

# 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, 2021 through March 31, 2022

# Table of Contents

<b>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, 2021 to March 31, 2022</b>	<b>1</b>
<b>Section 2 – Report of Independent Accountants</b>	<b>3</b>
<b>Attachment A – Description of the Boundaries of Grammarly</b>	<b>6</b>
Company background	7
Product overview	7
Scope	8
Principal architecture	10
Infrastructure provider	11
Network security	11
User data encryption and isolation	12
Supporting software, services, and tools	12
Management’s monitoring control over sub-service providers	17
Relevant aspects of the control environment	18
Governance and oversight	18
People management	18
Integrity and ethical values	19
Security organization	19
Vendor management	20
Policies and procedures	21
Information and communication	21
Risk management	22
<b>Attachment B – Principal Service Commitments and System Requirements</b>	<b>24</b>
<b>Attachment C – Other Information Provided by the Service Organization</b>	<b>27</b>

**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, 2021 to March 31, 2022**



## **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, 2021 to March 31, 2022**


We, the management of Grammarly, are responsible for:

- Identifying the Grammarly System (the “System”) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of Grammarly’s principal 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 principal service commitments and system requirements
- Selecting the trust services categories 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 boundaries of the System presented in Attachment A includes only controls of Grammarly and excludes controls of AWS. However, the description of the boundaries of the System does present the types of controls Grammarly assumes have been implemented, suitably designed, and operating effectively at AWS. Certain trust services criteria can be met only if the AWS controls assumed in the design of Grammarly’s controls are suitably designed and operating effectively along with the related controls at Grammarly. However, we perform annual due diligence procedures for third-party subservice providers, and, based on the procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy set forth in the AICPA’s TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

DocuSigned by:  
  
7295BF9BD7D64B0...

**Joe Xavier**  
**Vice President of Engineering, Grammarly**

## **Section 2 – Report of Independent Accountants**



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 System (System) were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in the AICPA’s TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### **Management’s Responsibilities**

Grammarly’s management is responsible for its assertion, 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 Grammarly System and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system
- identifying, designing, implementing, operating, and monitoring effective controls over the Grammarly System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

### **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 American Institute of Certified Public Accountants (“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 considered 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.

We are required to be independent of Grammarly and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement. We have complied with such independence and other ethical requirements and applied the AICPA’s Statements on Quality Control Standards.

The information in the accompany “Attachment C – Other Information Provided by the Service Organization” is presented by management of Grammarly to provide additional information and is not part of the Description. Such information has not been subjected to the procedures applied in our examination and accordingly, we express no opinion on it.

***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 principal 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.

***Opinion***

In our opinion, Grammarly’s controls over the system were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

A handwritten signature in black ink that reads 'Ernst &amp; Young LLP'.

San Jose, California

June 10, 2022

# **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 \$400 million in funding from Baillie Gifford, funds and accounts managed by BlackRock, General Catalyst, IVP, and others.

Grammarly is headquartered in San Francisco and has offices in Kyiv, New York City, and Vancouver. 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 assistant helps 30 million people and 30,000 professional teams 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, introduced in 2015, provides access to essential writing support for anyone who needs to communicate in English. Grammarly's enterprise offering, Grammarly Business, helps enterprises, organizations, and teams of all sizes accelerate business results through clear, consistent, and on-brand communication. Grammarly Business offers all Grammarly Premium suggestions, tailored administrative controls, and enterprise-level features. Grammarly also offers Grammarly for Developers, where developers can integrate Grammarly's writing assistance into their web applications by implementing the Grammarly Text Editor SDK.

## Scope

The scope of this report includes the following Grammarly client applications, available for organization customers (Grammarly Business), 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 Editor for Windows and Mac:** Grammarly's desktop application replicates the experience of the Grammarly Editor for users who prefer not to access Grammarly's writing interface through their browser. Native apps are available for Windows and macOS.
- **Grammarly browser extension:** Whether a user works in Chrome, Firefox, Safari, or Edge, Grammarly's browser extension offers suggestions on a vast array of websites, including Google Docs, Zendesk, LinkedIn, Twitter, 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, which is valid for users with the compatible operating systems and versions. (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.
- **Grammarly for Developers:** Developers can leverage Grammarly's Text Editor SDK and integrate Grammarly's writing to their web applications by adding just a few lines of code.
- **Expert Writing Service:** Offered to Grammarly Premium users looking to gain extra confidence in their work, Grammarly's expert writing service gives users the option to submit a piece of text for editorial review by a team of writing experts.

