How To Build A Sustainable Access Governance Program

eBOOKS
by Avatier

HOW TO BUILD A SUSTAINABLE ACCESS GOVERNANCE PROGRAM

INTRODUCTION

A sustainable access governance program is one of the best ways to keep your organization safe from security threats. You're about to learn how to choose access governance software, train employees on security, and continuously monitor your environment to proactively identify risks.

How to use this e-book whether you are a novice or pro in access management

This e-book is written with the access governance beginner in mind. In Section 1, you will discover why access governance matters. Also, you will find out the definitions of key terms commonly used in access governance. Once you understand the key concepts, you will find out how to develop a successful program's blueprint.

Some readers may not be new to the challenges of access governance. In that case, you have two options. If your main roadblock to access governance success is employing the right solution, turn to Section 2. You will discover how to select the right software solution and assemble your project plan.

If you already have an access management program up and running with the required software, we suggest you turn to the e-book's final part, Section 3. In this section, you will find the essential practices and methods to make your program sustainable.

In this part, you will find out how to refresh your IT security strategy quickly. Further, we cover the fundamentals of providing access governance to your workforce so everyone can play a role in maintaining access. Finally, you will learn how to proactively monitor your environment and engage senior leadership to maintain a sustainable program.

CHAPTER 1:
THE FUNDAMENTALS OF ACCESS GOVERNANCE

Why Does Access Governance Matter?

Access governance matters because it is your last line of defense against outside threats, disgruntled employees and failing audits. Specifically, access governance means the ongoing process of overseeing access management, fixing gaps and assessing the risks involved at each level.

The benefits of sustainable access governance

By developing an access governance program, your organization will not depend on heroic measures to stay safe. Instead, you will have tools and processes to detect problems right away.

As an IT leader, your organization gains two primary benefits from leading a sustainable access governance program.

FIRST,

the probability and severity of IT security incidents will be significantly reduced because gaining unauthorized access will be much more difficult. For example, a disgruntled employee might be motivated to steal company data, only to find that their access has been removed. Such protection safeguards the company from potential threats.

SECOND,

you will save money because you will not have to secure third-party forensic experts to manage critical security incidents. Finally, a successful access governance program empowers your workforce in practicing good security habits.

What happens when access governance fails

When an access governance program fails, the organization can suffer in multiple ways. In 2020, the U.S. government fined Capital One $80 million for a significant 2019 IT security incident. Beyond the fine, the company also had to devote resources to assist government agencies in their forensic investigations. By contrast, a more robust access governance program can make it much more challenging to infiltrate a secure network.

Sustainable access governance requires a comprehensive program

An effective access governance program requires technology to monitor systems and user accounts throughout the organization. However, technology is not enough. You also need employees to provide comprehensive and targeted training. Further, it would help if you had managers review monthly reports, audit findings and alerts to detect problems and fix them right away.

To achieve the benefits of a sustainable access governance program, you need to understand the key initiatives that support a successful program.

Further Reading:

Data Governance Matters Now More Than Ever (Microsoft)

Lessons Learned from Access Governance Failures in the News (Avatier)

CHAPTER 2:

THE KEY ACCESS GOVERNANCE CONCEPTS YOU NEED TO KNOW

To discuss access governance effectively, there are a few key initiatives necessary to direct an access governance program. Review these definitions with your team to make sure everyone understands them. The critical point is to have a clear definition that everybody in your organization understands.

The Top 6 Key Concepts You Need to Know

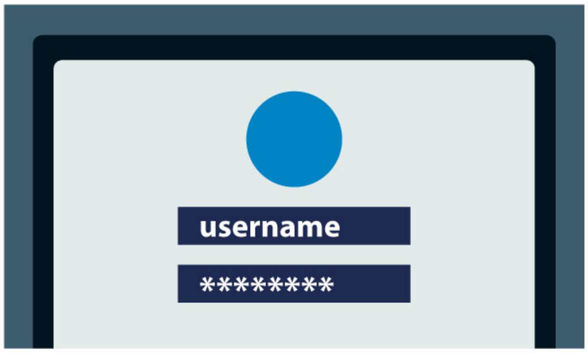
Identity and Access Management (IAM)

According to Gartner: "Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons."

