a forensic investigation needs to be carried out following a security incident. The information security team is responsible for the access management to customer data and governed by the principle of least privilege. Access is monitored by the information security team and can revoke access at any time.

Access to program production data is restricted and limited to authorized personnel. Templafy has role-based access control to Kubernetes clusters. Access to production information systems is enforced via Azure AD multi-factor authentication. Appropriate identification and authentication are required to perform actions on the production environment and cannot be circumvented.

Asset management

Templafy has an asset management program that identifies information assets in scope for the ISMS and defines appropriate protection responsibilities. Any assets associated with information and information processing facilities are identified and managed throughout their lifecycle in accordance with the information classification and handling procedures. The lifecycle of the information includes creation, processing, storage, transmission, deletion and destruction stages. All information assets have owners.

Information classification and handling

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.

Endpoint management

All end-user laptops (Windows and MacOS) and mobile devices (iOS and Android) are centrally managed using mobile device management tool Microsoft Endpoint Manager, which enforce full disk encryption, endpoint protection, secure configuration and the ability to remote lock and remote wipe in the event a device is compromised. The Acceptable Use Policy requires that all work-related activities can only be done from devices that are managed by Templafy.

Templafy uses hardened baseline configurations deployed via Microsoft Endpoint Manager. Full disk encryption is configured and enforced on all end-user laptops and desktops. Templafy continuously monitors all endpoints in conformity to Azure best practices, CIS, ISO27001 and SOC 2 compliance requirements and applies applicable recommendations and required remediations after review by the information security and IT teams.

Windows and MacOS workstations are configured with centrally managed anti-malware protections that scans daily. Endpoints are configured with tamper protections to prevent impairment, disabling, or removal of anti-malware protections.

Network management

Azure Monitor is used to monitor the status and load of each managed network device. Azure Monitor provides detailed information of system metrics in dashboards and the ability to write custom queries to get essential data for all system behavior. It is used to monitor systems' current performance and investigate any irregularities from the past. The production environment has auto-scaling enabled. Templafy production data center network traffic is routed through a distributed denial-of-service (DDoS) protection service provided by Microsoft Azure to limit the effect of denial-of-service (DoS) attacks. The cloud guild in the engineering department holds routine meetings to review system capacity and environment health.

The site reliability engineering team actively monitors network logging for the production network. Azure DDoS protection and Security Center generate alerts subject to review and investigation. An intrusion detection system (IDS) and intrusion prevention system (IPS) are configured to generate alerts following breaches of thresholds. Customer traffic is managed with load balancing. Templafy's network includes a demilitarized zone (DMZ) for web-facing systems using an Azure Network Security Group..

All external network connections to the SQL server are protected by a firewall that verifies inbound traffic based on source and destination address, protocol and port. The site reliability engineering

team maintains the whitelist regularly. Changes to the firewall require a pull-request as described in the change management section.

