grammarly

System and Organization Controls (SOC 3) Report

Management's Report of Its Assertion on the Effectiveness of Its Controls over the Grammarly System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy for the Period April 1, 2024 through March 31, 2025

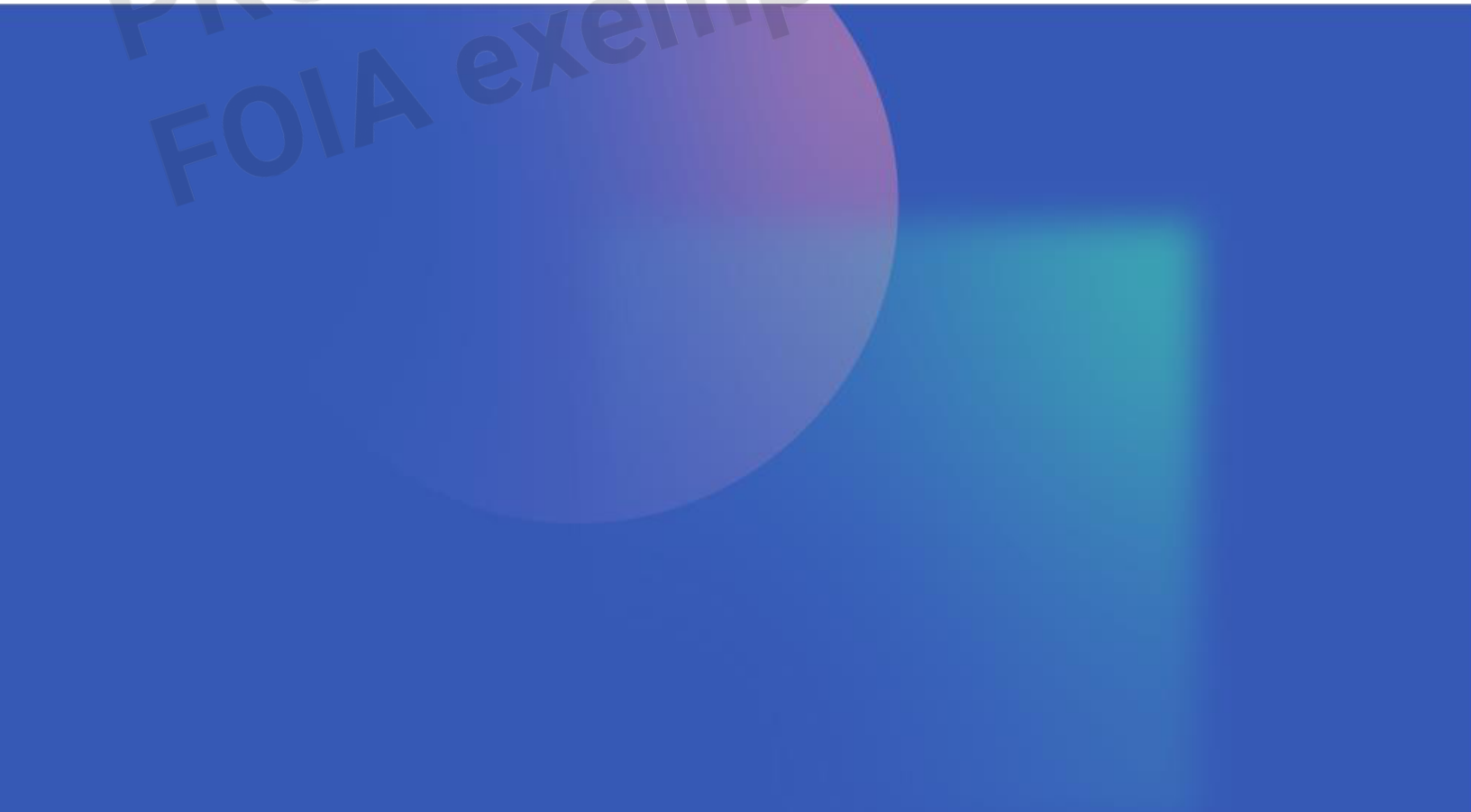

Table of Contents

Section 1 – Management's Report of Its Assertion on the Effectiveness of Its Controls Over the Grammarly System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy for the Period April 1, 2024 to March 31, 2025

Management's Report of Its Assertion on the Effectiveness of Its Controls Over the Grammarly System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy for the Period April 1, 2024 to March 31, 2025

We, as management of Grammarly, Inc. are responsible for:

- Identifying the Grammarly's Services (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of our service commitments and service requirements that are the objectives of our System, which are presented in Attachment B
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirement
- Selecting the trust services categories and associated criteria that are the basis of our assertion

Grammarly uses Amazon Web Services ("AWS", a subservice organization) to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The description of the boundaries of the system presented in Attachment A indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Grammarly to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Grammarly's controls. It does not disclose the actual controls at AWS.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Very truly yours,

Management of Grammarly, Inc.

Section 2 – Report of Independent Accountants

Shape the future with confidence

Ernst & Young LLP
303 Almaden Blvd
San Jose, CA 95110

Tel: +1 949 794 2300
Fax: +1 866 492 5140
ey.com

Report of Independent Accountants

Management of Grammarly, Inc.