Password Management

Password management includes the technology and practices of managing passwords in an organization. Effective password management also includes rules such as password complexity and updating passwords periodically. A password management software solution makes it easy to monitor all user passwords and ensure passwords align with company policy requirements.

Password



Multi-Factor Authentication (MFA)

The age of relying exclusively on passwords to enable access is over. Multi-factor authentication (also known as two-factor authentication) means users have to pass two hurdles before they gain access. For example, an MFA implementation may require users to enter a password and then enter a code sent to their phone.

Privileged User Management

In access management, some users have special capabilities, like creating new users and suspending accounts. These privileged user accounts may include IT administrators, executives and other people responsible for overseeing other employees.

Principle of Least Privilege

This best practice principle means employees are only given access to systems they need to do their jobs. That means that a finance employee would not have access to a human resources system, for example. By limiting access privileges, the impact of access credential misuse is minimized because a single access credential will only unlock a small number of capabilities.

Single Sign-On

The traditional sign-on approach requires end-users to enter different usernames and passwords each time they access a new system. By contrast, a single-sign-on system means users enter login details once and get on with their work.

Now that you understand the fundamental concepts of access governance, it is time to plan a successful program's blueprint.

References:

Identity Management Glossary (Solutions Review)

Identity & Access Management Glossary (Harvard University)

CHAPTER 3:
BUILDING AN ACCESS GOVERNANCE BLUEPRINT

THE 3 FUNDAMENTAL COMPONENTS FOR SUCCESS

There are three fundamental components to a successful access governance program. Discuss each of these elements with your team annually and determine where you can make adjustments.

Define your identity and access management goals and strategy.

Your approach to identity and access management should ultimately contribute to your organization's goals. For example, you might have a broader IT security goal to protect confidential data from misuse. Ultimately, this goal reduces unnecessary expenses such as lawsuits, fines and incident management. In addition to strategic goals, you may also wish to define project goals to improve capabilities by installing new tools or providing new training.

Review your identity and access management tools.

Modern companies have hundreds of applications and many different user accounts. Attempting to keep track of so many moving parts with email and spreadsheets is unlikely to work. Therefore, the second element of a sustainable program is to buy and implement specialized IT security software solutions. For example, you might buy a tool like Apollo, an IT security chatbot, to provide a 24/7 password reset service to employees.

Refine your management oversight processes.

Management attention and direction is the final part of the access governance blueprint. You can hire consultants to implement a system, provide training and other forms of assistance. Ultimately, only managers and executives can provide employees with ongoing direction to ensure access issues are fully assessed and solved.

In our experience, insufficient technology is a significant roadblock to successful access governance. That's why we discuss the benefits of employing the right access governance solution next.

References:

Identity and Access Management Program Plan (Harvard University)

10-Step Identity Access Management Process Design (IT Business Edge)

CHAPTER 4:
ACCESS GOVERNANCE TECHNOLOGY

WHAT ACCESS GOVERNANCE TECHNOLOGY CAN DO FOR YOU

There are three main ways that governance software makes your organization more effective.

Consistency

The success of an IT security program often comes down to the weakest link. If you leave one server or application poorly protected, that asset is most likely to fall victim to an attack. Access governance software makes it easy to scale up your access program to cover all user accounts, applications and locations.

Save time on administration

IT administration tasks, like reporting, need to get done each month. With software, collecting and organizing the data for these reports takes minutes. With those time savings, you can ask your staff to focus more time on proactive threat detection and training. As a result, your IT security team will have more capacity to handle unexpected threats.

Improve access governance quality

In access governance, the details matter. For example, you may have a rule stating that former employees' user accounts must be removed within 24 hours. Access governance software makes it easy to track these issues so your team makes fewer mistakes. By handling the fundamentals of access governance effectively, the IT department will gain more credibility.

