puppet

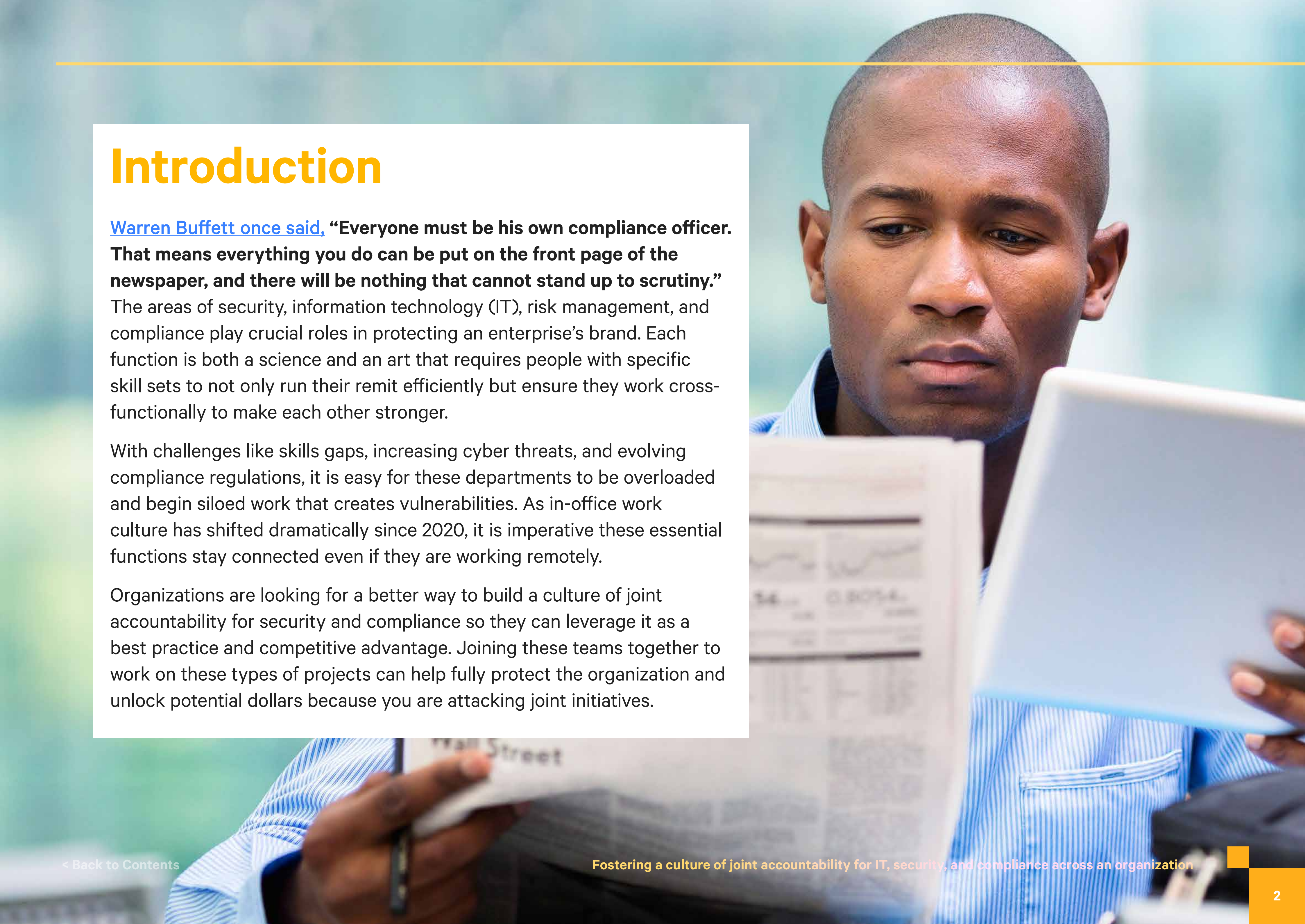
Fostering a culture of joint accountability for IT, security, and compliance across an organization

Introduction

Warren Buffett once said, **"Everyone must be his own compliance officer. That means everything you do can be put on the front page of the newspaper, and there will be nothing that cannot stand up to scrutiny."** The areas of security, information technology (IT), risk management, and compliance play crucial roles in protecting an enterprise's brand. Each function is both a science and an art that requires people with specific skill sets to not only run their remit efficiently but ensure they work cross-functionally to make each other stronger.

