wipro | edgile
a wipro company

Why Leading CISOs are Adopting a Strategy-First Approach to Identity & Access Management

With security breaches dominating the headlines, and audit and regulatory deadlines looming, today's CISOs can find themselves pulled in multiple directions. How should a CISO prioritize which problem to attack first? This is a particularly difficult question with respect to Identity and Access Management (IAM) programs, which are expensive and difficult to explain outside of IT.

As pressure mounts to deploy new technology as quickly as possible to meet audit or regulatory deadlines, IAM efforts are too often managed like so many other IT projects: from a technology-first perspective. Unfortunately, this type of approach—with technical requirements compared against various product's attributes—can turn into a painful mistake.

The problem is that IAM drivers—and potential solution sets—extend well beyond a technology perspective.

The problem is that IAM drivers—and potential solution sets—extend well beyond a technology perspective. The power of a strategy-first approach is that it looks beyond technology to incorporate other important perspectives. This paper explains the benefits gained from such an approach, followed by a 6-perspective methodology that has delivered proven results for our clients.

Two reasons to think strategy before technology

Perhaps you're wondering: "Why should I divert to this detailed work when I already know the problem? All my users complain that it's X."

Our clients have found two main considerations for executing an IAM strategy.

1

It ensures you solve the right problem.

There are many instances where a CISO discovers too late they're only addressing a symptom and not the problem. Two examples:

- A rip and replace effort to fix a bad user experience fails: halfway through it's discovered the company has a data issue that even the new technology will suffer from.
- An effort to consolidate a costly infrastructure stalls: it's discovered that a complex business process depends on legacy technology.

In both cases, the immediate pain point hid a more fundamental, underlying problem. Had this been discovered upfront, an entirely different approach would have been taken. In the above examples, fixing the data issue and the business process design would have made any subsequent technology change faster and cheaper.

