

FINANCE

Managing finances and reputational risk

Team: Finance

Responsible for: Organizational finances, managing financial and reputational risk

Shadow IT & Access Challenges:

- Services used often not supported by SSO, such as bank accounts
- Sharing of sensitive data across internal and external teams
- Financial impact of trying to secure everything behind SSO



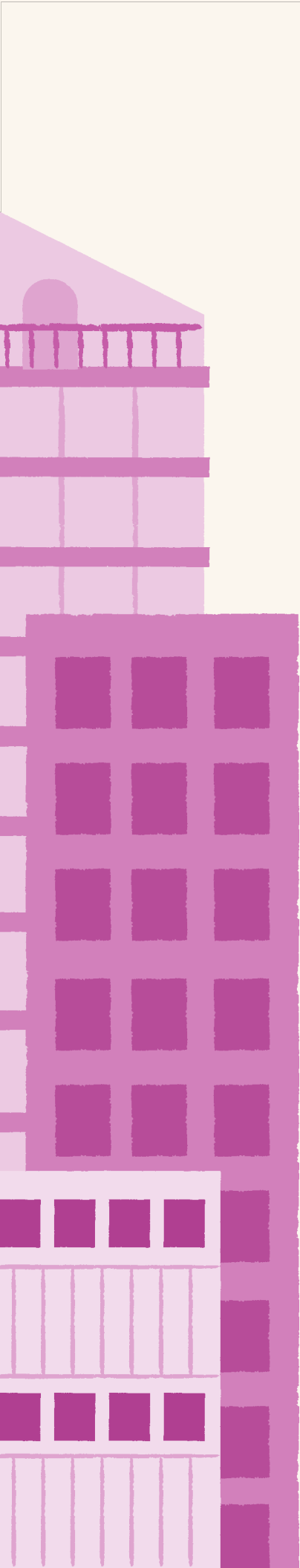
The finance team

serves as the backbone of the organization with a focus on its strategic financial planning and management. In addition to meticulous budgeting and forecasting to support the company's financial health, the finance team actively maintains accurate financial reporting to adhere to compliance standards. Finance plays a critical role in optimizing budget allocation, identifying cost-saving opportunities, and making sure they're satisfying requirements from their audit committee. The goal is to drive the organization's financial success with compliant financial practices, risk mitigation, and strategic financial planning. They handle critical financial data such as the company's banking credentials, confidential audit reports, and financial reporting, and they require robust measures to protect every user and, in turn, the organization.



Finance and security

Finance teams face distinct challenges, as they have access to the organization's most sensitive financial data. Malicious access to this data can significantly impact the company's reputation and financial standing, so it's absolutely necessary to protect every user on this team.



One example of a critical access point for finance is the organization's banking credentials, which are often excluded from SSO. Mismanagement of these credentials exposes the organization to unnecessary risk, as it could lead to direct access to the company's cash flow.

Finance teams not only have access to confidential financial data, they also often need to share documents with external partners like auditors, investors, or board members. External sharing may happen through unencrypted email or a messaging application, causing risk to the business. While these practices are born of necessity, they open the door to security risks as access to confidential information is not controlled.

Safeguarding finance requires proper credential storage and the ability to securely share sensitive data. Furthermore, the unexpected costs of a breach is a scenario that every finance team wants to avoid, making security a key priority for this team.

Your finance team also has to manage and forecast budgeting and spend for the entire organization. A large portion of that spend includes the cost of the software and tools each team needs to perform their day-to-day roles. The SSO tax, in combination with the cost for software and tool management, continues to rise, and can have major implications on technology-related spend.