With challenges like skills gaps, increasing cyber threats, and evolving compliance regulations, it is easy for these departments to be overloaded and begin siloed work that creates vulnerabilities. As in-office work culture has shifted dramatically since 2020, it is imperative these essential functions stay connected even if they are working remotely.

Organizations are looking for a better way to build a culture of joint accountability for security and compliance so they can leverage it as a best practice and competitive advantage. Joining these teams together to work on these types of projects can help fully protect the organization and unlock potential dollars because you are attacking joint initiatives.

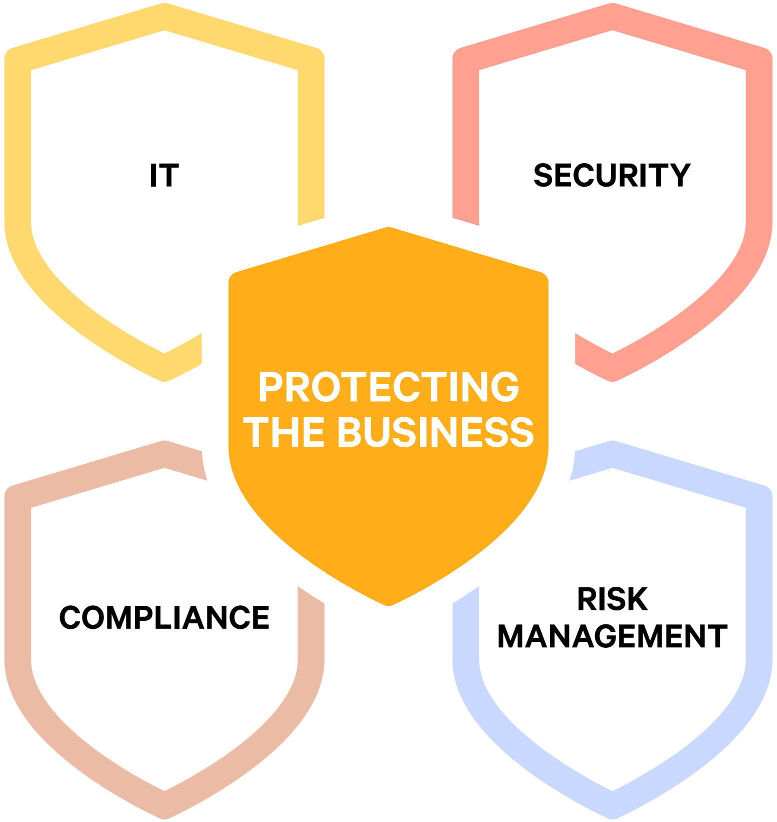


Which came first: compliance or security?

It is often debated among professionals that compliance does not necessarily mean something is secure, and that something being secure doesn't necessarily mean it is compliant. But the truth is they have a symbiotic relationship, and both are vital to ensuring a resilient business.

Both security frameworks and compliance standards can be strategically leveraged to reduce risk to an organization, and therefore protect its valuable data and brand, and reduce or avoid steep fines. According to the Ponemon Institute, the average cost for organizations that experience non-compliance is upwards of $14.82 million, a 45 percent increase from 2011, making it a more significant and more noticeable pain point for CIOs and CTOs.

IT, security, compliance, and risk management are all working toward the common business goal of protecting the organization from harm. Suppose these leaders join forces and work together on projects that have overlapping initiatives. In that case, it stands to reason they can unlock more opportunities for funds to meet the needs of many instead of just one...two birds, one stone.