## 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 Support, Legal, People, Sales, Marketing, Finance, Language Technology, Workplace Experience, and Customer Support.

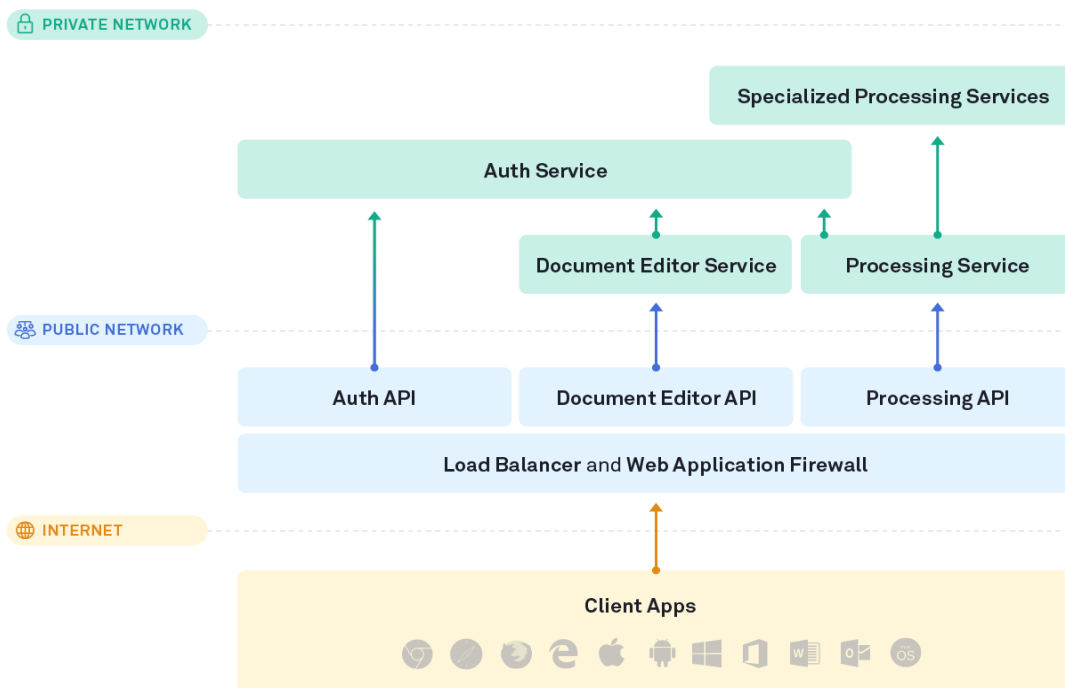
The following teams are relevant for this report:

- **Board of Directors:** Responsible for establishing and overseeing company strategy.
- **Executive team:** Responsible for overseeing all company operations.
- **Security team:** Comprises two teams responsible for ensuring security across the company.
  - **Product Security:** Consists of Security Operations, who supports Grammarly's security program by owning monitoring tools, incident response, and running a complex cloud infrastructure security toolkit, and Application Security, who collaborates with Grammarly Engineering to share advanced security expertise and help ship product offerings with industry-level application security.
  - **Governance, Risk, and Compliance team:** Establishes and coordinates security processes and practices across the organization in compliance with industry security standards.
- **Platform team:** 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 Support team:** Provides assistance with hardware issues, software licenses and management, office network laptop support, and other requests relating to information technology.
- **People team:** 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 team:** Provides timely, empathetic help that keeps the customer’s needs at the forefront of every interaction.
- **Legal team:** Provides legal review and support for all aspects of Grammarly’s product ecosystem and global company policies.

## Principal architecture

Grammarly’s product infrastructure comprises the following main components:





- **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 a number of 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.

## 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 Cryptographic and Encryption Policy:

- Connections between client applications and the back-end Grammarly infrastructure are protected by up-to-date encryption protocols, including TLS 1.2, until data is stored in the Grammarly environment.
- Grammarly customer data is encrypted at rest in AWS using AES-256 server-side encryption.
- 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.