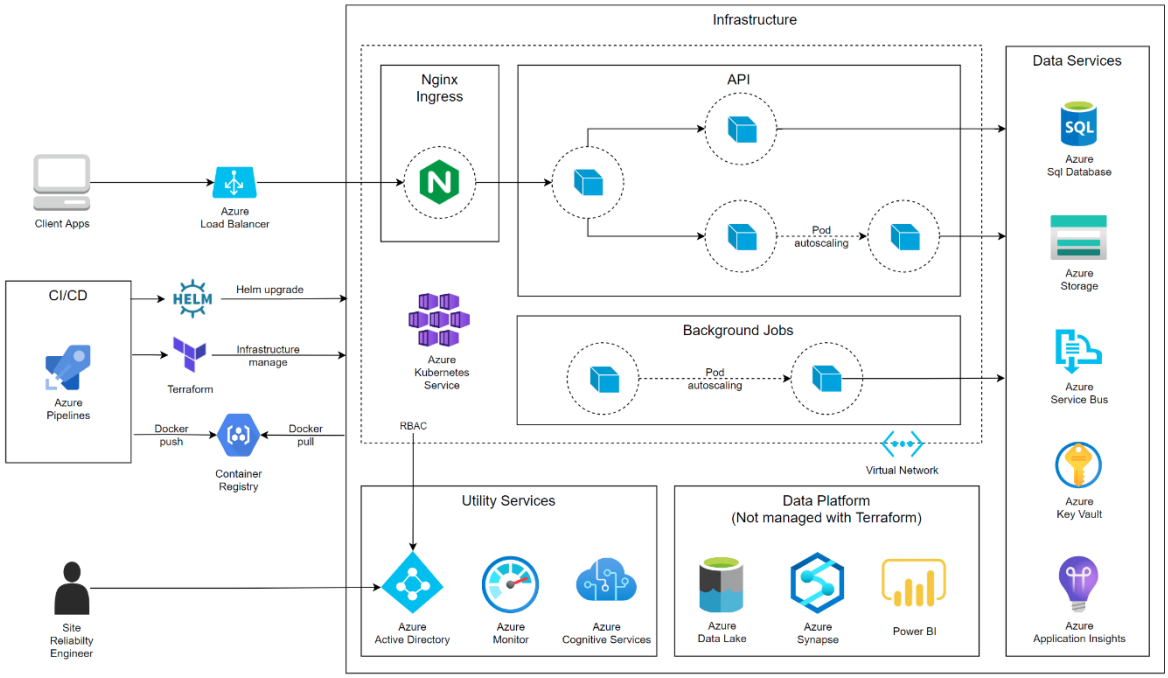

Figure 8 Network diagram

The corporate network supports internal business functions and is separate from the production network for each of the Templafy Services that support customer instances. Each corporate office location has multiple security controls to protect the network proportional to the risk assessment conducted on the network. Networking protocols that are not necessary for business purposes and/or are deemed to be non-secure are disabled. The corporate networks are segregated into VLANs based on business requirements.

Incident management

Templafy has implemented an incident management policy that includes defined processes, roles, communications, responsibilities and procedures for detection, escalation and response to incidents internally and to customers.

Templafy's information security team uses the established incident classification, escalation and notification process for assessing an incident's criticality and severity. Response procedures are specific and reflect the nature of the incident. Incident and resolution analysis are carried out by the information security team to reduce the likelihood or impact of a future incident. Incident procedures in relation to data privacy breaches have been implemented and include how and when to communicate with the data controller affected and the relevant authorities. Procedures for a forensic investigation of a security incident are in place when necessary to support potential legal action.

Incidents that impact availability of the Templafy Services are monitored and detected using Azure Application Insights and Container Insights. These alerts trigger PagerDuty which calls to action the site reliability engineers. The on-call responder identifies the incident severity. Depending on the severity, roles are assigned including primary responder, subject matter experts and communication coordinator. All activity around the incident is captured through video recording, internal notes and Azure DevOps Issue for tracking. A Blameless Postmortem is scheduled within six business hours of the resolved incident, inviting all the people involved in identifying, solving, and communicating about the incident. An official Postmortem, approved by Product Owners or CTO is posted to StatusPage for external communication in a timely manner.

Data backup and recovery

Data backup

For Templafy Services, tenant configuration data and binary data are backed up daily in SQL. In Templafy Hive, a 90-day point in time geo-redundant backup of SQL is available. Data in storage accounts are written to three disks for redundancy per site and replicated across multiple sites. The backup system automatically generates a backup log. Access to backup data is restricted only to authorized personnel using Azure AD with multi-factor authentication. Furthermore, all backups are encrypted using AES 256 encryption. Tenant backups are performed daily and automatically re-run as needed until successful. Templafy's support team responds to incidents related to backups and escalate to the appropriate team when necessary.

Redundancy

Templafy uses multi-site data centers with availability commitments to permit the resumption of Templafy Services in the event of a disaster or partial outage at its primary data center location. Templafy has a documented disaster recovery plan. This plan is reviewed and tested at least annually, and test results are reviewed by plan stakeholders. When necessary, plan documentation is updated.

Business continuity and disaster recovery

Templafy prioritizes the availability of the Templafy Services to its customers and plans for a variety of situations that may impact them. Templafy has established an organization-wide Business Continuity Policy that serves as a guideline for implementing uniform business continuity plans. Risk assessments are conducted to identify and assess business continuity risks across all office locations and Azure services. Protection measures are put into place to react to natural and human-made threats accordingly.

The business continuity plans cover the key personnel, resources and actions required to continue critical business processes and operations. Templafy performs an annual Business Impact Analysis (BIA) to identify the operational and financial impacts of any unplanned disruption to Templafy's business operations. The results of the BIA are integrated into the business continuity plans when relevant. The information security team conducts testing of the business continuity and disaster

recovery plans annually. Any issues identified during testing are resolved, and plans are updated accordingly. The business continuity plans are reviewed annually.