References:

Six Key Identity and Access Management Benefits (TechTarget)

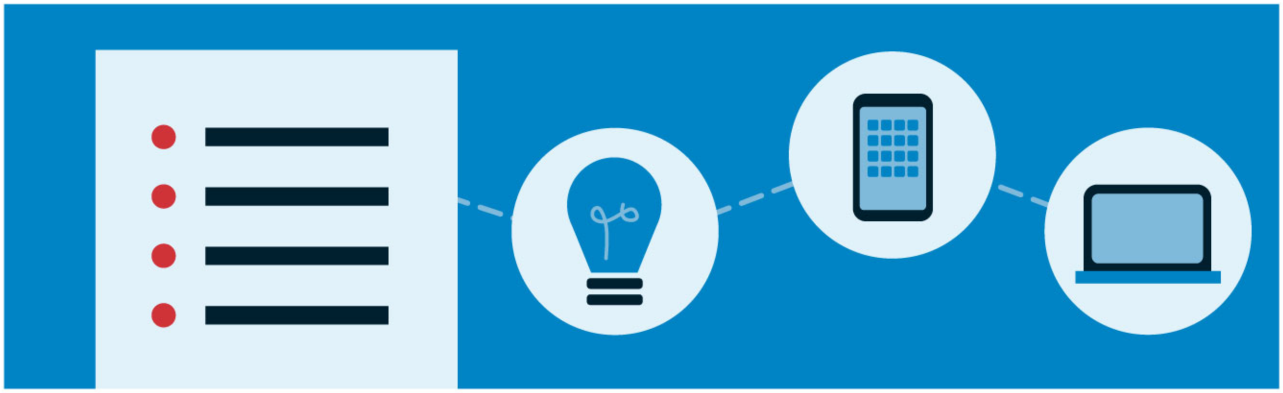
3 Reasons to Deploy an Identity and Access Management Solution (Biz Tech Magazine)

CHAPTER 5:
CHOOSING AN ACCESS GOVERNANCE SOFTWARE SOLUTION

The 3 Steps in Choosing a Solution

There are dozens of access governance software solutions on the market. You don't have time to sit in software demos day after day. Use this chapter's tips to speed up your software solution process.

Step 1: Develop selection criteria for your access governance software.



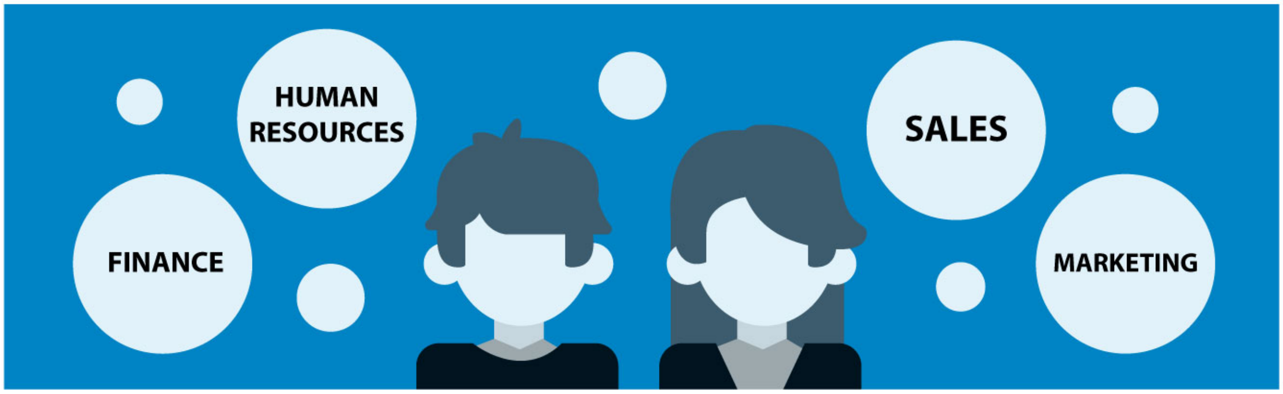
Start by drafting a series of critical features and capabilities you require. For instance, if your organization uses Android smartphones and Windows PCs, then compatibility with those platforms will be critical. Further, you may need advanced reporting capabilities for IT compliance and IT audit. After you list the key technical features consider non-technical factors like the vendor's experience with your industry and training materials.

Don't worry about crafting a perfect list of selection criteria. You will have the chance to validate initial ideas by engaging other stakeholders.

Step 2: Engage your stakeholders in the selection process.

