

The SaaS management playbook

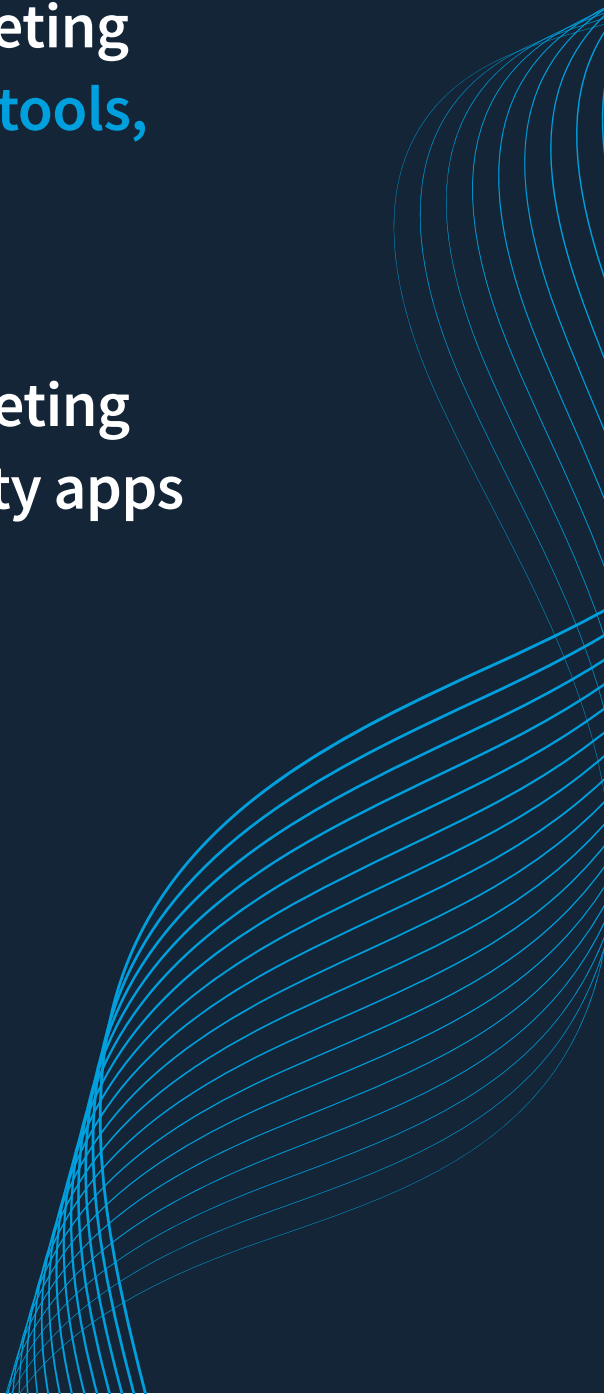
flexera™

Why NOW is the time for SaaS management

Over the past decade, SaaS has quickly and quietly become the dominant way organizations consume software.

Departments like HR, sales, marketing and finance are **buying their own tools, often without IT involvement.**

For many of those organizations, what started as a few rogue marketing tools and cloud-based productivity apps has evolved into **a sprawling, decentralized software estate.**



Whether you're in ITAM, FinOps, procurement or security, you're likely seeing the same things: growing SaaS spend, limited visibility and conflicting ownership.

SaaS management isn't just about tools—it's a discipline that helps organizations get control, improve collaboration and unlock real value.

Built from real-world experience, this playbook is designed to be your crash course on SaaS management. In it, you'll find a breakdown of value drivers, crucial insight into the intersection of SaaS management, ITAM and FinOps, a detailed maturity model and practical steps to help you move forward.

Let's get started.



Gary McAllister

Senior Product Marketing Manager
Flexera

Visibility: The foundation of SaaS management

SaaS visibility is about answering these fundamental questions:

- › What SaaS apps do we use?
- › Who owns them?
- › How are users accessing them?
- › How much are we paying?
- › Are people using these SaaS apps?

The challenge of SaaS visibility

SaaS is notoriously hard to track because it's so easy to buy. Multiply one easy purchase by hundreds of employees across dozens of departments, and you have a fast-moving mess of duplicate apps, unused licenses and tools that may not meet your security standards.