Physical security

Data center security

No servers or computer facilities for the Templafy Services are hosted onsite. All physical access to facilities and environmental controls are controlled at the Cloud Service Provider (CSP) locations of Microsoft. Stringent physical and operational controls are in place and are accounted for by Microsoft's numerous ISO certifications and standard compliance, which are reviewed during the sub-processor annual evaluation by the information security team against Templafy's information security requirements, as described in the supplier management section.

Office security

Templafy maintains a physical and environment policy for its offices to ensure the security and integrity of Templafy's facilities and the assets located within. Templafy has physically sound buildings protected by appropriate security controls such as alarms, locks, reinforced windows, and emergency equipment. Keycard controlled locked access is in use and are timely removed as described in the logical security section. Visitors to secure areas are required to sign in and out with arrival and departure times, are required to wear an identification badge, and always escorted while in secure areas. Delivery and loading areas are managed and appropriately protected.

Supplier management

Templafy has established an organization-wide Information Security Policy for supplier onboarding, monitoring and offboarding. The policy outlines the controls that are implemented to ensure that suppliers live up to security and privacy requirements laid out by Templafy, and that this is appropriately managed by Templafy personnel involved in supplier relationships. The policy applies to all suppliers used by Templafy that have access to or process Templafy information, and thus must adhere to Templafy's information security requirements. This includes Templafy's sub-processors. Supplier relationships are managed with a risk-based approach in line with the information security objectives.

Supplier assessments and monitoring

All suppliers undergo a procurement assessment to identify the amount and severity of risks involved in the supplier relationship, as well as how critical the relationship is to the business at the procurement phase and are monitored thereafter at a frequency proportional to the calculated level of criticality and level of risk. More thorough assessments on security and privacy are conducted to ensure that suppliers meet the minimum information security requirements set out by Templafy. Depending on the supplier, assessments may be in the form of one or more of the following:

- Questionnaires filled out by the supplier, Templafy, or both. These may be following standard security framework e.g., ISO27001) and/or standard security questionnaires e.g., SIG, or custom-made by Templafy.
- Review of audit reports and/or certificates, e.g., ISO27001, SOC 2.
- Technical review meetings with the potential supplier.
- Reviewing further evidence such as suppliers' written policies or SOPs.
- Other means deemed applicable to the nature of the supplier relationship in question.

Supplier agreements

Templafy enters appropriate contractual agreements with suppliers. Depending on the supplier relationship, multiple agreements may be required, e.g., information security requirements, data privacy requirements, service level agreements, data processing agreements. All sub-processors have data processing agreements and are updated on a frequent basis subject to regulation changes. Templafy requires that suppliers sign a confidentiality and non-disclosure agreement prior to sharing confidential information.

Information and communication

Internal 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.

External communication

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 security@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 knowledge base articles, as well as communication related to the resolution of submitted support cases on Templafy's ticketing system through the Templafy website.

Monitoring

Internal audit

Templafy has an internal audit function independent from control design and implementation periodically audits each area of Templafy's ISMS.

Legislative and contractual compliance

Contractual and legislative requirements are registered, reviewed, updated, and compliance monitored on an ongoing basis.

Knowledge and research

The Information Security team is responsible for keeping updated with changes in the cybersecurity and data protection threat landscape, through periodic research and contact with special interest groups, specialist security forums and professional associations.

Changes to the system during the period

There were no changes that are likely to affect report users' understanding of how Templafy provides the Templafy Services during the period 1 January, 2021 to 31 December, 2021.

Disclosure of incidents

There were no system incidents during the period 1 January, 2021 to 31 December, 2021 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.

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, to security@templafy.com.
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 setup.
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, including any third party access they may have granted.
10	User entities are responsible for removing terminated or unwanted user accounts from the system either manually with the use of the deletion feature made available by Templafy or through SCIM in a timely manner.

13	User entities are responsible for ensuring the appropriateness of designated administrators and maintaining a low administrator count according to the principle of least privilege.
14	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.

Figure 9 User entity responsibility

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
Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) are implemented to safeguard sensitive data and information systems.	Microsoft Azure	CC6.2, CC6.3, CC6.4, CC6.5
The data center facility is monitored 24x7 by security personnel	Microsoft Azure	CC6.4, CC7.2

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

Figure 10 Subservice organization controls