IT security will probably take the lead role in choosing access governance software. That said, it is helpful to involve other critical departments in the company in the decision. For example, corporate areas like finance and human resources may have particular confidentiality needs to protect with an access governance solution. Further, you may want to include business users in the selection process to verify if a product is genuinely user friendly for your users.

As you engage these stakeholders, find out more about their identity, access and IT security requirements so those ideas can be considered in the selection process.



Step 3: Compare access governance solutions on a technical and business level.

Based on the above steps, you are now in an excellent position to create a shortlist of possible access governance software options. By checking a software directory like Capterra, you can quickly determine and compare different software solutions' basic technical features.

However, you will have to bring your judgment to bear when it comes to evaluating business fit. To get the answers you need, expect to spend some time in meetings with vendors. Instead of passively sitting through software demos, come prepared with a list of questions (e.g., "I need monthly reports on IT compliance. How would I satisfy that need with this app?") to make the most of these meetings.

By this point, you will be able to recommend a software solution for your company. Choosing software is a significant step forward in improving access governance. Now you need to build a project plan to implement the software entirely.

References:

Do They Get It? Assessing a Vendor's Industry Experience (Avatier)

Will Your Vendor Selection Process Stand Up To Audit? (Avatier)

CHAPTER 6:

FROM AN ACCESS GOVERNANCE IDEA TO REALITY: YOUR PROJECT PLAN

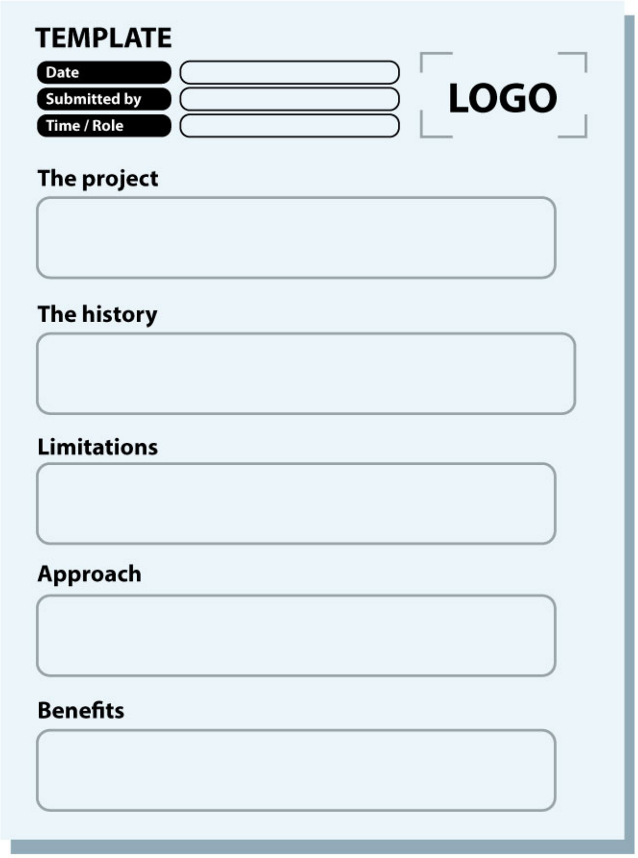
In the last chapter, you looked at the market of access governance software solutions and chose your company's product. Due to the complexity of access governance programs, you need to organize an IT project group to implement the software for your company's needs.

Create a business case to secure funding

Before you can leap into project implementation, you need funding. We recommend creating a business case explaining the benefits of access governance for your organization. To maximize your chances for approval, review other IT security projects have recently been approved by the company.

If your company does not have a formal business case template, make sure you cover the following key themes.

- The problem you're solving. Outline the fundamental IT security problem you seek to solve with an access governance software implementation.
- Your recommended solution. Explain the software solution you are recommending and summarize your rationale for making that selection
- The request. Request resources (e.g., budget and staff time) to implement the project.
- Appendix. Provide further details on your vendor selection and other supporting details for the request.