How organizations discover SaaS

Here are the most common methods companies used to discover their SaaS footprint:

SSO integration	Useful for centrally managed apps, but doesn't catch what's outside IT's control
Financial data	Reviewing expense and AP data (e.g., invoices from Zoom, Salesforce, Canva)
Browser extensions/ agent-based discovery	Powerful for catching unapproved and "shadow" apps
Surveys/manual processes	Helpful for validation, but not scalable or comprehensive
Vendor APIs	Easy to deploy, has license and financial data, but usage data isn't always present

Most mature SaaS management strategies combine these approaches for a fuller picture, but that may not be enough. Until you have **complete** visibility, cost optimization and governance will always be reactive and partial. That's why every successful SaaS management program starts here.

SaaS cost optimization

Once you've got visibility, the next logical question is: Are we spending wisely?

The answer is usually no.

Unlike infrastructure or on-premises software, SaaS waste doesn't show up as glaring overspend in one place. It trickles out silently in the form of unused licenses, auto-renewals and disconnected teams all buying the same thing.

Getting costs under control isn't about simply cutting tools—it's about aligning spend with value.

Common sources of SaaS waste

1. Underused or unused licenses

You may have 1,000 licenses for a SaaS product, but only 600 people logged in last month—and only 300 used it more than once. That's not just a usage problem; it's a cost problem.

2. Duplicate subscriptions and redundant tools

Multiple teams could be using different tools for the same job—each with their own contracts and costs.

3. Orphaned licenses

Employees leave, and their licenses stay active. Without a clean offboarding process tied to SaaS usage, these “ghost users” quietly drain your budget.

4. Unreviewed auto-renewals

Many SaaS vendors make it frictionless to renew—and surprisingly hard to cancel. Contracts roll over without a second thought, often at higher rates.

Key levers for optimizing SaaS spend

License reclamation

Identify and recover licenses people aren't using. This doesn't mean cancelling access, just reallocating it to people who actually need it.

Rightsizing plans and tiers

Not everyone needs the full featured "Pro" version. By understanding who's using what, you can shift users to lower-cost tiers or downgrade plans entirely.

Renewal calendar management

SaaS renewals come often and at different times—monthly, quarterly, annually. Maintaining a central calendar with ownership assignments helps prevent blind renewals.

Application rationalization

When you discover three apps doing the same job, it's time to evaluate which ones stay. Rationalizing your app stack not only saves money but reduces complexity.

What "good" SaaS cost optimization looks like

Instead of merely tracking SaaS spend, a mature SaaS cost optimization practice will:

- Measure **value vs. usage**
- Make **data-driven renewal decisions**
- Identify **ownership** for every app
- Create **feedback loops** with finance, procurement and IT



The result?

Fewer surprises, better forecasting and budgets that match actual business value.

Security and governance: closing gaps and banishing shadow IT

SaaS has revolutionized how businesses get things done, but it's also rewritten the rules of governance. IT used to be a tool gatekeeper. Today, any team with a credit card can access and use a new tool in minutes.

This shift creates opportunity—and threat exposure. No threat looms larger than **shadow IT**.

What is shadow IT and why it matters

Shadow IT refers to SaaS applications being used without formal approval from IT or procurement—apps that are often invisible to security, finance and compliance teams.

These tools might seem harmless at first glance: a free trial of a video editor, a forgotten password manager or a new team chat app. Collectively, however, they create a massive visibility gap in your organization's digital footprint.

The risks of shadow IT



Security gaps

Many apps are connected to sensitive data (email, calendars, cloud storage) with little oversight or access control



Unmanaged risk

If no one knows who owns a tool, no one is managing contract terms, privacy policies or vulnerabilities



Compliance exposure

You can't protect data you don't know exists—making it hard to comply with regulations such as GDPR, HIPAA, or CCPA



Audit failures

When regulators or auditors ask for a complete software inventory, shadow IT makes it impossible to provide accurate records

How SaaS management fights shadow IT

SaaS management shines a light into the corners of your technology environment—where shadow tools lurk—and makes them visible.

Truly effective SaaS management helps you:

Discover unapproved apps

Identify apps in use via SSO, finance data, browser activity and integrations—even those that IT never officially sanctioned.

Create enforceable policies

Define what types of tools are acceptable, how to review them and to handle data how data is handled. Flag or block tools that don't meet your criteria.

Map usage and ownership

See who's using each app, how often and whether it's still relevant. Assign ownership to ensure accountability.

Offboard cleanly

Ensure you revoke access not just from core apps, but also from fringe or forgotten tools that still hold sensitive data.

“With the right discovery and controls in place, we can uncover shadow IT, enforce identity and access policies, and make sure applications align with security and data residency requirements. It's about making SaaS safer—without slowing you down.”

