Scrut Automation

Best Practices and Expert Insights

Becoming Best-in-Class in Cloud Compliance

Scrut Automation

Contents

Introduction

Organizations are under constant pressure to adopt new technologies that will improve efficiency and competitiveness.

However, with the adoption of new technology comes new risks.

One of the biggest risks facing organizations today is the loss of control over their data. When data is stored in the cloud, it is stored on servers that are outside of the organization's control. This can lead to compliance issues if the data is not properly secured.

Did you know?

As Foundry (formerly IDG Communications) said in their 2022 Cloud Computing Study executive summary, "As in every aspect of the business, security remains top of mind when investing in cloud solutions. The number one business driver for cloud computing is to enable disaster recovery and business continuity, while data privacy and security challenges are one of the top obstacles to [implementing] a cloud strategy."

Achieving cloud compliance requires a multi-faceted approach that includes people, processes, and technology.

People are the foundation of any compliance effort, as you need the right people in place to set the tone for the organization and drive the compliance effort forward.

Processes must be established and followed to ensure compliance with applicable regulations.

Technology must be leveraged to automate compliance-related tasks and to monitor compliance status.

Organizations must adopt an approach to cloud compliance that includes risk assessment, risk management, and the implementation of best practices to manage and mitigate risk.

By taking a holistic and comprehensive approach, your organization can become best-in-class cloud compliant.

The Cloud Compliance Landscape

The Need for Cloud Compliance

Businesses are **increasingly turning to cloud-based solutions** to improve efficiency and cut costs, especially since the advent of the COVID-19 pandemic and the substantial shift of the workforce from office-based to home-based.

This transition was often done hastily, as companies scrambled to maintain operations while complying with COVID protocols.

For many organizations, their focus was on establishing new or sometimes all but completely transforming their standard business operations in order to accommodate a newly-remote workforce, and this transition often failed to account for diligent compliance with data security standards.

As a result, the **sudden shift to a remote workforce** and subsequent **rapid adoption of cloud technology** also introduced **new compliance risks.**

What Are the Compliance Risks Associated with the Cloud?

There are a number of compliance risks associated with the cloud, but the most significant are:

Data security:
Confidential or sensitive data stored on the cloud, vulnerable to attack

Data corruption:
Introduction of malware, ransomware etc., into the cloud computing system

Data Privacy:
Personal data stored or processed in the cloud, potentially accessible by unauthorized parties

Data security concerns arise when confidential or sensitive data is stored or processed in the cloud, as this data is more vulnerable to attack by cyber criminals than data on a hard drive not connected to a network or online entry point. The criminals may be after personal customer data with which to perpetuate identity theft, blackmail, or extortion. They may also seek financial data such as credit card information.

Data corruption, i.e. data loss, can occur as part of the abovementioned attacks if malware, ransomware, or other malicious viruses are introduced into the cloud computing system by nefarious agents. According to a recent International Data Corporation (IDC) report,

Did you know?

"79% of organizations have activated a disaster recovery response within the past 12 months, with 61% of these incidents triggered by ransomware or other malware." Of these organizations, 83% experienced at least one incident of data corruption as a result.

Data privacy concerns arise when personal data is stored or processed in the cloud, as this data may be subject to access by unauthorized parties and used without the owner's consent or knowledge. This can lead to a loss of privacy for the individual, or even identity theft.

Businesses and individuals must adhere to certain laws and regulations to ensure that their use of cloud based technologies like web hosting and cloud storage is secure, and thus legally compliant. Compliance with data privacy laws may depend on the location of the cloud provider and the storage of data.

It's crucial for information security professionals to not only know the applicable regulations for every jurisdiction in which they do business, but to also know the **difference between data security laws and data security compliance standards.**

These laws and standards govern the way data is stored and accessed in the cloud, and help to ensure that only authorized individuals have access to sensitive information. The two terms are often used interchangeably, but they carry different consequences if violated.

Laws vs. Standards

Laws	Standards
Definition	
These are rules of the land, generally enforced by local authorities or governing bodies.	These are a collection of guidelines put together to provide direction on building a solid information security posture
Adherence	
Adherence is mandatory to these laws and is enforceable by the governing bodies.	Adherence is not mandatory and is not enforced by any governing body.
Repercussions	
The repercussions can vary depending on the degree of non-adherence and often include hefty fines, dismissal of licenses, etc.	Compliance is often used as a lever to build trust with customers, and non-compliance can lead to loss of revenue.
Scope	
The laws to date have been mostly focused on Data Privacy.	The standards cover a variety of areas (some mandatory, some optional), including security, confidentiality, integrity, availability, and privacy.
Examples	
Some examples include GDPR, CCPA, PDPA, HIPAA, etc.	Some examples include SOC 2, ISO 27001, NIST, etc.

Laws vs. Standards

Laws

Some of these are laws that are enforced by the government of a particular country. Two of the most well known are the EU General Data Protection Regulation (GDPR) and the US Health Insurance Portability and Accountability Act (HIPAA).