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 through Grammarly Business 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, EBS
Container orchestration	AWS ECS, AWS Fargate
Databases	AWS DynamoDB AWS RDS

Component	Service
	AWS ElastiCache AWS Redshift
Storage services	AWS Simple Storage Service (S3) AWS Elastic Block Store (EBS)
Log management and SIEM	Sumo Logic
Monitoring	AWS CloudWatch Opsgenie Panopta Graphite in Grafana
IdM and access management service	Okta
Security and audit	AWS CloudTrail AWS GuardDuty AWS Inspector AWS Security Hub
DDoS protection	AWS Shield, AWS Shield Advanced
Endpoint protection	CrowdStrike
Vulnerability management	GitLab Ultimate, 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
VPN service	F5 BIG-IP
Payment system	PayPal, Braintree
Customer support system	Zendesk, Drift
Customer management	Salesforce
Talent performance	Lattice

Component	Service
Learning and development	EverFi
Hiring	Greenhouse
HRIS	BambooHR
Password management	1Password
Corporate asset management	Jamf Pro

AWS is a subservice organization and is contractually bound to implement applicable security, confidentiality, 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 assessment 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 SaaS systems listed in the overview above are also managed by third-party vendors and are used by Grammarly, including Paypal, Braintree, Drift, and Salesforce, among others. These vendors are support tools that do not directly 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



AWS control activity	Applicable criteria
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
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; CC6.7; 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
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 master key unique to the customer’s AWS account.	CC6.1; CC6.7

AWS control activity	Applicable criteria
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
AWSCA-5.3: Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.	CC6.4; CC6.7
AWSCA-5.4: Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.	CC6.4
AWSCA-5.5: Physical access points to server locations are 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.	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 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.	CC6.1; CC6.8; CC7.5; CC8.1



AWS control activity	Applicable criteria
Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service.	
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 Legal teams evaluate third-party services regarding their compliance with Grammarly requirements for security, availability, confidentiality, and privacy. This includes a review of the service’s SOC 2 report along with the ISO/IEC 27000 family and other applicable certifications, assessment of the service’s security maturity score in Grammarly’s vendor risk management platform, checking if any data breaches associated with the service have been noted in recent years, and other verifications. Only when the security review is completed does the service request go to the Legal team, which proceeds with the signing of a Data Privacy Addendum with the vendor and ascertains that 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 so are able to 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 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. Then all other Grammarly's teams 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 updated quarterly and 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 and contractors are required to sign a Confidentiality Agreement and an Acceptance of Grammarly Policies, which states that employees and contractors are obliged to stay in compliance with the company’s information security requirements.

All existing employees undergo a semi-annual performance review process, which includes an assessment of their technical and soft-skill competency by peers and managers. Employees have the opportunity to 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, anti-harassment practices, 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.

## **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 Security Strategy 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 quarterly to review information-security objectives, risk-assessment results, independent audit results, security vulnerabilities, and information-security or privacy incidents.

Dedicated teams have been established to monitor and protect the Grammarly control environment by responding to and preventing issues. The Governance, Risk, and Compliance (“GRC”) team is responsible for corporate compliance and risk management. Within the Production Security team, Security Operations (“SecOps”) is responsible for security monitoring and the fortification of Grammarly’s infrastructure to protect against cyber-attacks, and Application Security (“AppSec”) is responsible for guiding secure design, development, and implementation of the Grammarly product ecosystem, and for management of Grammarly’s bug bounty program.

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 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 controls (e.g., passwords, encryption, access and change management) through control testing. The Security Strategy team reviews all audit results and decides on the appropriate corrective measures to improve Grammarly’s security 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 review of existing vendors, and vendor offboarding.

The Security and Legal teams evaluate third-party cloud services regarding their compliance with Grammarly requirements for security, availability, confidentiality, and privacy. Before starting the evaluation, the Security team analyzes the request for the service and determines 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 security review is required. This includes a review of the service’s SOC 2 report along with the ISO/IEC 27000 family and other applicable certifications, assessment of the service’s security maturity score in Grammarly’s vendor risk management platform, checking if any data breaches associated with the service have been noted in recent years, and other verifications. Only when the security review is completed does the service request go to the Legal team, which proceeds with the signing of a Data Privacy Addendum with the vendor and ascertains that 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.

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

Should Grammarly make a decision 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 of the Information Security System Manager ("ISMS" 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**

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 and procedures require approval of the Information Security System Manager (“ISMS” 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.

## 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 ISMS Manager and Security team define lessons learned to improve the risk management program and periodically present the results to the Security Strategy team that includes the company’s executives.