How we got here

The business goals of digital transformation were to leverage innovative technology and data to drive better business outcomes. Things like cloud migration, the Internet-of-Things (IoT), mobility, artificial intelligence (AI), and machine learning can drive remarkable business outcomes from efficiency to revenue growth.

But as many security leaders know, the more technology you add to your tech stack, the more opportunities are created for vulnerabilities that put the business at risk. This creates an opportunity for security, risk, and compliance teams to work together and put proactive safeguards in place to protect against both the known and unknown risks.

> "With challenges like skills gaps, increasing cyber threats, and evolving compliance regulations, it is easy for the departments of IT and Security to be overloaded and begin siloed work that creates vulnerabilities."

How GDPR was a catalyst for innovation

According to Forrester, risks and threats to businesses are increasing and they expect privacy regulations across the globe to intensify. As it became clear that regulations like GDPR were going to keep coming, organizations had to identify who was in charge of managing the operations to find this valuable data and ensure its security and compliance.

In 2018, GDPR required the role of the Data Privacy Officer (DPO) to head up all things around data protection accountability. GDPR is a mammoth regulation, but enterprise leaders needed to know how its requirements align and overlap with other regulations such as HIPAA, PCI DSS, FedRAMP, etc., and how these regulations align with current security frameworks they may be leveraging, such as NIST, ISO, etc.

The role of the DPO didn't widely exist yet in 2018 for many enterprise companies, so it became a driver for organizations to consider redefining who owns what within the scope of compliance. Enterprise organizations soon realized there were many crossovers between various business problem owners, especially in compliance, IT, security, and risk management.

Forcing the unraveling of the silos and speeding up innovation

Since the pandemic, there has been an additional evolution of the roles and responsibilities of IT, compliance, security, and risk management. The beginning of the pandemic forced organizations to shift to a remote-first work culture seemingly overnight. IT Operations teams are challenged with constantly changing and competing priorities from the business and must be agile to keep the business running smoothly. Many organizations also chose to accelerate their digital transformation plans in response to the pandemic.

Keeping the business running securely and not drifting from compliance standards was quite another battle. The larger the infrastructure or hybrid infrastructure, the more complexities presented themselves. IT Operations and Information Security teams had to truly partner to focus on hardening security and to enforce continuous compliance across the IT Infrastructure.

The players to build the culture of joint accountability

Each of these functions has a vested interest in ensuring the proper creation and enforcement of policies and procedures to protect the organization.

IT Operations

IT Operations have end-to-end responsibility for the services provided by the IT department, infrastructure, and systems that support an organization's business digital policy enforcement and processes. ITOps is responsible for maintaining the organization's operational stability and supporting new initiatives to help the business innovate.

Information Security

Information Security (InfoSec) refers to the tools and processes deployed to ensure the protection of sensitive information from inspection, modification, disruption, or destruction. It can encompass application security, cloud security, cryptography, infrastructure security, incident response, and vulnerability management.

Risk Management

According to Gartner, "Risk managers look at more operational and tactical exposures to the business that can be summarized and abstracted to inform enterprise risks. They manage areas such as vendor risk management, audit management, corporate risk and compliance, legal matters that affect risk, and even business continuity risks...This is also the bridge where cyber risks are addressed, using information to and from the security management layer."

Corporate Compliance

Corporate Compliance departments help a company ensure it is following laws and regulations that are applicable to the organization. It involves designing, implementing, and monitoring policies and includes training, processes, and procedures.

< Back to Contents

Become a rule follower: leverage it all

Regulations are a regular occurrence

Regulations can seem as never-ending as cyber threats, but truthfully, they are usually born in response to poor practices that lead to mass breaches. These regulations provide organizations with best practices to plug some of the holes that have caused breaches. Global regulations, such as GDPR, with unprecedented penalties, have forced organizations to identify the types of data within their network and infrastructure in order to best manage and protect it.