Gary McAllister
Flexera

Governance that mitigates shadow IT and preps for audits and compliance

SaaS management supports broader **technology governance** and helps you prepare:

- **Internal audits** to maintain a clear inventory of all SaaS apps—licensed, freemium or rogue—with evidence of ownership and usage
- **Compliance reviews** to demonstrate control over where data lives, who has access and how you manage user access across your SaaS stack
- **Vendor risk assessments** to document third-party vendors in use across the business—even those procured outside central procurement channels

- **Regulatory frameworks** to meet standards like ISO 27001, SOC 2 or other industry-specific requirements by showing that you manage offboarding, control access and limit data exposure

Governance isn't just about saying "no." It's about having **documentation, visibility and processes** that prove you're managing SaaS responsibly.

SaaS governance: not just a security job

SaaS governance is a team sport. It requires collaboration between:



IT

For access, identity and integration



Security

For data protection and risk assessments



Legal

For vendor agreements and privacy compliance



Procurement

For approval workflows and renewals



HR

For onboarding/offboarding flows



Finance

For tracking costs and spend attribution

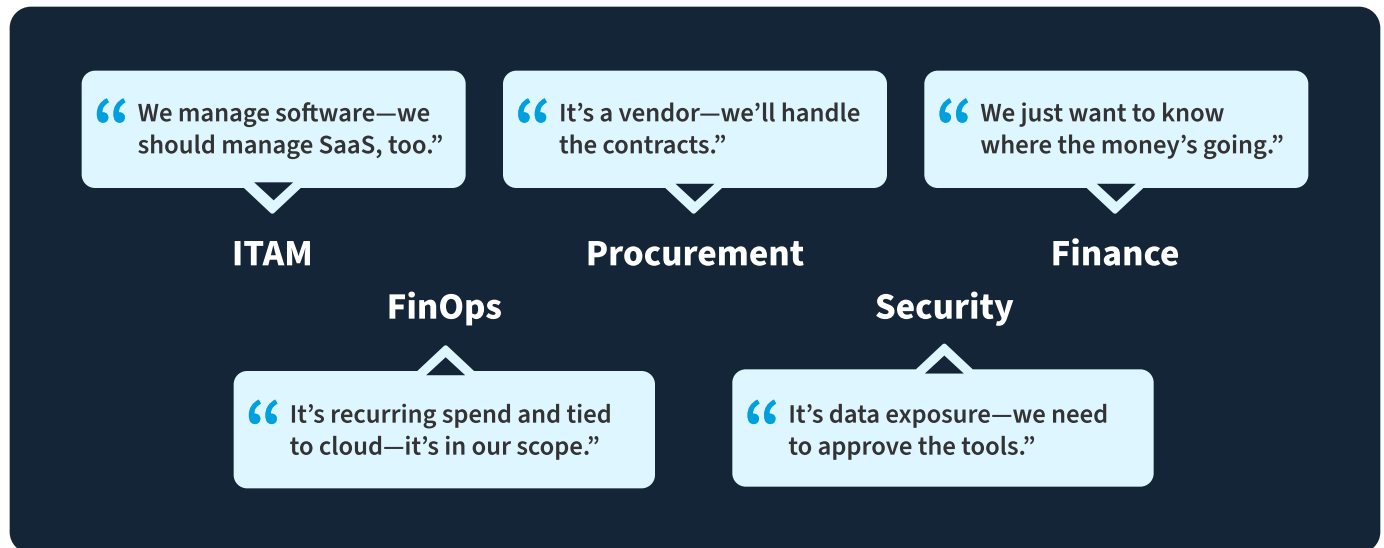


SaaS management becomes the **system of record** across these groups—each of whom plays a part in maintaining control.

Who owns SaaS management

SaaS once lived in the margins. It was something another department handled on their own, far from the core of IT or finance strategy. That time is over.

We know SaaS management *matters* to ITAM, FinOps and beyond, but no one is quite sure who *owns* it.



Here's the funny part: they're all right.

SaaS touches everyone. That's why a siloed approach doesn't work.

Sharing ownership across teams

Teams that successfully share ownership of SaaS management have a few key traits in common:

- **They align around data**
Everyone looks at the same source of truth for SaaS inventory, usage, and spend
- **They assign ownership**
There's a named person or team responsible for the renewals, access, cost and compliance for each SaaS application
- **They collaborate early**
FinOps, ITAM, procurement and security are brought in at the start of renewals and sourcing decisions—not just at the end
- **They clarify and adhere to roles**
Each team has clearly defined and communicated responsibilities—and they stay within those boundaries

Where SaaS management, FinOps and ITAM intersect

Today, SaaS spend is large enough—and risky enough—to matter deeply to both ITAM and FinOps.