Scope

We have examined management's assertion, contained within the accompanying Management's Report of Its Assertion on the Effectiveness of Its Controls Over the Grammarly System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy (Assertion), that Grammarly's controls over the Grammarly Services (System) were effective throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Grammarly's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Grammarly uses Amazon Web Services (subservice organization or "AWS") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Grammarly, to provide reasonable assurance that Grammarly's service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our procedures did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period April 1, 2024 to March 31, 2025

Management's Responsibilities

Grammarly's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Grammarly's service commitments and system requirements were achieved. Grammarly management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Shape the future
with confidence

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Grammarly's relevant security, availability, confidentiality, and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Grammarly's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Grammarly's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Grammarly's AI services.

We are required to be independent of Grammarly and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Grammarly's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Shape the future
with confidence

Opinion:

In our opinion, Grammarly's controls over the System were effective throughout the period April 1, 2024 to March 31, 2025 to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

May 20, 2025

Attachment A – Description of the Boundaries of Grammarly

Description of the Boundaries of Grammarly

Company background

Max Lytvyn, Alex Shevchenko, and Dmytro Lider founded Grammarly in 2009 with the goal of helping people communicate more effectively. Focusing first on supporting students' grammar and spelling through a subscription-based product, they soon saw the potential of how Grammarly could help in all circumstances—from professional writing to everyday correspondence. Since then, the company has grown the capabilities of an AI-powered writing assistant to go far beyond grammar and spelling into supporting complex aspects of language and communication so that all people can be understood as they intend. Grammarly's growth and further investment in cutting-edge language research have been helped along by more than $200 million in funding, led by General Catalyst.

Grammarly is headquartered in San Francisco and has offices in Kyiv, New York City, Vancouver, Seattle, Berlin, and Warsaw. Grammarly's mission-driven team is connected by their EAGER values—ethical, adaptable, gritty, empathetic, and remarkable. Team members are deliberate about applying these values to everything Grammarly does—whether it's committing to an inclusive and learning-oriented work environment, supporting Grammarly users with compassion and integrity, or thoughtfully creating a secure product that connects people.

Product overview

Grammarly's digital writing assistance helps 30 million people, and 70,000 professional teams to write more clearly and effectively every day. Grammarly's real-time suggestions offer feedback on correctness, clarity, engagement, and delivery. The product supports users across various product offerings—including Windows and Mac desktop applications, a web editor, browser extensions, mobile keyboards and apps, and a Microsoft Office add-in. A free version of the assistant provides essential writing support to anyone who needs to communicate in English. Grammarly's paid offerings help enterprises, academic institutions, and teams of all sizes accelerate business results through clear, consistent, and on-brand communication by providing all Grammarly suggestions, tailored administrative controls, and enterprise-level features.

Scope

The scope of this report includes the following Grammarly client applications, available for organization customers, as well as individual users:

- **Grammarly Editor**: Grammarly's intuitive text editor is a central place on the web to write. Users can customize the types of writing suggestions they see based on their goals.
- **Grammarly for Windows and Mac**: An all-in-one desktop application that works in browsers and on many desktop apps including word processors, email clients, and more.
- **Grammarly browser extension**: Whether a user writes in Chrome, Firefox, Safari, or Edge, Grammarly's browser extension offers suggestions on a vast array of websites, including Google Docs, Zendesk, LinkedIn, X, and Medium.
- **Grammarly for Microsoft Office**: Grammarly's add-in for Microsoft Office brings Grammarly's writing suggestions to users writing in Word or Outlook. (On Mac, the add-in is only available for Word.)
- **Grammarly for iPad**: Grammarly's iPad app provides users with:
    - Grammarly Keyboard for iPadOS
    - Grammarly iPad Editor
    - Grammarly for Safari on iPad
- **Grammarly for iPhone**: Grammarly's iPhone app provides users with:
    - Grammarly Keyboard for iOS
    - Grammarly iPhone Editor
    - Grammarly for Safari on iPhone
- **Grammarly Keyboard for Android:** For writing on the go, the Grammarly Keyboard offers Grammarly's writing assistance directly through Android mobile devices.
- **Grammarly for Samsung Keyboard:** A direct integration of Grammarly's writing assistance technology into Samsung native keyboards allows users to get suggestions wherever they type.

Organizational structure

Grammarly has defined structures and reporting lines, outlined clear areas of authority, and assigned responsibilities in order to achieve its company-wide objectives. This structure includes clearly delineated operational practices of teams and functions across the

organization, including Security, Engineering, Product, IT, Legal, People, Sales, Marketing, Finance, Language Technology, Workplace Experience, and Customer Support.

The Chief of Information Security Officer ("CISO") is responsible for managing security (confidentiality, integrity, availability) and privacy within its organizational structure. The CISO acts as Information Security and Privacy Management System ("ISPMS") Manager and is responsible for overseeing the ISPMS operations.