Security frameworks

There are several security frameworks that IT and security leaders can leverage in order to reduce risk and fortify their security posture. Using one or more of these frameworks assists these leaders in defining processes and procedures to assess, monitor, and mitigate cybersecurity risk such as malware, Distributed Denial of Service (DDoS) attacks, zero-day exploits, etc.

CCPA
CALIFORNIA CONSUMER PRIVACY ACT
GDPR
GENERAL DATA PROTECTION REGULATION
BRAZIL
LGPD
Lei Geral de Proteção de Dados Pessoais

Become a rule follower: leverage it all

Internal policies & desired state

Just as regulations are reactive and born based on gathered data around problems that affect the masses, they can drive internal policies that must be enforced. And leaders in security, compliance, risk management and IT have valuable experience that can help create effective policies. But enforcing digital policies can feel daunting if you go it alone.

The knowledge and experience of your peers who are experts in their remit can be invaluable when trying to create and enforce policies. Suppose risk management, compliance, and security leaders can work together to leverage automation technology to continuously push a "desired state." In that case, they can improve efficiency by allowing highly skilled IT and security professionals to focus on the items that are the highest priority while reducing risk by having an ever-vigilant infrastructure always aligning to policy.

According to the Center for Internet Security (CIS) it's best to put policy into practice to avoid configuration drift through effective monitoring. A recent CIS blog post stated that "the best way to deal with configuration drift is to stay on top of it. A well-managed cybersecurity program helps ensure that you maintain ongoing awareness and proof of secure configurations."

A better way: shared transparency policy as code

Prior to the pandemic, both IT and security teams had been leveraging some form of automation to work smarter, not harder. But solving for security and compliance is not a one-person or single department's job. Everyone needs to pull their weight, and the best way to do that is to partner cross-functionally within your organization with the common goal of protecting the organization with both internal policies and external regulations and standards.

Savvy organizations understand that leveraging automation technology in both security and compliance efforts plays a crucial part in building the bridges that connect every facet of an organization. Automation based on human-readable policy as code allows for shared Infosec-IT transparency into configuration policies encoded into infrastructure definitions so they are continuously enforced and auditable. Trusting that the desired state is being automatically enforced helps with productivity, yes, but it also allows IT and security teams to focus on novel threats and vulnerability remediation to reduce risk.