Modern ITAM is evolving and shifting from compliance policing to value creation. That means focusing on how often people use software, where it's delivering ROI and where it introduces risk.

For **FinOps** teams focused on cloud optimization, SaaS is often overlooked. Cloud cost management tools such as AWS Cost Explorer or Azure Portal don't cover SaaS—and many FinOps practitioners assume that finance has it handled.

(They don't.)

SaaS spend typically flows through different systems (e.g., corporate cards, departmental budgets), making it hard to track in one place. **That's why SaaS management must become part of the FinOps strategy—because it's where a growing share of spend is hiding.**

SaaS management sits right at the intersection of these evolving practices. Here are the main areas where SaaS bridges them:

ITAM

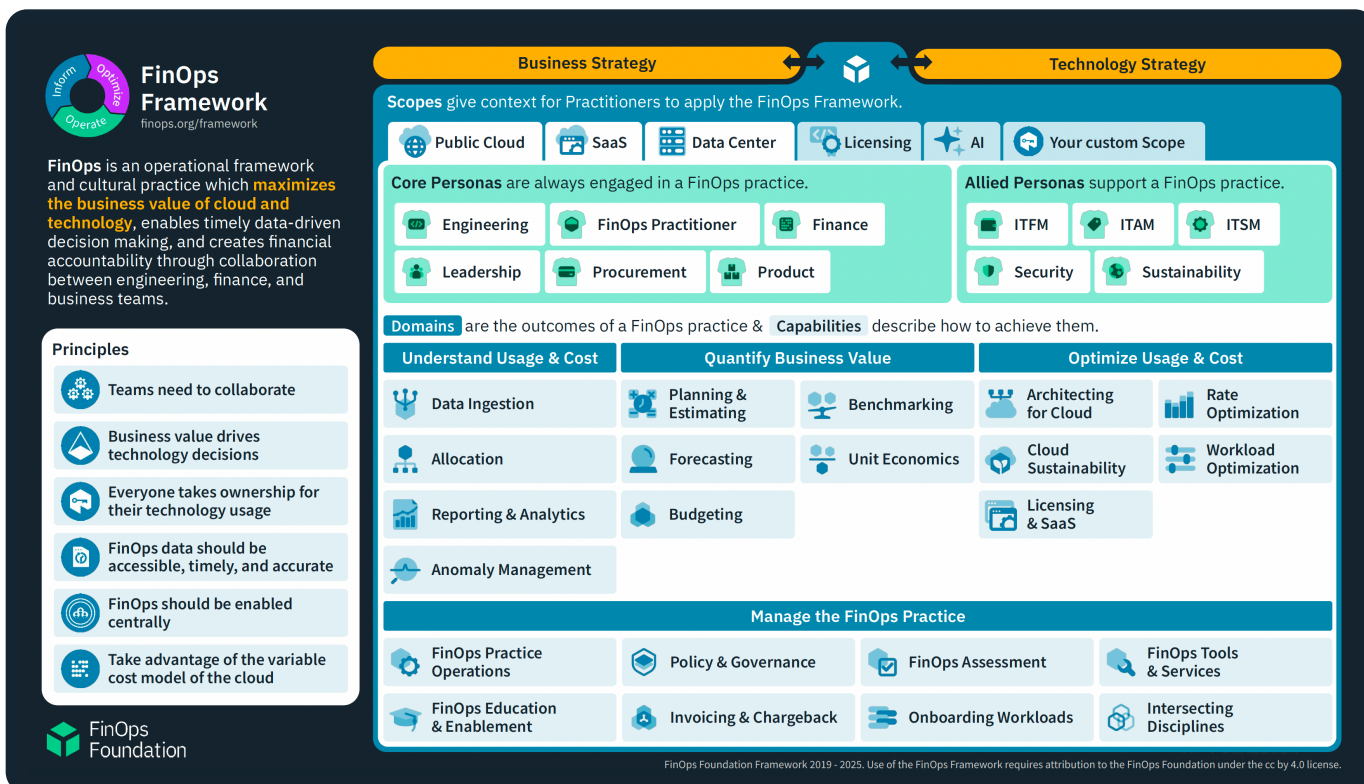
- › Visibility of all SaaS assets
- › Lifecycle governance
- › Access control and compliance
- › Vendor tracking and contract management

FinOps

- › Cost optimization of SaaS spend
- › Budget ownership and spend attribution
- › Usage metrics and rightsizing
- › Forecasting and cloud-to-SaaS integration

The Cloud+ model and expanding scope of FinOps

The FinOps Foundation's Cloud+ model acknowledges this very real need for greater visibility. As a key component of the foundation's FinOps Framework 2025, the Cloud+ model expands FinOps to cover not just IaaS and PaaS, but also SaaS, on-premises software and licensing.