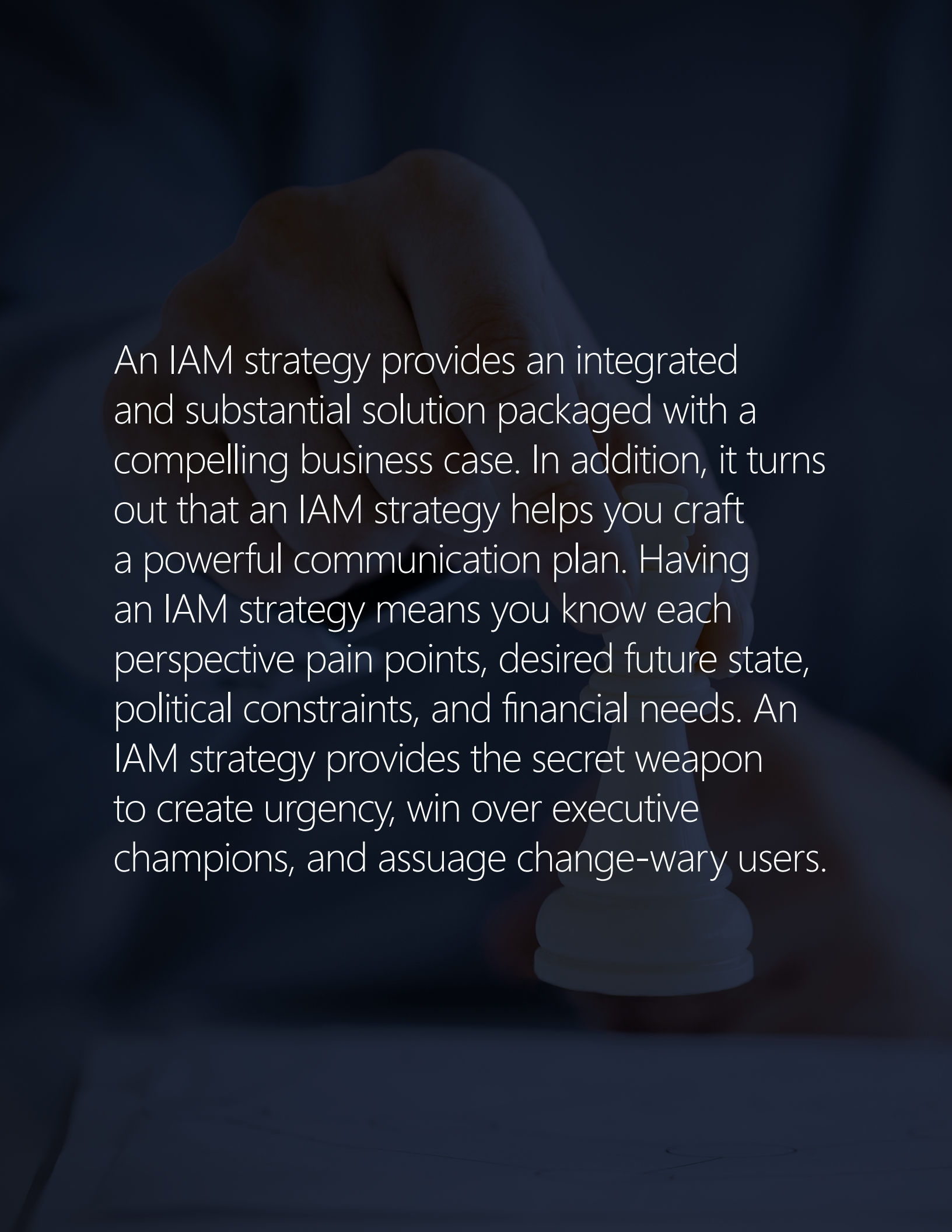
2

It provides the business case for an integrated and substantial solution.

A CISO may at times feel as though he or she is playing a game of whack-a-mole because of top priority problems popping up each day from internal audit, regulators, business leadership, and the security team. Obtaining funding and business commitment for each solution individually can prove daunting, as well as leading to conflicting and overlapping solutions.

To avoid this, a CISO must find a way to address all issues in a comprehensive fashion. Such a comprehensive solution must be able to:

- Provide an integrated solution set across the IAM services.
- Substantially address business and risk drivers.
- Package the above into a compelling business argument that supports internal selling of the proposed investment.



An IAM strategy provides an integrated and substantial solution packaged with a compelling business case. In addition, it turns out that an IAM strategy helps you craft a powerful communication plan. Having an IAM strategy means you know each perspective pain points, desired future state, political constraints, and financial needs. An IAM strategy provides the secret weapon to create urgency, win over executive champions, and assuage change-wary users.

Six perspectives of a comprehensive IAM strategy

At its most basic level, an IAM strategy will reveal where the organization stands, where it needs to go, and the path to get there—while communicating the resulting benefits.