Grammarly’s risk management program includes the following phases:

- **Identify:** The GRC team performs an annual Business Impact Analysis to identify services requiring examination. The services Grammarly uses to provide its product offerings are included in the scope of the security risk assessment and implementation of all applicable security controls. Other members of the Security team then work in collaboration with functional leads and owners of these services to identify relevant risks for information security, privacy, and fraud. Security team leaders, along with the ISMS Manager, then review the results and formulate a list of actionable security risks to Grammarly.
- **Assess:** Teams assess each identified risk as Low, Medium, and High based on their likelihood and impact, taking into account previous security incidents, known vulnerabilities, and existing security controls. Grammarly’s Security Strategy team approves a risk treatment plan with the timeframe for risk resolution. Resolution may include measures related to avoidance, mitigation, and transference of risk. Each risk has established owners who are responsible for the risk resolution.
- **Resolve:** The Security team coordinates and provides guidance to risk owners and other teams at Grammarly to facilitate the successful implementation of the risk treatment program.
- **Monitor:** The Security team monitors the existing security risks to determine the success of the risk treatment program and to plan any additional necessary actions over the course of the following year.





- **Improve:** After the annual risk management cycle, the Security Strategy team, which includes the ISMS Manager and the Security team, defines what lessons were learned with the goal of improving the risk management program.

## **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 handling policy, 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.

## **Attachment C – Other Information Provided by the Service Organization**

## Maintaining Secure Remote Work amid COVID-19

Grammarly has adopted a remote-first hybrid work model long term. We believe the future of work blends the power of digital communication with in-person connection, and we have long had policies and procedures in place to maintain our strong security commitment in a remote environment. The company was quick to respond to the COVID-19 outbreak, supporting the health and well-being of our team members while maintaining our commitment to keep Grammarly user data secure. Throughout the extended remote-work period spurred by the pandemic, we effectively achieved business continuity and support collaboration.

Grammarly has stringent security measures and safeguards in place to ensure customer data is safe and secure. Some existing controls that we carry forward with our remote-first hybrid model include:

- Grammarly team members are required to store all user data in trusted cloud systems and in the AWS cloud. The only exception is email contacts, which may be present on company laptops for team members whose job duties require it.
- We deploy fine-grained VPN rules protecting internal services, AWS access policies, and Remote Desktop solutions to maintain security of all data. This applies across all systems and roles with access to user data.
- We have implemented unauthorized access preventative controls, which include least privilege principle, secure multi-factor authentication with Okta and enforced FIDO2 WebAuthn protocol, access provisioning/deprovisioning procedures, user access reviews, encryption, and endpoint detection and response (“EDR”). We also perform vulnerability scans, penetration tests, and patch regularly as part of ongoing vulnerability management.
- To maintain the confidentiality of internal conversations and conversations with external parties (e.g., customers, partners), we have mandatory password and waiting room requirements for all Zoom meetings.
- Our team members must use centrally managed and encrypted corporate-issued laptops for all Grammarly communication and work.
- Mobile devices used by our team do not have VPN and cannot access systems containing sensitive data.

Grammarly’s infrastructure has been set up to support consistently available optimal services. Sustaining this steady, predictable performance is possible through the usage of multiple AWS availability zones and regions, maintenance of fault tolerance, adoption of best scaling and auto-scaling practices, usage of AWS native backup and data protection solutions, and an established disaster recovery approach.

## The War on Ukraine

Since early indications that Russia was planning an invasion, our top priority has been helping our affected team members remain safe while continuing to securely serve Grammarly's users. As a company, we have implemented contingency plans to help ensure Grammarly's services will not be disrupted. This includes, for example, securing backup communication methods and temporary transfer of business-critical responsibilities to team members outside of Ukraine to ensure our Ukraine-based team members can focus on the immediate safety of themselves and their families.

The war has not affected Grammarly's control environment described in this Report. Our existing infrastructure is a strong foundation to ensure security and business continuity amid the ongoing war, with all data and codebase stored on servers hosted by Amazon Web Services in the United States.

Some additional policies and procedures to reinforce secure work amid the ongoing war include:

- We have a documented IT procedure in place to revoke access to Grammarly systems and wipe a laptop immediately if needed, rendering all data unreadable. The procedure has been tested by our IT team successfully and clearly defines scenarios and criteria to enable rapid action.
- We've geographically distributed business-critical responsibilities among select team members to ensure service continuity. We have contingency plans in place should a dynamic development require us to transfer key responsibilities.
- We deny access to our Okta and connected services from occupied regions of Ukraine, as well as Russia and Belarus, preventing connection through proxies, public VPN services, and Top of Rack device endpoints.
- We quickly activated our contingency plans to help our affected team members and their families with relocation support.

Grammarly continues to monitor the situation closely and assess new developments—and is prepared to make any necessary adjustments as needed.