You can read more about the similarities and differences between the two laws in this article, but to summarize:

The GDPR requires businesses to take steps to protect EU user data from accidental or unauthorized access, destruction, alteration, or unauthorized use. Businesses must also ensure that data is quality controlled to protect against unauthorized access, alteration, or destruction.
The regulation applies to any type of data, including personal data, processing activities, and storage.

HIPAA is a US federal law that imposes similar regulations on any health or medical data stored by any organization in the healthcare or medical field. It applies to all healthcare providers, including hospitals, clinics, and insurance companies.

The law requires healthcare providers to take measures to protect the privacy of patients' health information, and to ensure the security of that information. HIPAA also gives patients the right to access their own health information and to control how that information is used and shared.

Many other countries have laws relating to digital privacy. Argentina has the 2000 PDPA (Personal Data Protection Act), Australia has the Privacy Act of 1988, Mexico has the 2010 Federal Law on the Protection of Personal Data Held by Private Parties, and so on.

If your company stores data on a physical server located in any of these locations, it is subject to those laws.

Laws vs. Standards

Standards

There are a number of different data security standards that have been developed by various organizations, such as the Cloud Security Alliance (CSA), the International Organization for Standardization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE).

Each of these compliance standards has different requirements, so it's important to know which one applies to your situation.

The compliance standards that apply largely depend on the type of data you are storing in the cloud. For example, if you are storing credit card data, you will need to comply with the Payment Card Industry Data Security Standard (PCI DSS).

Ultimately, compliance with cloud data standards can help to improve the overall quality and usefulness of your data.

Failure to comply with laws can result in significant fines and penalties, loss of business licenses, and even criminal charges if the negligence of the law is particularly outrageous. In addition, companies may be required by law to provide customers with notice of any data breaches that occur, in addition to costly remediation measures such as identity protection, which can lead to reputation damage and financial strain.

Failure to comply with data security standards may not lead to legal consequences, but they can lead to loss of reputation and business when vendors, suppliers, customers, clients, etc. discover that their personal data or that of their customers has been stolen or destroyed.

The Dangers of Poor Cloud Compliance

Unfortunately, not all businesses take cloud compliance seriously. This can lead to a number of dangerous consequences, including data breaches, data loss, and regulatory fines.

Common Issues Discovered after Risk Assessments

Some of the most common issues discovered after a cloud security risk assessment include:

By making the necessary changes to mitigate these risks, organizations can improve their overall security posture and better protect their data in order to avoid severe problems, not the least of which is public embarrassment and poor publicity.

Examples of Poor Cloud Compliance Leading to Serious Problems

There are numerous public examples of when poor cloud compliance has caused serious issues for a business.

1. Colonial Pipeline

The Colonial Pipeline ransomware attack was a cyberattack that took place on May 7, 2021, on the Colonial Pipeline system. The attackers used the ransomware strain known as DarkSide to encrypt the system's files and demand a ransom payment in order to decrypt them.

The attack caused a shutdown of the pipeline, which supplies fuel to the East Coast of the United States. The attack caused massive gas shortages and was also viewed as a national security concern, leading the president to declare a national emergency.

The Colonial Pipeline Company paid the $4.4 million ransom and the system was restored on May 12. The FBI did eventually recover roughly half of the ransom about a month later, but that was still a loss of approximately $2 million in addition to the massive costs incurred due to loss of business operations.

The cause of the breach? A reused VPN password. That’s a common and, in this case, a very expensive mistake, one that could have been avoided by utilizing stricter authentication procedures.

2. Lakeview Loan Servicing

In March of 2022, Lakeview Loan Servicing notified customers that it had suffered a data breach. The breach affected over 700,000 people, and resulted in the exposure of sensitive information such as Social Security numbers and bank account information.

Allegedly, the breach occurred October-December 2021, but Lakeview didn't take steps to ascertain what data had been stolen until January 2022, and didn't alert customers until several months after that.

The breach has caused many customers to lose trust in the company, and has resulted in financial hardship for some. Lakeview has been facing a class action lawsuit since the breach was made public, and the case is still ongoing.

3. Beetle Eye

In mid-2021, cybersecurity researchers discovered that an Amazon Web Services (AWS) cloud bucket belonging to marketing firm Beetle Eye was misconfigured and had no password protection or data encryption, compromising the data of over 7 million people.

Without proper data security and encryption, sensitive information was at risk of being compromised. Per the researchers who discovered the lapse, "...Beetle Eye could be subject to sanctions from the U.S. Federal Trade Commission if they have mishandled consumer data. [...] Under Section 5 of the FTC Act, the maximum fine for mishandling US consumers' data is $100 million with the potential arrest of guilty individuals."

The researchers state that Beetle Eye acted immediately to resolve the issue and secure the data, but it's not known how the lapse initially occurred.

Challenges Faced by Startups and Mid-Size Companies in Achieving Cloud Compliance

In the above examples, Colonial Pipeline and Lakeview Loan Servicing were both large businesses, with annual revenues of $500 million and $60 million, respectively, but Beetle Eye was much smaller, with an estimated annual revenue of less than $5 million.

In their particular case, there are several reasons why they may have struggled with implementing appropriate data security protocols.