TEMPLATE

Date

Submitted by

Time / Role

LOGO

The project

The history

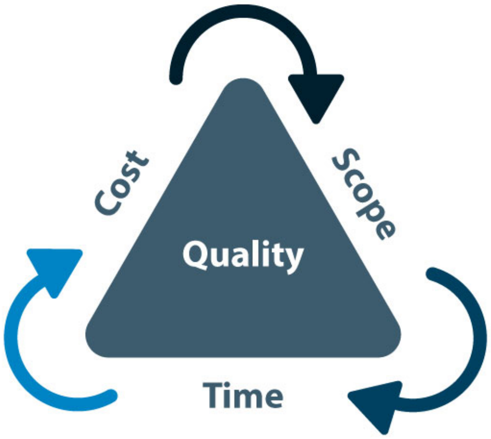
Limitations

Approach

Benefits

Set your project's key parameters

In this step, you are applying Project Management 101. You need to develop a project budget, schedule and project team. If possible, we recommend working with an IT project manager equipped with a professional credential like the Project Management Professional (PMP) certification. Remember that your project plan needs to cover more than software considerations. You will probably need a plan to provide training to employees and integrate the software into existing IT security processes.



Common implementation mistakes to avoid

There are a few common problems that commonly occur when it comes to leading an access governance project. Review these mistakes and make plans to minimize their likelihood.

- **Inadequate quality assurance and testing**

  IT security effectiveness requires that you build comprehensive programs. A single missed app could increase your hacking risk substantially. To mitigate this risk, plan for extensive testing to find problems and get them fixed quickly.

- **Lack of change management**

  New software, even if it is easy to use, means change. To succeed with the new access governance solution, your employees need guidance. Failure to provide training and communication to employees about the new software's implications means you are likely to see less success in your implementation.

- **No plan to sustain the software after the project is completed**

  During an IT project's excitement, it is easy to forget that the project will eventually end. That means your existing IT security staff will need to take on responsibility for using the access software. As you plan the project, consider which managers or teams will take responsibility for using the software after the project is completed.

  Now that you have the right access governance software solution in place, what's next? It is best to support the software with an effective program and strategy.

References:

6 Questions To Answer Before You Start an Access Governance Project (Avatier)

10 Identity and Access Management (IAM) Implementation Mistakes (Computer Weekly)

CHAPTER 7:

BUILDING A SUSTAINABLE ACCESS GOVERNANCE PROGRAM: KEY MANAGEMENT AND TRAINING BEST PRACTICES

Access Governance Program and Strategy

Putting software in place to manage access is a good step. However, that software will not accomplish much unless it is attached to a broader strategy. We are now going to move away from tactical questions of software selection so you can build a comprehensive IT security program and strategy.

Start with strategy

Ultimately, access governance is a way to enable your company's IT security strategy. Taking some time to review and update your IT security strategy annually is smart to maintain alignment between the strategy and business reality. Use these strategy questions to develop an up-to-date IT security strategy:

- What is the company's recent experience with IT security? (If you have experienced a major hacking incident in the past year, recovering from that incident will be a crucial part of your strategy.)

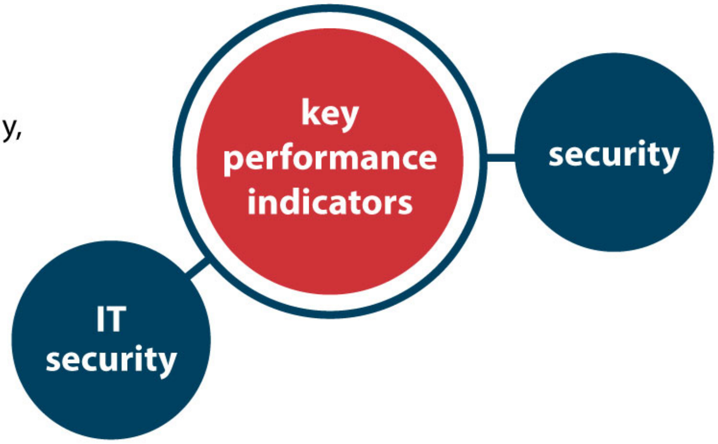
- What changes in the external environment change your IT security situation? (Example: The growing influence of ransomware may be a concern for some companies.)

- What has changed inside the company in the past year, especially in terms of technology? (Example: Your company has expanded its use of cloud computing services, which pose new security risks.)

