SOC2 Compliance Datasheet

Worried about how to meet the SOC2 Common Criteria controls before your next compliance audit? We've got you.

Lumos

When it comes to SOC2 compliance, there are no one-size-fits-all answers or a guide that tells you exactly which criteria make sense for your business. Not sure where to begin? Use this reference guide to learn how Lumos can help.

Control Activities	Requirement	Additional Points of Focus	How Lumos can Help
CC3.2	COSO PRINCIPLE 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	• Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities • Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties	Lumos's continuously up-to-date list of applications and users at your organization helps you make sure you have a full view of the vendors that you need to assess for risk and threats.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in Vendor and Business Partner Relationships	Lumos's continuously up-to-date list of applications and users at your organization helps you stay on top of changes in vendor and business partner relationships and makes periodic vendor assessment processes easier.
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	• Considers a Mix of Ongoing and Separate Evaluations • Establishes Baseline Understanding	Lumos helps with continuous monitoring of shadow IT, allows you to keep the approval statuses of apps in your organization continuously in one place (Approved, Blocklisted, Needs Review), assists with periodic review of user access, and helps you enforce least privilege with access requests, including time-based access.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		Lumos access requests will ensure users are authorized for least privilege access to an application. Users can only request access on Lumos after they are registered in a primary integration like Microsoft, Google Workspace, or Okta. Access reviews and offboarding help you stay on top of over-provisioned users.

Control Activities	Requirement	Additional Points of Focus	How Lumos can Help
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		Lumos mitigates over-provisioning risk with access requests and periodic access reviews. With Time-Based Access Requests, employees can request access to an application only for a limited time. Lumos will automatically suspend or remove their account when the access expires. Within access reviews you can remove users from applications automatically. Lumos link users to manager, team, and role data stored in other applications, which makes it easy to maintain access based on roles and responsibilities.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		Lumos access requests help ensure users are authorized for least privilege access to applications, and therefore data. Approvers in access requests let you make sure the right people are authorized to approve access.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		Lumos helps you find all the apps your employees are using - even those rogue purchases - with our AI-powered discovery agent. Lumos uses OAuth tokens and email headers to sniff out shadow IT apps - no endpoint agent or network access is required.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		Lumos helps you track all vendors and their status from a single dashboard. With Lumos, you can spot new vendors that were onboarded between vendor review cycles as well as vendors that were off-boarded and no longer used. You can also keep the approval status of each app in one place (Approved, Blocklisted, Needs Review).

Compliance Enforcement With Lumos

Automated access Reviews

Reviewing user access takes a long time, and compiling review documentation for auditors is no fun. With Lumos Access Reviews, you can say goodbye to the endless spreadsheets, VLOOKUPs, IT tickets, and back-and-forth with your auditor. We automate this work away to keep your company compliant and safe, all in one place.

Automated Report Creation for Auditors

View and act on all access requests pending your review! You can see all requests that you are assigned to and are currently pending approval or provisioning.

Access Request Audit Log

Gather all the app access evidence you need for SOC2 audits. Keep track of every employee who requests, gets approval for, and uses every app across your enterprise. Lumos tracks details like employee name, role, group, app approver, date, time, reason, the status of app request, and approval or denial.