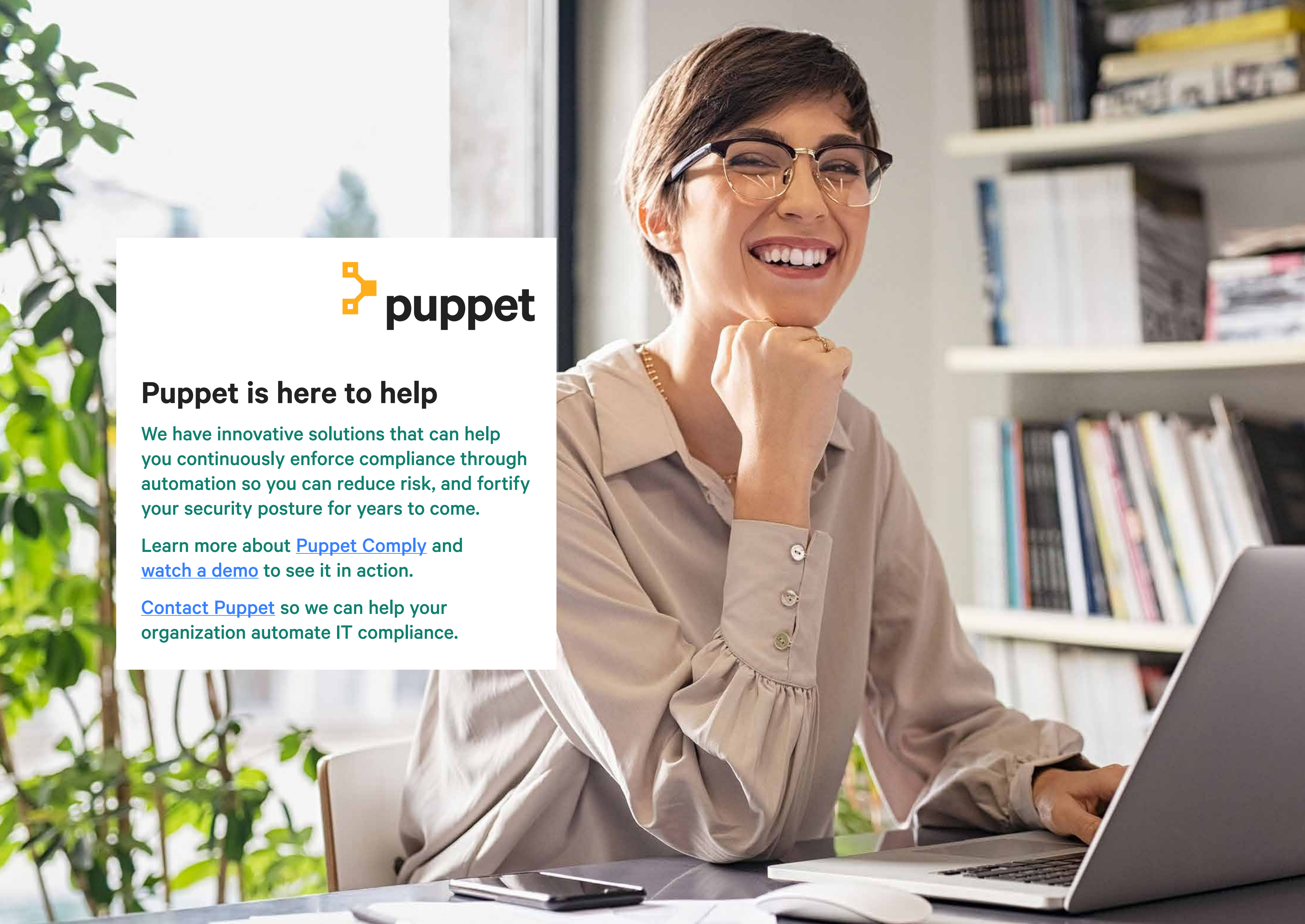
Start today: Build your "better way" taskforce

If you are an enterprise organization, you've likely already been in a physical or virtual room with various team members from each of these departments, especially during the pandemic. During 2020, you were probably trying to be agile and "stop the bleeding" as the world was forced into remote working.

But now, you have an opportunity to break down these silos further and discuss proactive solutions that continually drive a culture of joint accountability for compliance and security.

Here are 8 areas of focus for your new "Better Way" Taskforce:

1. **Discuss the regulations** with which you must comply. Make sure everyone understands them and how they fit into the big picture.
2. **Discuss what security frameworks** you are leveraging and ensure they are still the best ones for you today.
3. **Review your internal policies** to ensure they align with those regulations with which you must comply.
4. **Review your vulnerability management program** and processes for remediation to ensure they are all-encompassing.
5. **Review automation tools** to ensure you have both reactive and proactive solutions and identify how they are helping you meet your shared goals.
6. **Consider other possible automation tools** that align the organization, reduce silo working, improve efficiency and harden security.
7. **Review your cloud services** and understand how compliance and security apply on those platforms.
8. **Review upcoming audits** that require preparation and decide if you want to perform an internal audit. If so, consider how automation tools help you be compliant and demonstrate it.



Puppet is here to help

We have innovative solutions that can help you continuously enforce compliance through automation so you can reduce risk, and fortify your security posture for years to come.

Learn more about Puppet Comply and watch a demo to see it in action.

Contact Puppet so we can help your organization automate IT compliance.