By answering these questions thoroughly, you will be positioned to make adjustments to your IT security strategy.

Measuring your access management program

A clear IT security strategy gives you guidance about the broad areas of emphasis. To measure your performance weekly, monthly and quarterly, you will need metrics and key performance indicators. To start your measurement process, look at the key performance indicators articles referenced in the article's references section.



TIP: Access governance software will track many different types of data points. Only a few metrics will likely be helpful for your company's needs. Choose a handful of metrics that best measure whether you are making progress toward your strategy.

Access Governance Program tips and tricks

The following tips will help you maintain your program in light of new security threats.

- Check your employee training program. Most employees do not think much about IT security best practices. Therefore, you need to help them succeed by regularly providing training.

- Check your compliance with industry-specific requirements. Some industries have unique IT security requirements, like HIPAA in health care. Reach out to your network to find out the most significant industry standards. If your company has an IT compliance function, ask for their suggestions as well.

- How do you use reporting to improve? Producing IT security reports is not valuable on its own. The true value in IT security reports lies in using this data to improve your IT security defenses. Take some time to evaluate the content and design of access reports you produce. If your leadership finds them challenging to understand, they are less likely to act. Go back to the drawing board and simplify your reporting until the information becomes actionable.

References:

Advances in Access Governance Strategy and Technology (TechTarget)

Identity & Data Access Governance (PWC)

Find Out If Your Access Management Program Is Successful with KPIs (Avatier)

The Must-Have IT Security Maintenance KPIs (Avatier)

CHAPTER 8:

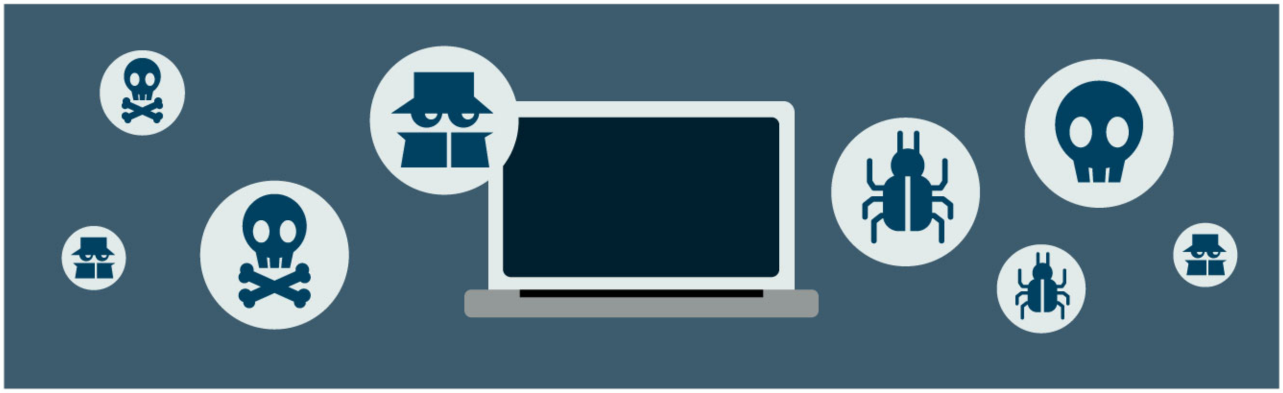
ACCESS GOVERNANCE - TRAINING YOUR EMPLOYEES

Why do your employees need access governance training?

You have an access governance strategy in place and the right software to bring it to life. Now you need to engage your workforce to support access governance.

Your IT security department probably handles most IT security matters. They run the program, answer specialized help desk tickets, and more. No doubt about it, your IT security department plays a leading role. That said, there is a limit to what that team can reasonably achieve. Each and every employee needs to understand the risks and dangers presented by modern technology and empower them to make smart, security-focused decisions.

Take phishing attacks as one example. CSO, an IT security publication, reports the following about phishing attacks in 2019:



- 94% of malware is delivered via email
- Phishing attacks account for more than 80% of reported security incidents
- $17,700 is lost every minute due to phishing attacks

Training your employees on the fundamentals of IT security awareness will reduce the chances of a successful attack. After all, it is not feasible to expect IT security to directly answer questions about every suspicious email or message users receive.