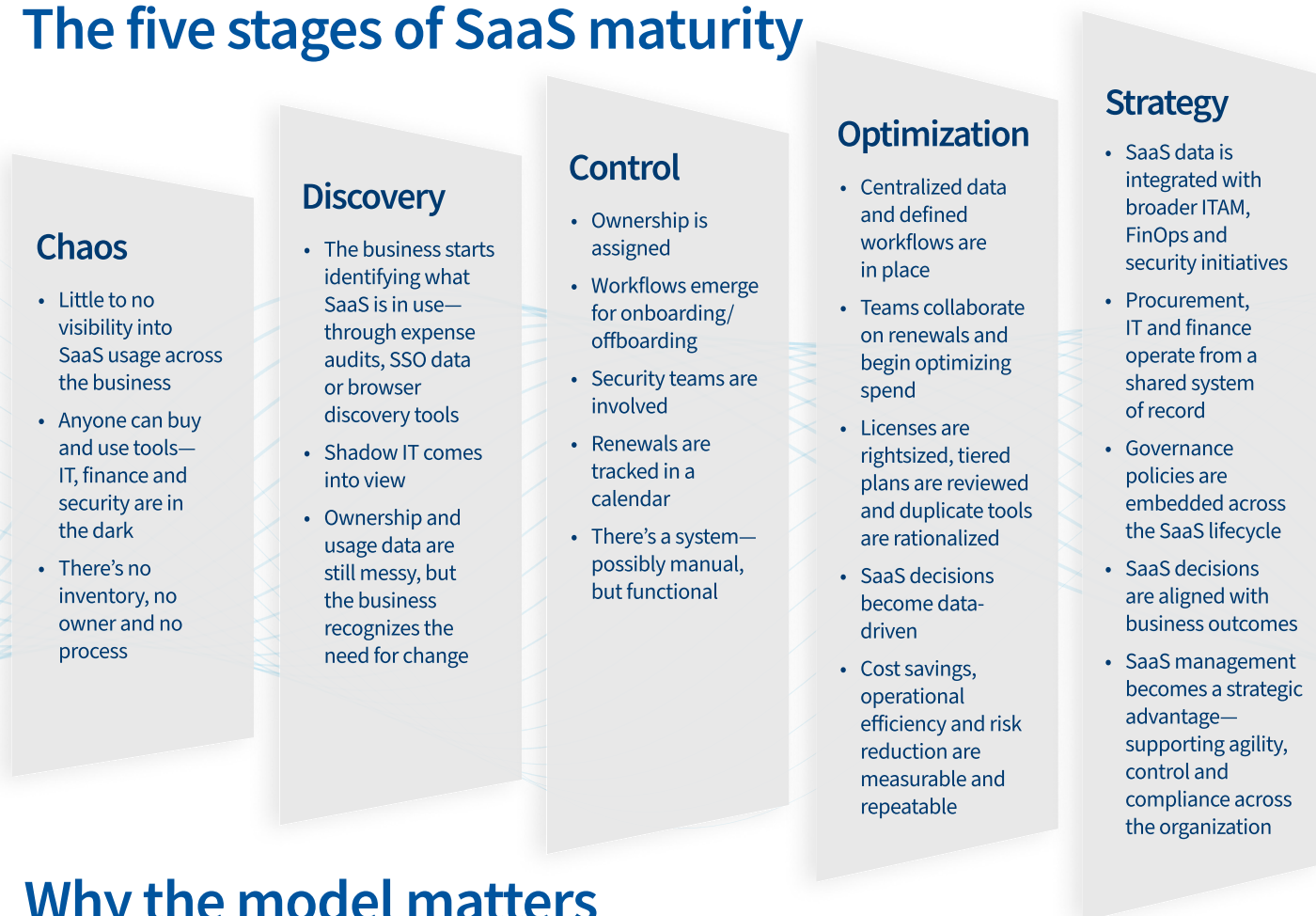
Source: The FinOps Foundation

The SaaS management maturity model

One of the biggest challenges with SaaS management is simply figuring out where to begin. Without a clear map, it's easy to get stuck or overwhelmed. That's where a maturity model comes in.