The following teams are relevant for this report:

- **Board of Directors**: Responsible for establishing and overseeing company strategy.
- **Executive**: Responsible for overseeing all company operations.
- **Security**: Comprises of six sub-teams responsible for ensuring security across the company.
    - **Product Security**: Collaborates with Grammarly Engineering to share advanced security expertise and help ship product offerings with industry-level application security.
    - **Platform Security**: Builds and supports the production infrastructure's security, focusing on the cloud and data platform.
    - **Detection and Response**: Supports Grammarly's security program by owning monitoring tools and security incident response.
    - **Corporate Infrastructure:** Builds and supports enterprise infrastructure, focusing on identity and access management, corporate networks, and endpoint security.
    - **Trust Engineering**: Builds services for authorization, authentication, privacy, and security, providing Grammarly's user-facing products with functionality to manage identity, consent management, encryption, and related privacy functionality.
    - **Security Intelligence**: Enhances security prioritization by proactively generating and processing information from diverse sources to identify, prioritize, and mitigate potential threats to Grammarly assets.
- **Legal**: Provides legal review and support for all privacy-related aspects of Grammarly's product ecosystem and global company policies.
    - **Governance, Risk, and Compliance:** Establishes and coordinates security processes and practices across the organization in compliance with industry security standards.
- **Developer Experience and Cloud Infrastructure**: Considers custom requirements and constraints to provide an optimal company-wide infrastructure toolkit that helps engineers focus on product development and maximize value for end users.

- **Engineering Organization**: A collaborative group of technical teams responsible for building and supporting Grammarly's product ecosystem. Also referred to as Grammarly Engineering.
- **IT**: Provides assistance with hardware issues, software licenses and management, office network laptop support, and other requests relating to information technology.
- **People**: Comprises multiple teams delivering company-wide programs and solutions for Grammarly's team. The People Operations, the Learning and Development team, and the People Partners address organizational learning needs, deliver benefits and team support systems, develop and manage people programs, implement global compensation and benefits strategies, manage diversity and inclusion programs, and provide coaching and partnership solutions to meet business needs. The Recruiting team oversees Grammarly's hiring processes and operations.
- **Customer Support**: Provides timely, empathetic help that keeps the customer's needs at the forefront of every interaction.

Principal architecture

Grammarly's product infrastructure comprises the following main components:

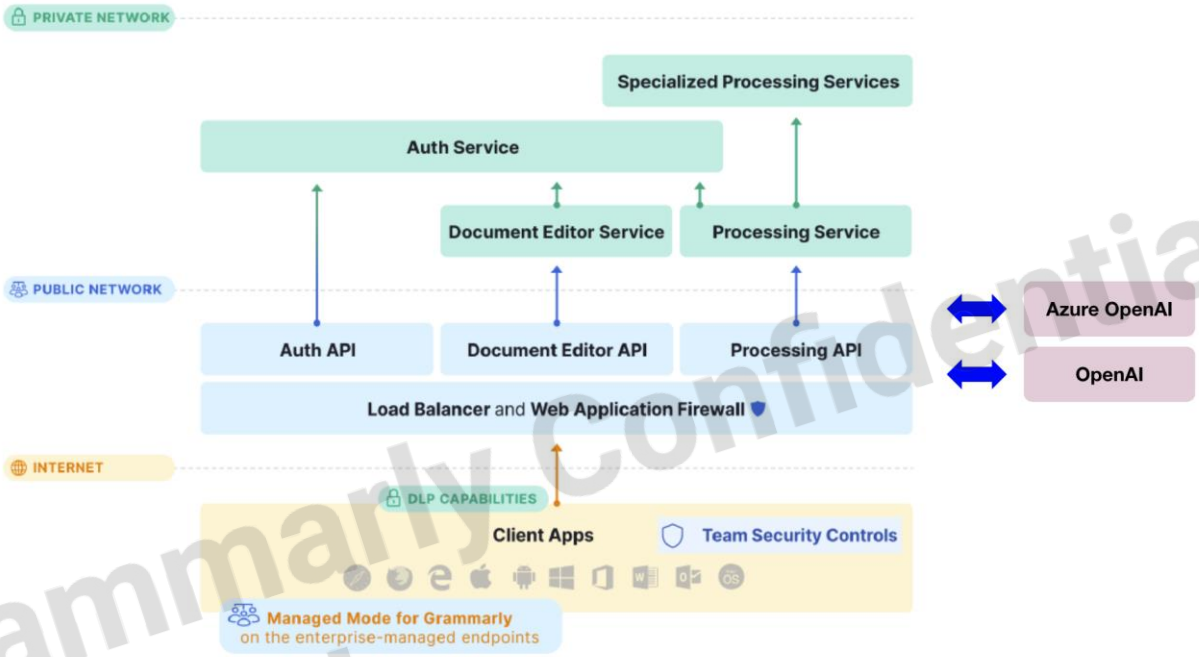

Figure 1 – Product Infrastructure

- **Client Apps** are Grammarly's product offerings that could be installed and used on different platforms.
- **Load Balancer** and **Web Application Firewall** are AWS services used to distribute traffic across several servers to increase capacity and reliability as well as, to filter, monitor, and block traffic.
- **Authentication API**, **Document Editor API**, and **Processing API** are application programming interfaces that facilitate interaction between users and relevant Grammarly services.
- **Authentication Service** authenticates both internal and external users of Grammarly by login/password, single sign-on ("SSO") via SAML, or social sign-on with Google or Facebook.
- **Document Editor Service** facilitates users' ability to create, edit, and save documents via the Grammarly Editor or desktop apps.