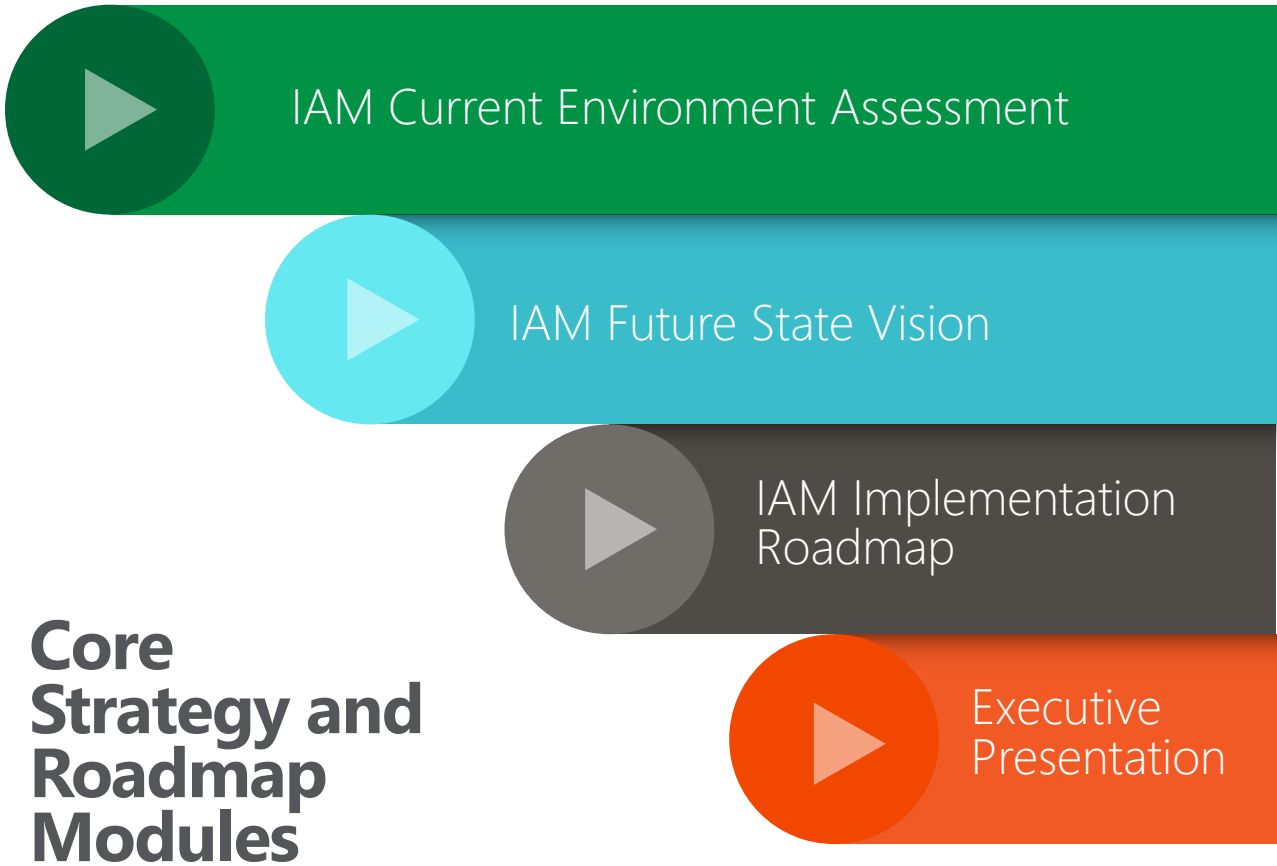


Figure 1. Basic steps for a strategy effort.

Core Strategy and Roadmap Modules

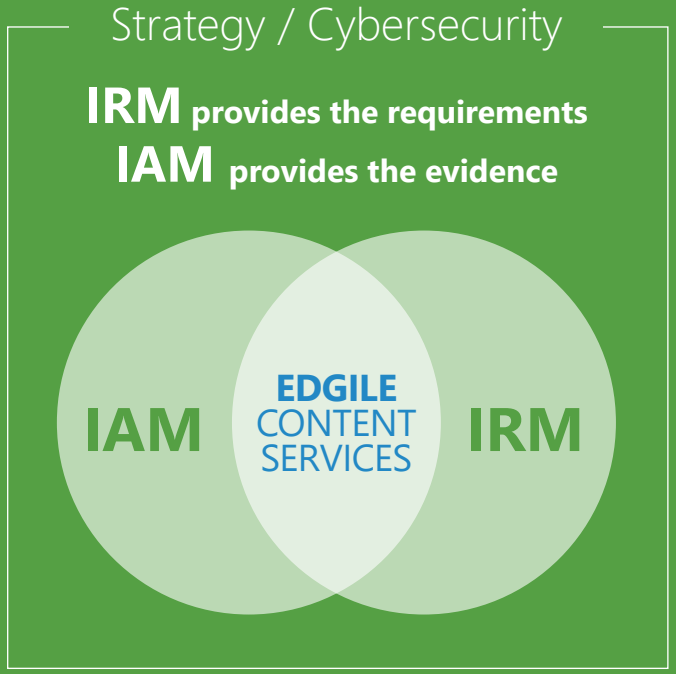
The secret to an effective strategy lies within how each step is accomplished. It requires the team to look beyond technology to other equally important perspectives. To build a business argument, the strategy must consider the Business context and integrated risk management. To ensure a comprehensive solution set, the strategy must consider the people, process, and data perspectives—in addition to the technology.