Time-Based Access Requests

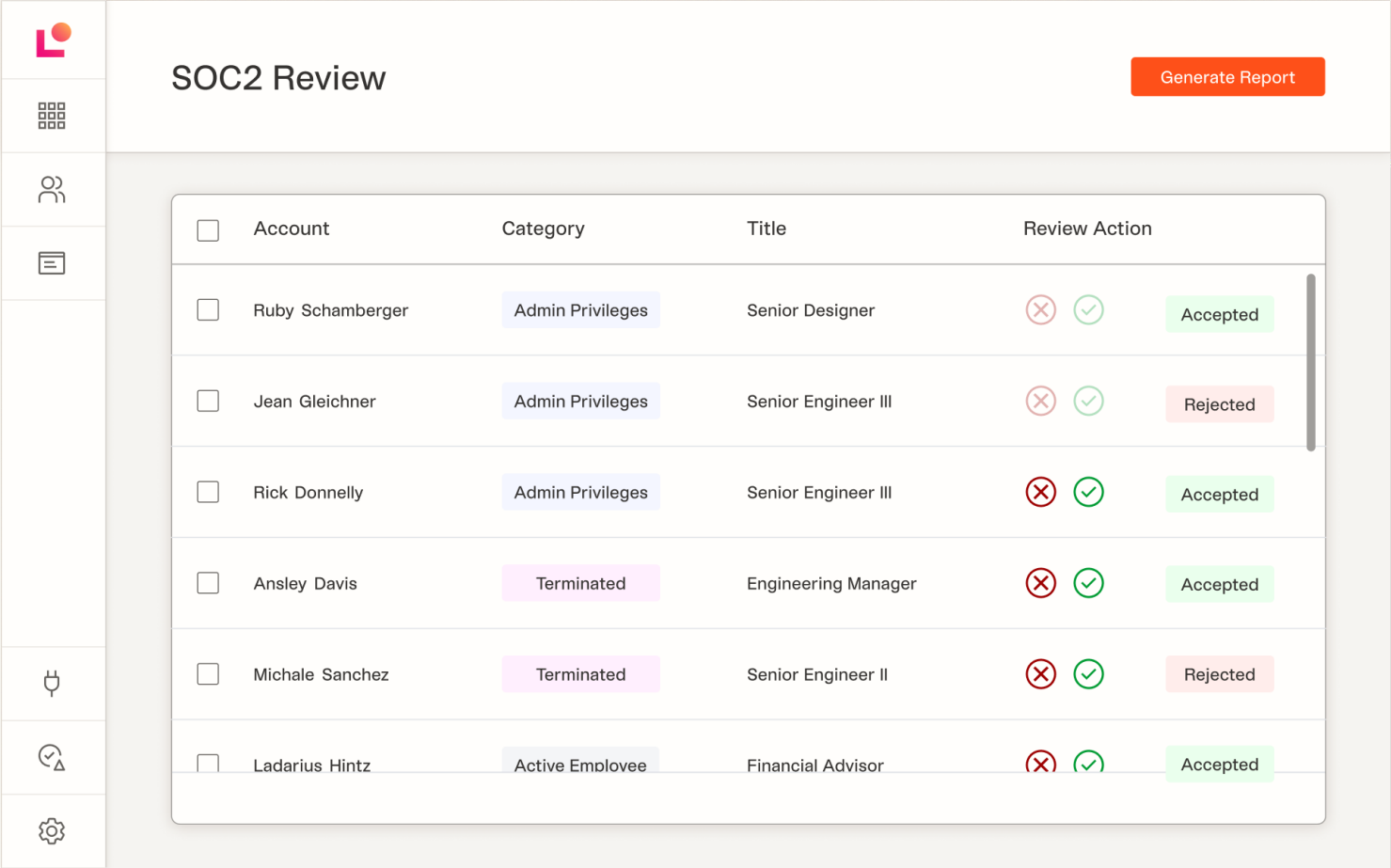
Minimize over-provisioning by leveraging least privilege for users. With Time-Based Access Requests, employees can request access to an application only for a limited time. Lumos will automatically suspend or remove their account when the access expires.

Just-in-Time Access Requests

Manage under-provisioning by allowing users to request ad hoc access to apps and resources. Lumos will route these requests through Slack for quick approval or rejection to minimize wait times.

Discovery of Active Accounts of Terminated Users

Get complete visibility and take action from a single dashboard. Off-board terminated users and ensure that off-boarding processes are complete. Lumos helps you discover and de-provision terminated users from active accounts.



Employees shouldn't be admins for hundreds of web apps with excessive permissions. But then again, nobody wants to be stuck in IT ticket queues for days to get the right access. With Lumos, you make your company more productive and compliant with self-service app requests, access reviews, and license removals. Learn more at Lumos.com