- **Processing Service and Specialized Processing Services** manage connections from all client apps (such as the browser extension and mobile keyboard) to provide writing suggestions from Grammarly.
- **Azure OpenAI and OpenAI services** are third-party Learning Language Model ("LLM") providers for the generative AI capabilities in Grammarly's product offering. The scope of the report does not include the evaluation of performance or integrity of the third-party LLM providers and the services that is provided.

Infrastructure provider

All Grammarly server infrastructure is hosted in Amazon Web Services ("AWS") data centers located in the United States in the US East region (North Virginia).

As an infrastructure provider and solutions partner, AWS helps Grammarly in supporting the scalability, availability, and durability of Grammarly's platform and services.

Grammarly is registered for an enterprise support plan, the highest tier of the AWS support program, which provides rapid response from the AWS team (responses come as fast as within 15 minutes). A signed contract agreement between AWS and Grammarly is maintained to uphold the agreed responsibility and agreement between AWS and Grammarly. As a part of the plan, AWS provides consulting support to Grammarly's engineering teams regarding specific use cases and applications. This high-touch support also includes design reviews and architectural guidance.

Network security

Only a small number of Grammarly's servers and network ports that are used for the provisioning of services are accessible from the internet. These are protected behind load balancers and a web application firewall ("WAF"). All components that process user data operate in Grammarly's private network inside Grammarly's secure cloud platform.

User data encryption and isolation

Customers' data is encrypted in transit and at rest. The management of cryptographic keys for Grammarly assets follows the Key Management Requirements in the company's Cryptography and Encryption Policy:

- Connections between client applications and the backend Grammarly infrastructure are protected by up-to-date encryption protocols, including TLS 1.2.
- Grammarly customer data is encrypted at rest in AWS using Advanced Encryption Standard ("AES-256") server-side encryption.

- User text in cache key is hashed. Key value is encrypted using AWS Key Management Services.
- Passwords are stored in encrypted databases with applied bcrypt hashing.
- Grammarly uses AWS Key Management Services ("KMS") for database encryption and key management. Access to the cryptographic keys is restricted to authorized personnel.
- Grammarly provides Grammarly-managed key ("GMK") and Bring Your Own Key ("BYOK") solutions for application-level encryption for Grammarly Enterprise accounts.

Each Grammarly user's data is isolated logically from other users' data. Each user is assigned a unique user ID upon account creation; user data, such as documents stored in the Grammarly Editor, is associated with this user ID. A user must be logged in to their Grammarly account—and any client request must be authenticated and authorized—in order for the user to access their data. Organization accounts are also isolated logically via unique organization IDs. Authorized members of an organization's account are the only ones who have access to the administrative features in their account, and they do not have access to any other organizations' accounts. User access rights and authority levels are verified for every administrative action or request to access restricted information.

Supporting software, services, and tools

The table below lists the software, services, and tools that support Grammarly's control environment and its offerings to customers.

Component	Service
Computing	AWS EC2, AWS Lambda
Hosting	AWS S3, AWS EBS
Container orchestration	AWS ECS, AWS Fargate
Databases	AWS DynamoDB AWS RDS AWS ElastiCache AWS Redshift
Storage services	AWS S3 AWS EBS
Log management and SIEM	Sumo Logic
Monitoring	AWS CloudWatch PagerDuty

Component	Service
	Graphite in Grafana
IdM and access management service	Okta Opal
Security and audit	AWS CloudTrail AWS GuardDuty AWS Security Hub Wiz
DDoS protection	AWS Shield, AWS Shield Advanced
Endpoint protection	CrowdStrike
Vulnerability management	Wiz, Detectify
Bug bounty platform	HackerOne
Vendor risk management	BitSight
Code and release management	GitLab, Artifactory
Corporate communication	GSuite, Slack, Zoom
Team collaboration	Atlassian Jira and Confluence Cloud
Secure Remote Access	Zero Trust Cloudflare
Payment system	PayPal, Braintree, Stripe
Customer support system	Zendesk, Drift
Customer management	Salesforce
Vendor management	Coupa, Onspring
Talent performance	Workday
Learning and development	Docebo
Hiring	Greenhouse
HRIS	Workday
Password management	1Password

Component	Service
Corporate asset management	Oomnitza, JamF, Workspace One, Automox

AWS is a subservice organization and is contractually bound to implement applicable security, confidentiality, privacy, and availability controls. Grammarly performs a review of the SOC 2 report at least annually, which includes an assessment of complementary user entity controls, subservice organizations, and mapping of the controls to key risks. Any exceptions identified in the SOC 2 report are evaluated for impact. During procurement of these third-party services and products that might affect the information security of Grammarly assets, Grammarly performs vendor and system security risk assessments to understand risks related to the new system and to adequately confirm that safeguards and controls are established. The remaining systems, services, and tools identified above are only applicable to support certain controls and criteria.

A variety of additional Service-as-a-System ("SaaS") systems listed in the overview above are also managed by third-party vendors and are used by Grammarly, including PayPal, Braintree, Stripe, Drift, and Salesforce, among others. These vendors are support tools that do not impact Grammarly's ability to meet the trust services criteria.

