How Salesloft's CISO Scaled SOC 2 and ISO 27001

While Growing From a Startup to an Enterprise

- 7 Strategies That Support Scalable Security
- Maturing SOC and ISO During 25x Growth
- 3 Key Takeaways to Streamline Compliance

Mike Meyer

SVP of Security at Salesloft

"We've gotten our compliance program to a level of maturity I'm very proud of and will continue to make it sharper."

risk3sixty

Challenge

SalesLoft, a revenue orchestration platform, faced the growing challenge of maintaining robust cybersecurity practices as it rapidly scaled from a startup to an enterprise **with over 25x growth.**

Mike Meyer, SalesLoft's SVP of Security, has played a pivotal role in guiding the company through its cybersecurity journey, from initial compliance with SOC 2 to obtaining ISO 27001 and ISO 27701 certifications, while embedding security into the company's broader strategic goals.

As a fast-growing SaaS company, SalesLoft needed to meet increasing customer demands for rigorous security and privacy protocols. **Achieving and maintaining compliance with both SOC 2 and ISO 27001 frameworks were vital steps to establish trust with enterprise clients.**

Additionally, navigating privacy regulations like GDPR became essential as the company expanded its global presence.

Key Challenges

- **Building a scalable security program from the ground up.**
- **Ensuring security practices aligned with evolving business and customer needs.**
- **Gaining executive leadership buy-in to support security investments.**
- **Supporting enterprise sales by automating security processes and addressing customer inquiries efficiently.**

Solution

Mike Meyer joined SalesLoft after working as a consultant and auditor, bringing deep experience in SOC 2 and cybersecurity best practices.

Mike Meyer

SVP of Security at Salesloft

His Best Practices Included:

1 Initial Assessment and Roadmap Development

Meyer led an internal gap assessment against the ISO 27001 framework, identifying areas where the company was compliant and where additional controls were necessary. This laid the groundwork for a formalized cybersecurity roadmap.

Collaborating with SalesLoft's leadership, he secured buy-in to invest in a dedicated security team and additional resources. **A key aspect was creating a roadmap that addressed both immediate compliance needs and long-term risk management strategies.**

2 Strategic Hiring for a Scalable Program

One of Meyer's key early decisions was to hire a security operations lead, enabling the team to monitor security alerts and manage vulnerability scanning. This hire provided the foundation for SalesLoft to shift **from reactive security measures to a more proactive stance.**

As the company grew, Meyer expanded the team into specialized functions, including application security, governance, risk, and compliance (GRC), and security engineering.

This structured approach allowed SalesLoft to mature its security operations while maintaining agility.

Solution

3 Establishing an Information Risk Council

To formalize risk management, SalesLoft introduced an Information Risk Council (IRC), composed of key executives from operations, legal, and engineering. The council met quarterly to discuss strategic security concerns and risk mitigation.

Early on, the IRC was a small group, but its consistent focus on cyber risk allowed security issues to be surfaced and addressed at the highest levels. The council has met every quarter since 2018, playing a pivotal role in maintaining a proactive security posture.

4 Vista Equity's Impact and Increased Maturity:

After SalesLoft became a Vista Equity portfolio company, expectations for cybersecurity maturity increased significantly. Investors began inquiring about the company's cyber risk strategy, and a portion of the funding was allocated specifically to improving security.

This shift allowed the team to move from reactive firefighting to a more structured, proactive security approach with a clear roadmap for growth.

5 Aligning Security and Business Objectives:

A key aspect of SalesLoft's success was embedding cybersecurity into broader business goals. Meyer emphasized translating security risks into business impacts, ensuring the executive leadership team understood the financial and operational benefits of a robust security program.

He worked closely with product and engineering teams to integrate security measures into the platform's development process, ensuring security was built into the product rather than bolted on as an afterthought.

Solution

6 Expanding Compliance with ISO 27001 and ISO 27701

After achieving SOC 2 compliance, SalesLoft pursued ISO 27001 certification to demonstrate its commitment to international security standards. Later, ISO 27701 was added to address growing customer concerns about data privacy, particularly in light of regulations like GDPR and CCPA.

These certifications provided SalesLoft with a competitive edge in the market, especially when dealing with enterprise clients with stringent security requirements.

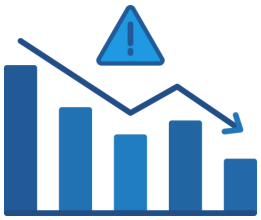
7 Quantifying Risk to Secure Executive Buy-In:

Meyer leveraged data-driven approaches, including cyber maturity frameworks and risk quantification models using insurance data, to communicate the value of security investments to leadership.

Results

Reduced Security Risks

By formalizing security operations and scaling security practices, SalesLoft mitigated significant risks that could have impacted its rapid growth trajectory.



Increased Customer Confidence

Achieving SOC 2, ISO 27001, and ISO 27701 certifications demonstrated SalesLoft's commitment to security and privacy, directly contributing to customer acquisition and retention.

Proactive Risk Management

The establishment of the Information Risk Council ensured that cybersecurity remained a top priority at the executive level, enabling proactive management of emerging risks.

Enhanced Operational Efficiency

Automating routine security processes allowed the security team to focus on more strategic initiatives while ensuring compliance with industry standards.

Key Takeaways

Collaboration Across Teams is Crucial:

By building strong relationships with internal stakeholders, including product, engineering, and legal teams, SalesLoft's security program aligned with broader business objectives, enabling more effective risk management.

Early Investment in Security Pays Off

SalesLoft's decision to prioritize security from its early stages which allowed it to scale its operations securely and maintain customer trust through various phases of growth.

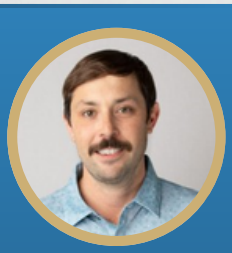
Automation Drives Efficiency

Introducing automation in security operations allowed the team to handle more tasks with fewer resources, reducing the burden of manual processes and improving response times.

Conclusion

SalesLoft's cybersecurity journey showcases the importance of embedding security into the core business strategy, leveraging automation for scalability, and maintaining a continuous focus on risk management.

By aligning security initiatives with business goals and customer expectations, SalesLoft not only safeguarded its data but also positioned itself as a trusted partner for enterprises around the globe.



Contact us today!

Ross McCurdy
ross.mccurdy@risk3sixty.com

risk3sixty.com/contact