Developing the "minimum effective dose" for access governance training

Your approach to offering access governance training probably combines both general best practices and company-specific considerations. As a starting point, assume that you only have one or two hours of training to teach your employees what they need to know. Given that constraint, consider offering training on the following topics.

- The risks of sharing logins and passwords to the company and customers:
- How to use single sign-on technology so you have fewer passwords to memorize
- A walk through the fundamental principles of your company's IT security policies with a focus on access and password issues
- The role managers play in access governance success (e.g., reviewing and approving access changes)
- Who to contact for support when employees have questions

Understanding your options when providing employee training

There are a variety of methods available to deliver access governance training to employees. If your company is making a significant change, like installing an access governance software platform for the first time, offer more high-touch training options (e.g., webinars with plenty of question-and-answer time). On the other hand, if you have a well-established program, you can emphasize self-study resources like "Frequently Asked Questions" on your corporate intranet.

TIP: November is National Cybersecurity Awareness Month, and it is an excellent opportunity to provide additional guidance and training to employees.

References:

The Benefits of Information Security and Privacy Awareness Training Programs (ISACA)

Evaluate The Effectiveness of IT Security Training In 5 Steps (Avatier)

How To Design A Role-Based IT Security Training Program (Avatier)

National Cybersecurity Awareness Month (Cybersecurity & Infrastructure Security Agency)

Top Cybersecurity Facts, Figures and Statistics for 2020 (CSO)

CHAPTER 9:

ACCESS GOVERNANCE: USING MONITORING AND METRICS EFFECTIVELY

In a previous chapter, we briefly touched on monitoring and metrics. These techniques are critical in determining whether or not you are achieving your strategic goals. That's not all. Monitoring can help you find security problems and fix them before a hacker comes after you!

Why you need access governance monitoring and metrics

Think of monitoring and metrics like your annual medical exam. It is a way to evaluate your IT security program's health, receive advice and address problems while they are still manageable. In our experience, most companies see the value in monitoring and metrics. Unfortunately, they have an altogether different problem: too many metrics!

Using too many metrics, especially when discussing IT security with non-technical executives, is not wise. Instead, it would help if you learned the art of drawing conclusions from the data and preventing actionable recommendations based on your complete monitoring work.

Build your monitoring and metrics dashboard with the end in mind

Before digging into your data, ask yourself about the ultimate purpose behind your dashboard. It is a means to an end—to find problems quickly and drive action in the company. Therefore, it is best to use a combination of leading and lagging indicators. Use the following examples as you build your monitoring report.

Leading Indicators

- Percentage of users who have completed access governance training in the past 12 months
- Average time (in hours) to deactivate user accounts when employees leave the organization

Lagging Indicators

- Number of IT security findings reported by IT compliance or internal audit every quarter
- Frequency of negative press mentions due to company IT security failures

There is no single perfect indicator for access governance. Instead, choose a few indicators that you believe will be helpful and use them for a few months. If they provide no value to the organization after six to 12 months, then look for other ideas.

How to use your access governance report to safeguard your business

Using an access governance report to protect your business is easy. After you finish preparing your report, ask yourself the following questions:

- In the past month (or quarter), what is the most significant access governance problem?
- What was the root cause of the problem?
- How can we use automation and software to prevent these access governance issues from recurring?
- Who will lead the effort to address the IT security deficiency?

References:

Find Out if Your Access Management Program Is Successful with KPIs (Avatier)

10 Identity Management Metrics That Matter (CSO)

CHAPTER 10:

ACCESS GOVERNANCE – MANAGEMENT OVERSIGHT

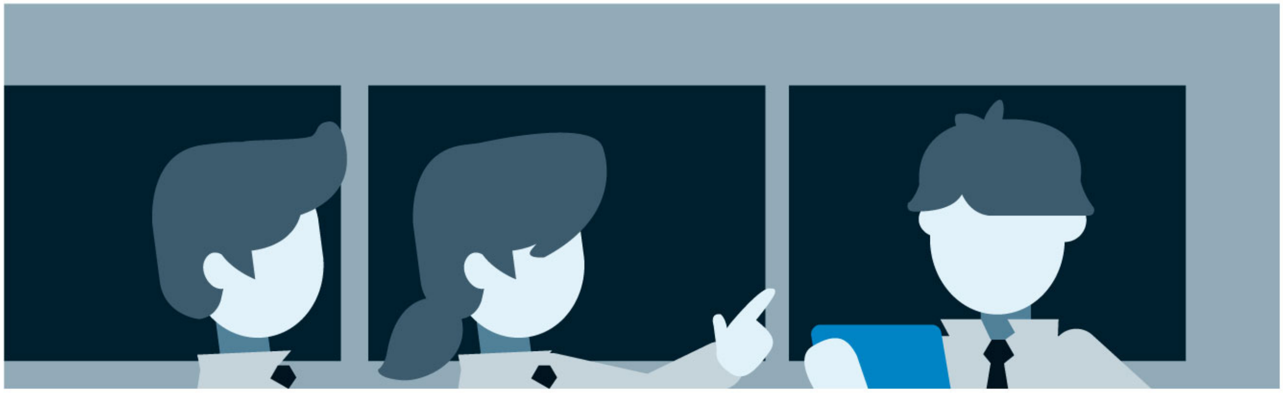
3 CRITICAL ROLES FOR SENIOR MANAGERS

Managers, especially IT security managers, are the last line of defense in access governance. Indeed, your IT security specialists will manage most of the day-to-day access work. However, there are three critical roles senior managers can play to ensure your access governance program is sustainable.

Role 1: Act as the project sponsor on access governance projects.

From time to time, your IT security team will need to organize a project team to improve. For example, you may decide to install a new security software application like a password management tool. Specialists will handle most of the details on the project. As a senior manager, you can help keep the project moving along well by acting as the project sponsor.

During the project, make sure you meet regularly with the project manager to discover problems. For example, you may be called upon to persuade another department to sign off on the project plan. Or you might need to exert your influence to encourage employees to attend access governance training.



Role 2: Use your judgment to balance IT security with other business needs.

As a manager, you have a broader insight into the company's operations. You know the company is getting ready to go public. Or you might get a warning about a new acquisition. These business developments all have an impact on the company's appetite for IT security. Therefore, when your IT security specialist recommends a new project idea to tighten access governance, you can play a role in evaluating the criticality of that idea.

You might ask your team members to develop a more robust business case. Alternatively, you might decide to direct them to solve the problem differently. For example, it might be better to improve employee training to solve the problem of using low-quality passwords.

Role 3: Develop your staff.

The first two roles for managers are essential, but they have one drawback. Project sponsorship and balancing IT security matters only come up occasionally. By contrast, staff development is an ongoing need for all of your employees.

Start by meeting regularly with your employees to hear about their progress and needs. Sometimes, they may turn to you for advice. In those circumstances, you have the opportunity to help them develop through coaching. For example, instead of picking up the phone to persuade a reluctant stakeholder to follow password rules, guide your employee on how to take on this responsibility.

Finally, look for ways to encourage the long-term career goals of your staff. For example, some IT security professionals may be keen to learn newer technologies like cloud apps or container technology. In those cases, ask your employee how you can best support their professional development growth goals. If they need budget approval to purchase training, aim to approve those requests. Cybersecurity talent remains in high demand and failing to give your staff growth options may cause them to look for better opportunities outside your company.

References:

The Impact of Governance on Identity Management Programs (ISACA)

Get Your SSO Software Project Funded With a Business Case (Avatier)

Conclusion

You have learned all the fundamentals to build an effective access governance program. You know how to select the right software solution for your company. You have also learned how to design the "minimum effective dose" of IT security training for employees. Finally, you have learned when and how to use monitoring and metrics to detect and fix problems.

Your next step from here will depend on your situation. Building an access governance program from scratch will go back to Chapter 1 and start by building your foundation. If you are aiming to enhance an existing program, focus on Chapters 7-10 instead. Access governance requires constant discipline. Using the principles and practices outlined in this book will help you keep your company's data safe from attacks.

AVATIER

How To Build A Sustainable **Access Governance Program**

Avatier.com