The affected control objective / criteria are included below along with the expected minimum controls expected to be in place at AWS:

AWS control activity	Applicable criteria
AWSCA-1.10: AWS has a process in place to review environmental and geo-political risks before launching a new region.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3; CC9.1; CC9.2; A1.2
AWSCA-2.1: User access to the internal Amazon network is not provisioned unless an active record is created in the HR System by Human Resources. Access is automatically provisioned with least privilege per job function. First time passwords are set to a unique value and changed immediately after first use.	CC6.2; CC6.3
AWSCA-2.2: IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.	CC6.2; CC6.3; CC6.7; CC6.8

AWS control activity	Applicable criteria
AWSCA-2.3: IT access privileges are reviewed on a periodic basis by appropriate personnel.	CC6.1; CC6.2; CC6.3; CC6.7; CC6.8
AWSCA-2.4: User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.	CC6.1; CC6.2; CC6.3
AWSCA-2.5: Password configuration settings are managed in compliance with Amazon.com's Password Policy.	CC6.1
AWSCA-2.6: AWS requires two-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations.	CC6.1; CC6.6
AWSCA-3.1: Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.	CC6.1; CC6.6; CC7.1; CC8.1
AWSCA-3.4: AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.	CC3.2; CC3.3; CC3.4; CC4.1; CC6.8; CC7.1; CC7.2; CC7.4
AWSCA-3.5: AWS enables customers to articulate who has access to AWS services and resources (if resource-level permissions are applicable to the service) that they own. AWS prevents customers from accessing AWS resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified AWS service or resource (if resource-level permissions are applicable to the service).	CC6.1
AWSCA-4.4: S3-Specific – S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.	CC6.1; CC6.7
AWSCA-4.7: KMS-Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES key unique to the customer's AWS account.	CC6.1; CC6.7
AWSCA-5.1: Physical access to data centers is approved by an authorized individual.	CC6.4; CC6.7
AWSCA-5.2: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.	CC6.4; CC6.7

AWS control activity	Applicable criteria
AWSCA-5.3: Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.	CC6.4; CC6.7
AWSCA-5.4: Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.	CC6.4
AWSCA-5.5: Access to server locations is managed by electronic access control devices.	CC6.4; A1.2
AWSCA-5.6: Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.	CC7.2; CC7.3; A1.2
AWSCA-5.7: Amazon-owned data centers are protected by fire detection and suppression systems.	A1.2
AWSCA-5.8: Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.	A1.2
AWSCA-5.9: Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.	A1.2
AWSCA-5.10: Amazon-owned data centers have generators to provide backup power in case of electrical failure.	A1.2
AWSCA-5.13: All AWS production media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS Secure Zones.	CC6.5; CC6.7; C1.2
AWSCA-6.1: AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service.	CC6.1; CC6.8; CC7.5; CC8.1

AWS control activity	Applicable criteria
AWSCA-6.6: AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.	CC6.8; CC7.1; CC8.1
AWSCA-6.7: Customer information, including personal information, and customer content are not used in test and development environments.	CC8.1
AWSCA-7.7: AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.	CC6.5; C1.2
AWSCA-10.3: AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.	CC2.2; CC3.2; CC3.3; CC3.4; CC5.3; CC7.3; CC7.4; CC7.5; CC9.1; A1.1; A1.2; A1.3
AWSCA-11.2: AWS has a program in place for evaluating vendor performance and compliance with contractual obligations.	CC1.1; CC1.4; CC2.3; CC4.1; CC9.2

Management's monitoring control over sub-service providers

Due diligence procedures are in place upon engagement and at least annually for third-party service providers.

The Security and GRC teams evaluate third-party cloud services regarding their compliance with Grammarly requirements for security, availability, confidentiality, and privacy. Before starting the evaluation, the GRC, Security and Privacy teams analyze the request for the service and determine the service criticality based on its potential impact on Grammarly's business processes, security of Grammarly's information, and impact on Grammarly's product ecosystem. If the service is assessed as critical, then a review is required. This includes a GRC review of the service's SOC 2 report, along with the ISO/IEC 27000 family and other applicable certifications. Security assessment of the service's security maturity score in Grammarly's vendor risk management platform involves checking if any data breaches associated with the service have been noted in recent years, and other verifications. Privacy review of the vendor approaches for personal data processing and definition of the need to sign a Data Privacy Addendum with consideration of other legal, security, and privacy provisions are outlined in the service contract. These provisions include, but are not limited to, requirements for secure information processing, actions that would be taken in case of a data breach, the right to audit

the vendor's security, and other relevant requirements to protect the information of Grammarly and user entities of Grammarly.

Relevant aspects of the control environment

Governance and oversight

Grammarly is committed to maintaining customer trust, as well as compliance, with the applicable regulatory requirements. To support this objective, its Board of Directors is assembled from highly qualified individuals who lead with core values of ethics and integrity, establish the company's strategic goals, and monitor the company's performance. The Board of Directors includes members independent of Grammarly's management team and can provide an impartial perspective in evaluations and decision-making.

Grammarly's Board of Directors reviews the results of the formal audit program, which includes independent audits of information security, privacy, and financial statements along with, corrective measures for remediation.