Together, these create six perspectives for IAM Strategy that are considered during each core module. This provides a way to design a comprehensive solution set that balances the needs and constraints of each perspective. The insights and data gained are used to plan for organizational change and to make a business argument, and to build urgency, gain executive sponsorship, and build a cross-functional team.

INTEGRATION OF IDENTITY AND RISK MANAGEMENT

The inclusion of an Integrated Risk Management (IRM) perspective illustrates how we see risk as tightly connected with Identity and Access Management (IAM). While IRM supplies the requirements for IAM, it is IAM that provides the access control evidence to support effective risk management. Hence, IAM provides both risk control and awareness capabilities.

Successful Identity programs reflect this coupling within the governance and decision making structures. Programs with long-term success are justified on a risk reduction basis, as opposed to just a cost reduction basis. Organizations with mature risk programs are best able to quantify risk and build a strong, risk-based argument.



Within each of these perspectives, there are relevant questions to be addressed, including:

1 Business Context

What are the business drivers? Measures of success? What digital strategy must a solution support?

2 Integrated Risk Management

What are the governance, risk and compliance drivers? Are they known? What are the relevant risk economics driving decision making? Who owns risk?

3 Process

What is the current user or customer experience? Can it be simplified? What processes must the solution support? Are there automation opportunities? Can business processes be designed to better use in-place technology? What is the cost of process re-design compared to the cost of new technology?

4 People

Is there an engaged, cross-functional IAM team representing all the key technologies and business owners? Do they have the right skillsets and roles within the organization?

5 Data

Who owns what data? Where is data duplicated? What are the relevant data risks? Are there opportunities to provide a data service layer?

6 Technology

What is the current IAM technology maturity? What maturity level is needed to address the business and risk drivers? Where are any functional gaps and/or overlaps?

Case Studies: Two companies evaluate a technology vs. strategy-first approach

Case #1: A strategy effort re-oriented a planned project from focusing on a single IAM vertical to look across all IAM verticals, and in doing so delivered far greater business value.

BACKGROUND

A publicly traded company was planning to expand their provisioning solution to hundreds of additional databases. This expansion was viewed as the highest IAM priority and carried a multi-year and multi-million-dollar price tag. An IAM strategy was completed using the six-perspectives model. Several insights were gained from this effort.

INSIGHTS GAINED FROM THE IAM STRATEGY

During workshop interviews it became clear that the planned solution was partial and overlooked many non-technical business needs, including:

- **Overlooked risk findings:** The solution didn't address a significant open risk finding regarding ownership of non-employee identities.
- **No data access solution:** The solution didn't help the organization answer who has access to what data.
- **Poor user experience not addressed:** The solution didn't assuage a frustrating user experience regarding access request and multiple logins that was actually a business driver of the program.

ACTIONS TAKEN

The planned solution was re-oriented from only access provisioning focused, to look across all IAM verticals. Broadening the solution focus allowed the pain points across all perspectives to be addressed.

- **Re-factored technology roadmap:** The solution set was reconsidered and expanded to address the pain points discovered during the strategy workshops across all perspectives.
- **Business process changes:** Many discovered issues were addressed through process (not technology) solutions. For example, HR was declared the owner of non-employee identities and IAM process were designed accordingly.

RESULTS

- **Significant risk reduction:** The improved solution addressed a far broader set of identity related risks than the original solution, allowing the organization to significantly improve its risk posture.
- **Improved cost savings:** Improved management of non-employee access alone reduced license cost enough to pay for the technology improvements. This is an item the original solution would have skipped.
- **Broad organizational support:** The program has broad organizational support and is on track for successful completion.

TAKE AWAY

The results of this effort showed a common picture: the technology-first solution would have plunged the IAM team into a multi-year, multi-million-dollar project without fully meeting the business goals.