SaaS management maturity is about progress, not perfection. The goal is to understand your current state and take practical steps to improve. SaaS management doesn't require a giant leap; it's a series of progressions.

The five stages of SaaS maturity



Why the model matters

The maturity model isn't about passing judgment. It's about setting priorities.

- If you're in **Chaos**, your first step might be visibility
- If you're in **Control**, you might focus on usage analytics or renewal optimization
- If you're approaching **Strategic**, your challenge is scaling and cross-functional alignment



By understanding where you are today, you can start taking confident steps forward—and bring your business with you.

Tooling, automation and data strategy

In practice, SaaS management involves a ton of data, stakeholders and moving parts. To succeed, you need **the right tooling and a solid data strategy** to support it.

What tooling should do

At their best, SaaS management tools bring together siloed data and automate critical workflows that are impossible to maintain manually.

Great tooling enables:

- › Centralized discovery
- › User-level usage insights
- › Contract and renewal management
- › Automated role-based access reviews
- › Integration with finance, HR and IT systems

Why automation matters

A well-run SaaS management program must keep up with constant change.

Trying to manually track every change, user, invoice and renewal isn't just time-consuming—it's risky. **Automation** reduces that risk by handling the routine, flagging the unusual and ensuring consistency across departments.

Automation also:

- › Frees up humans to focus on higher-value decisions
- › Enables real-time insights instead of quarterly audits
- › Standardizes processes across global teams

Data is the backbone

Even the best tools are useless without clean, reliable data. That's why a **SaaS management data strategy** is just as important as the tooling itself.

A solid data foundation should include:

- **Source-of-truth identifiers**
Unified application names, owners and categories
- **Usage metrics**
Real engagement data, not just access
- **Financial attribution**
Link SaaS spend to cost centers or departments
- **Lifecycle metadata**
Onboarding, offboarding, renewal and termination dates
- **Risk metadata**
Security posture, compliance flags, approval status

When data is fragmented or inaccurate, it leads to confusion, duplication and missed opportunities. But when data is unified, enriched and accessible, it unlocks powerful insights and efficiencies.

Tooling without strategy is just software

A SaaS management tool is only as good as the processes it supports, the data it ingests and the people who use it.

The right approach is people + process + platform:

- Empower your teams
- Define repeatable workflows
- Choose tools that support those workflows
- Build a data model that evolves with your business

That's when SaaS management becomes more than just another IT project—it becomes an enabler of smarter, safer and more efficient software decisions across the organization.

Quick wins and first steps

You don't need a full-blown SaaS management program from day one.
You just need momentum.

Here are three low-friction actions you can **take right now** that deliver real value and help **build internal support** for SaaS management.

1 Build a SaaS inventory

- Start by discovering what SaaS apps people are using across your business
- Talk to finance and look at expense reports
- Pull a list of apps connected to your SSO platform
- Run a browser discovery tool, if available

Impact:

Visibility, risk reduction and a solid foundation for everything else

2 Identify high-risk or redundant apps

- Tools with no assigned owner
- Duplicate tools doing the same job
- Apps with access to sensitive data but no oversight

Impact:

Immediate risk reduction, smarter renewals and improved collaboration

3 Engage a stakeholder champion

- Find an ally—ideally, someone in IT, finance, procurement or security—who already feels the pain of unmanaged SaaS
- Share what you've found, offer to help and build a coalition

Impact:

Cross-functional buy-in, political capital and momentum to scale

Scaling from there

Once you've got traction, you can start formalizing your program:

- Assign app ownership
- Create a renewal calendar
- Establish an offboarding checklist
- Define a SaaS intake or approval process
- Choose tooling to support the processes that are working

You can start simple, but **start now.**

Let Flexera accelerate your SaaS management journey

Speak to an expert →

Flexera helps organizations understand and maximize the value of their technology, saving billions of dollars in wasted spend. Powered by the Flexera Technology Intelligence Platform, our award-winning IT asset management, FinOps and SaaS management solutions provide comprehensive visibility and actionable insights on an organization's entire IT ecosystem. This intelligence enables IT, finance, procurement and cloud teams to address skyrocketing costs, optimize spend, mitigate risk and identify opportunities to create positive business outcomes.

More than 50,000 global organizations rely on Flexera and its Technopedia reference library, the largest repository of technology asset data. Learn more at flexera.com.