Grammarly's Board of Directors has established and maintained the company's five-year strategic goals. From these strategic goals, the Executive team further establishes annual goals. All other Grammarly teams then prepare and consolidate quarterly Objectives and Key Results ("OKR") plans.

Grammarly also has established standard operating procedures to provide each operating unit and its team members with the support necessary to securely and effectively perform the tasks required to fulfill company-wide objectives.

People management

To support Grammarly's achievement of established objectives, the People team creates an annual hiring plan that is approved by the Executive team.

Grammarly's recruitment process evaluates prospective new hires by their competency to perform their roles, as well as their demonstration of established company values. To maintain these standards, candidates undergo comprehensive evaluation against detailed requirements by different stakeholders, including the hiring manager, the recruiter, experts in relevant domains, and the executive-level manager.

All new employees and contractors who have access to Grammarly services undergo background verification checks as a part of the hiring process. This step validates that those who work at Grammarly uphold a high degree of ethics, can produce work of the necessary quality, add qualitatively to corporate culture, and establish product security for customers.

During the onboarding process, new employees participate in training and information sessions with the People team, teammates, and their direct manager to enhance their understanding with current operational procedures, as well as their individual job responsibilities, their team, and personal Objectives and Key Results ("OKR"). As part of this process, all new employees are required to sign a Confidentiality Agreement and an Acceptance of Grammarly Policies, which states that employees are obliged to stay in compliance with the company's information security requirements.

All existing employees undergo an annual performance review process, which includes an assessment of their technical and soft-skill competency by their managers. Employees can receive continuous professional education with the company's support; this education could be initiated based on performance review results or at any other time upon manager approval.

Integrity and ethical values

Grammarly's control environment originates from the highest levels of the company—executives and other members of senior leadership play active roles in establishing the organization's core values.

Every employee is provided with details about Grammarly's history, product, and standards of communication, as well as Grammarly's policies governing the organization, which operates in alignment with EAGER values: ethical, adaptable, gritty, empathetic, and remarkable. These values and associated behaviors are defined in materials that are made available company wide. During onboarding, as well as on a periodic basis, all Grammarly employees receive training to promote awareness about information security, privacy, values-based behavior, and unconscious bias.

Grammarly has established a whistleblower hotline that is available for employees and contractors to anonymously report known or suspected misconduct or violations of the company's policies. Material violations, including gross violations of company values, are addressed via a formal disciplinary process that outlines appropriate disciplinary action, including the possibility of termination. External users can report matters of known or suspected misconduct or violations via multiple external channels.

Security organization

Grammarly is committed to securely delivering its services and protecting customer information with ethics and integrity. To support these commitments, Grammarly has established various organizational units to develop and implement security throughout the organization.

The Trust Leadership team oversees the development of Grammarly's approach to security, including organizational and technical measures. To establish effective operation of these measures, the team meets semi-annually to review information-security objectives, risk-

assessment results, independent audit results, security vulnerabilities, and information-security or privacy incidents.

Dedicated sub-teams have been established to monitor and protect the Grammarly control environment by responding to and preventing issues.

- Product Security is responsible for secure design, development, and implementation of the Grammarly product ecosystem, and for management of Grammarly's bug bounty program.
- Platform Security is responsible for secure design, development, and implementation of the Grammarly Cloud and Data platforms.
- Detection and Response is responsible for security monitoring and incident response.
- Corporate Infrastructure is responsible for managing access to the Grammarly systems, maintaining corporate network and endpoint security.
- Trust Engineering is responsible for providing Grammarly's user-facing products with functionality to manage identity, consent management, encryption, and related privacy functionality.
- Security Intelligence is responsible for gathering and processing security information from diverse sources to identify, prioritize, and mitigate potential threats to Grammarly assets.
- Governance, Risk, and Compliance ("GRC") is responsible for corporate compliance and risk management.

Grammarly maintains a company-wide Security Champions program to embed security specialists on each set of Engineering teams to implement and scale security effectively for Grammarly's product offerings. Security Champions own each team's security backlog, make decisions affecting security, spread their knowledge within the team, communicate with other Security Champions, and notify the Security team about any potential security concerns.

Grammarly has established a formal audit program that includes periodic independent audits. This program validates the design and operational effectiveness of security and privacy across Grammarly processes, infrastructure, and product offerings. Audits assess management processes (e.g., governance, risk, and assurance processes and activities) and the implementation of security (e.g., passwords, encryption, access, and change management) and privacy controls through control testing. The Trust Leadership team reviews all audit results and decides on the appropriate corrective measures to improve Grammarly's security and privacy posture.

Vendor management

Grammarly has implemented a formal vendor management program for managing risks related to third-party services. The program includes processes for vendor onboarding, periodic reviews of existing vendors, and vendor offboarding.