However, a strategy-first approach allowed a stronger plan to emerge. The final plan addressed each of the discovered pain points; it drove process and data improvements in addition to a broader technical solution. Finally, it prioritized the planned technical solutions to ensure business drivers were addressed early.

2

Case #2: A strategy effort lead an organization to pivot from a customer-focused IAM solution to a more valuable internally focused IAM solution.

BACKGROUND

A financial services company desired to improve its customer experience by consolidating multiple website logins using a single sign-on solution. Prior to moving ahead with this approach, an IAM strategy was created which raised key considerations previously overlooked.

INSIGHTS GAINED FROM THE IAM STRATEGY

Analysis of the organization's customers and processes revealed that the solution addressed the wrong problem.

- **No business value in planned solution:** Not only were just a small percentage of customers affected, but a

business-driven long-term solution already addressed the problem.

- **Significant opportunity for internal process automation:** The Identity team was understaffed with a high percentage of workload focused on automatable tasks.
- **Significant risk exposure due to manual process:** The high level of manual process created heightened residual risk exposure for the organization.

ACTIONS TAKEN

After assessing the organization from all perspectives, the organization pivoted to focus on more valuable investments.

- **New technology roadmap:** A new technology roadmap was developed to address each of the pain points discovered during the workshop process.
- **Process simplification:** Business processes were redesigned to take advantage of automation opportunities.

RESULTS

- **Costly mistake avoided:** An approximately $1M project was avoided that would have delivered no long-term value to the organization.
- **Internal cost savings:** Dozens of new hires avoided as the Identity team refocused on non-automatable work.

- **Reduced risk posture:** IAM technology provided new visibility into the management of access rights and roles across the organization.

TAKE AWAY

Not only were both Technology and the Business Line working on a solution to the same problem, the Technology proposal would have been a band-aid approach.

The strategy-first process brought the right players—and the right data—to the table, and allowed a holistic plan to emerge. The final plan avoided a costly mistake and focused the organization towards the areas truly needing investment.

Summary

Before moving forward with an expensive IAM program, CISOs should ensure they've developed a comprehensive strategy that considers each of the six perspectives: Business Context, Integrated Risk Management, People, Process, Data, and Technology.

By leveraging this six-perspective, strategy-first process, CISOs can ensure they're solving the right problem, building the business case for an integrated and substantial solution, and delivering high value at relatively low cost.

wipro | edgile a wipro company

ABOUT EDGILE

Edgile, a Wipro company, is the trusted leader in cybersecurity transformation and risk services partnering with the world's leading organizations, including 31% of the Fortune 100 and 20% of the Fortune 500. Our strategy-first model optimizes today's enterprise journey to the cloud and modernizes identity and security programs through a risk lens and expert compliance knowledge. We secure the modern enterprise by transforming risk into opportunity with solutions that increase business agility and create a competitive advantage for our clients.

Edgile Leadership

Gretchen Wichmann | Partner

Gretchen is a Partner and the National Identity Service Line Leader for Edgile. She brings over 20 years of experience in technology and security consulting services. She works with client executives to successfully develop and deliver strategic, business-aligned Security and Identity programs. She specializes in managing client relationships, ensuring successful project delivery and overall client satisfaction. She has worked with the leading IGA solutions including SailPoint, CyberArk, Microsoft, Ping, Radiant Logic, SecZetta and others. She started off her security career at PwC as a Director for the Technology and Data Services practice. She then worked as a Director for Logic Trends/ Optiv and Hub City Media. She holds a Bachelor of Science degree in International Business from Auburn University.

Lawrence Wolf | Managing Partner

As a partner with Edgile, Larry Wolf is responsible for managing client relationships across the United States. He has an extensive background with more than 30 years of experience including software development, project management, consulting management and building small firms. For the past 15 years, Larry's focus has been in the areas of identity and access management (IAM), governance and security. Prior to joining Edgile, Larry held partner and vice president roles at Capgemini, Ernst & Young, Fishnet/Optiv, Sun Microsystems and EMC.