The Security, Privacy, and GRC teams evaluate third-party cloud services regarding their compliance with Grammarly requirements for security, availability, confidentiality, and privacy. Before starting the evaluation, the Security and Privacy teams analyze the request for the service and determine the service criticality based on its potential impact on Grammarly's business processes, security of Grammarly's information, and impact on Grammarly's product ecosystem. If the service is assessed as critical, then a review is required. This includes a GRC review of the service's SOC 2 report along with the ISO/IEC 27000 family and other applicable certifications. Security assessment of the service's security maturity score in Grammarly's vendor risk management platform involve checking if any data breaches associated with the service have been noted in recent years, and other verifications. Privacy review of the vendor approaches for personal data processing and definition of the need to sign a Data Privacy Addendum with consideration of other legal, security, and privacy provisions. These provisions include, but are not limited to, requirements for secure information processing, actions that would be taken in case of a data breach, the right to audit the vendor's security, and other relevant requirements to protect the information of Grammarly and user entities of Grammarly.

Grammarly also enters into business associate agreements with its sub-processors to help ensure that the sub-processor will appropriately safeguard the information.

During contract renewal for third-party services, these same procedures apply, including the full GRC and security review of the service.

Should Grammarly decide to terminate a contract with a third-party technology service provider, Grammarly would confirm that the vendor does not maintain access to Grammarly's information after contract termination. This process would be outlined via appropriate data retention provisions in the agreement. Before the data is deleted, respective teams would migrate it to another service or to Grammarly's cloud infrastructure. Upon completion of data transfer, the responsible Grammarly team would request a confirmation that Grammarly's data has been fully deleted by the vendor.

Policies and procedures

Grammarly's GRC team maintains a Policy Central with all documents that are required for the performance of business processes and related security aspects. Such processes include, but are not limited to, security risk assessment; information classification; and vendor, access, and

change management. These documents range in detail—from policies defining the company's overall approach in managing a specific area to detailed guidelines offering specific instructions to responsible staff members.

Policies require approval by the Information Security and Privacy Management System Manager ("ISPMS" Manager) and relevant functional heads. Such documents are reviewed annually or in cases of relevant changes to the existing processes, technologies, or organizational structure.

Documents become effective when they are published on the Policy Central portal and are announced to the company in the relevant corporate Slack channel. The portal is available to all employees beginning their onboarding.

Information and communication

Internal communication

Grammarly has established various global internal communication channels to communicate significant events in a timely manner and assist employees in understanding their roles and responsibilities. The internal communication channels include but are not limited to, the following:

- **Show-n-Tell (former Global All-Hands)** are weekly company-wide meetings hosted by the Executive team to communicate important information to all Grammarly team members.
- **Grammarly 101** is a set of sessions used to provide new employees with training about the company, its product offerings, its values, and its rules for conduct and communication.
- **Online Learning Management Service** is used to educate employees about information security and privacy.
- **Grammarly Wiki** is an online document repository available to all employees to store and share key information across Grammarly, including policies and procedures, guidelines, and training materials. For information security policies, there is a dedicated Policy Central space that gathers all documents relevant for compliance with industry security practices.
- **Slack** is a corporate messaging service used for a variety of internal communication needs, including sharing company updates, conveying changes to information policies, team collaboration, and alerting the organization to new security concerns and procedures. Commonly used channels to communicate about security are a #global-announcement channel and a #security channel, along with privacy channel #privacy-

awareness-champions, and channels specific to local offices and channels relating to other work topics.

- **Corporate-managed email** is used by employees to report security incidents according to the established Incident Management Procedure. Significant changes to systems and operations are also communicated through the corporate email client.
- **Weekly Mail** is a weekly company-wide newsletter from the CEO sent via email, which provides updates for the internal staff.

External communication

External channels enable timely communication of important updates and significant changes to Grammarly's customers. Each channel has been designed to direct user and customer communications to the appropriate recipients. The external communication channels include the following:

- **Grammarly's official website** contains information about Grammarly's corporate brand, product offerings and plans, careers and culture, and affiliate program, among other areas of information. The Grammarly Blog is a part of Grammarly's official website. Readers can find periodic updates about the product and company, along with writing tips. Additionally, the Grammarly Engineering blog focuses on content describing Grammarly's technology and innovation, while the Grammarly Business blog focuses on our B2B offering.
- **Mobile application stores** communicate information about installing on specific devices. All most recent changes are reflected in the description of the application at the application store.
- **Browser extension stores** are used for communication of the links for application installation at specific browsers. All recent application changes are reflected in the extension store description.
- **Microsoft Office add-in** can be accessed through the application itself or through the Microsoft website.
- **Social networks** are used to post information about company and product updates, including X, LinkedIn, Facebook, Instagram, TikTok, and YouTube.
- **Websites on which Grammarly maintain profiles** support employer brand and recruiting initiatives, including Glassdoor, AngelList, Built In, Crunchbase, dou.ua, Capterra, and G2.

- **Subscriber emails** include the following. Grammarly customers can unsubscribe from marketing emails at any time. Customers in the European Economic Area ("EEA") will only receive such emails if they opt-in.
    - **Weekly Insights emails**: A weekly report with statistics and insights on how the user is writing with Grammarly.
    - **Product Updates emails**: Important info on new features and product offerings. From time to time, these emails also request product feedback.
    - **Grammarly Offers emails**: Special upgrade offers, limited-time events, or coupons.
    - **Survey emails**: Surveys conducted by our Human Insights team to gather input from our users to help improve the product for them.
    - **Newsletter emails**: A newsletter from the Grammarly Blog that includes fun tips on all things writing, as well as a newsletter intended for prospective engineering employees.
    - **Grammarly Business emails**: Updates and information on Grammarly product offerings for multi-person teams, including a quarterly newsletter of product updates and a monthly newsletter of relevant content for prospective customers.
    - **Premium Reports emails**: Reports with details on Paid suggestions related to user personal writing activity.
    - **Billing/transaction-based emails**: Customers will receive emails from Grammarly about billing information during renewal periods.
- **In-product messages** are delivered to users within the product directly occasionally. These messages include information about new features or product offerings.
- **Grammarly Support Portal** is available for all users to find answers to frequently asked questions or to contact Customer Support agents for further information about product or account use.
- **Grammarly status page** provides publicly available information about the operational performance of Grammarly services and provides up-to-date information on any outages and problems.
- **Reports about data breaches** are communicated to users based on the procedures described in the Personal Data Breach Notification Policy.

- **Communication with authorities** is performed by Grammarly Legal Counsel if required, based on the Contact List for Authorities.

Risk management

Through a formal risk management program, Grammarly continuously identifies, assesses, resolves, and monitors risks to information security, privacy, and fraud that could have an impact on Grammarly, compliance with the regulatory requirements, or customers' data security. The Security team monitors the risk management program on an ongoing basis. The ISPMS Manager and Security team define lessons learned to improve the risk management program and periodically present the results to the Trust Leadership team that includes the company's executives.

Grammarly's risk management program includes the following phases:

- **Risk Identification**: A baseline library of threats, vulnerabilities, and asset types is maintained, and new threats (sourced both internally and externally) are added to the library on an ongoing basis. The GRC team also performs an annual Business Impact Analysis to determine the criticality of services and their risk level to Grammarly.
- **Risk Analysis and Risk Evaluation:** Based on the information collected during the risk identification, the impact and likelihood of the threats and vulnerabilities are determined to calculate the Inherent Risk Score. The Risk Owner and GRC team then map the relevant GRC controls that mitigate each risk. The aggregated effectiveness score of the mapped GRC controls is factored in to calculate the final Residual Risk Score. Where the Residual Risk Score is higher than the risk tolerance level, actions are taken to implement and/or improve controls to bring the Residual Risk Score down to an acceptable level.
- **Risk Treatment:** Risk Owners are responsible for selecting and implementing measures to reduce risk. Risk treatment involves methods such as risk avoidance, risk mitigation, risk transfer, risk sharing, and risk acceptance. The GRC team documents risk treatments in the risk register. The Risk Owners are responsible for the implementation of risk treatment controls.
- **Risk Monitoring and Control:** The GRC team and Risk Owners perform annual risk assessments that include identification of new risks, updated risk analysis and control effectiveness, and monitoring of treatment plan progress. The GRC Manager and the ISPMS Manager report the results of the annual risk assessment process to the Trust Leadership team.

Attachment B – Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Grammarly designs its processes and procedures that support the product ecosystem in scope for this report to meet objectives of Grammarly product offerings based on the following trust services criteria: security, availability, confidentiality, and privacy.

Those objectives are based on the service commitments that Grammarly makes to user entities; the laws and regulations that govern the provision of services; and the financial, operational, and compliance requirements that Grammarly has established for its control system.

Security, availability, confidentiality, and privacy commitments to user entities are described and communicated in detail in Grammarly's Terms of Service and Privacy Policy, as well as on its Security landing page and its User Trust Guidelines, which are all available to end users and organization customers on Grammarly's public website. The Terms of Service and Privacy Policy are also described and communicated on Grammarly's sign-up page, browser extension stores, and through the iOS, Mac, and Android app stores. The same security, availability, confidentiality, and privacy commitments detailed in the Terms of Service and Privacy Policy are also defined in the Master Service Agreements ("MSA") with enterprise customers.

The security, availability, confidentiality, and privacy commitments include, but are not limited to, the following:

- **Product Security:** Grammarly has a range of security controls designed to keep the Grammarly system secure, protect customers' data against unauthorized access and guide necessary changes. These controls include, but are not limited to, implementing security processes and tools for change, vulnerability, and incident management to prevent, detect, and remediate security threats and vulnerabilities.
- **System Availability**: Grammarly monitors its systems' availability to customers by using cloud hosting in multiple availability zones across AWS regions, maintains optimal infrastructure performance through continuous monitoring, and establishes backups and Disaster Recovery Plans for quick and effective recovery in case of an incident.
- **Data Security and Confidentiality**: Security and confidentiality controls at Grammarly are designed to address the relevant criteria to protect confidential information. Such controls include establishing and maintaining an information classification and service criticality procedure , business impact analysis and risk assessment processes, proper access management, and encryption and other practices to restrict access to customers' data.

- **Privacy Process:** A range of privacy controls are designed to address the privacy criteria of Grammarly's product offerings and to protect customers' personal information. Such privacy controls include maintenance of a public Privacy Policy, providing a privacy notice to customers when there is a major change in the Privacy Policy, public communication about Grammarly's sub-processors and changes to them, timely responses to customer requests, and maintenance of an established procedure to notify customers of breaches.