1. Budget

One of the biggest challenges is the cost of compliance. **Compliance can be costly**, and many startups and mid-size companies aren't able to or are unwilling to invest in compliance costs. For those that do, the cost of cloud services, including data security measures, constitute a large portion of their budget.

Did you know?

According to Flexera's 2022 State of the Cloud report, "53 percent of [small businesses] spend more than $1.2 million—up from 38 percent last year."

2. Lack of Expertise

Another challenge is the lack of expertise, which relates to the issue of cost. Startups and mid-size companies often don't have the resources to dedicate to compliance. They may have a small IT staff and lack the expertise to properly configure their systems for compliance.

With new regulations and standards constantly being introduced, it can be difficult for startups and mid-size companies to keep up if they don't have a department or even an employee dedicated to that purpose.

However, it cannot be overstated how critical cloud compliance is for any business that wants to operate in the cloud. The cost of a cyber attack is estimated to be approximately $200,000, a figure that can bankrupt many small businesses.

The best way to ensure compliance with cloud security standards is to educate yourself and your employees on the importance of following best practices, and by taking a holistic and comprehensive approach to cloud compliance. In the next sections, we'll go over those best practices and how you can implement them.

Best Practices for Cloud Compliance

When it comes to compliance, there is no one-size-fits-all solution. Every organization has different compliance needs based on its size, industry, location, complexity of its application and infrastructure landscape, and operational processes.

As a result, it's important for each organization to establish a baseline understanding of compliance, and then define compliance in a way that makes sense for them.

Defining What Compliance Means for Your Organization

Simply put, compliance programs are designed to help organizations identify, manage and control risks. By understanding the purpose of compliance, mid-level organizations can develop more effective compliance programs that protect their business and reputation.

There are two elements that should be included in any compliance definition; namely, the purpose of compliance and the goals of compliance.

Purpose of Compliance

For mid-level organizations and small businesses, for example, compliance provides a framework for best practices and ensures that the organization is adhering to all relevant laws and regulations. Compliance also helps to protect the organization from potential legal liability and reputational damage.

Compliance must be aligned with the organization's business goals and embedded into the organization's culture. By establishing and maintaining effective compliance programs, mid-level organizations

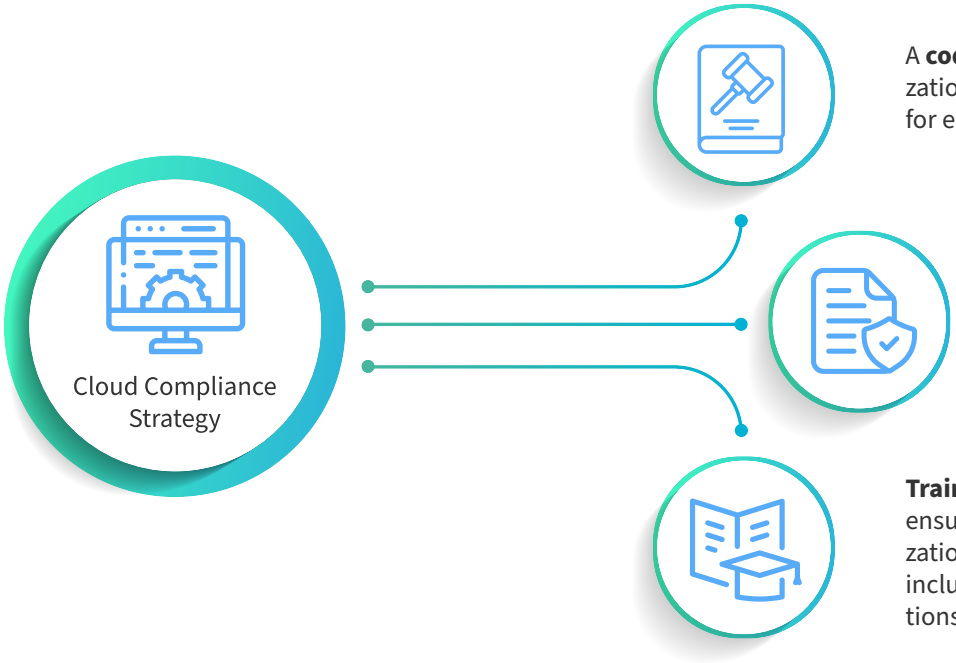
Goals of Compliance

The goals of a compliance program are to ensure that an organization is adhering to all applicable laws and regulations, and to prevent and detect criminal and unethical behavior.

An effective compliance program will take into account the specific risks faced by an organization and put in place controls to mitigate those risks. For example, a healthcare organization will have different compliance risks, and therefore different compliance goals, than a financial institution.
and small businesses can safeguard their operations and ensure that they are meeting their obligations to employees, shareholders (if applicable), and their customers/clients.

As such, their compliance program will be tailored to address those specific risks. It will set forth realistic and attainable compliance goals regarding data security practices, and will be reviewed and updated on a regular basis.

There are three important aspects to compliance strategy that should be considered when preparing logical and coherent cloud compliance goals for your organization:



A **code of conduct** that sets out the organization's ethical standards and expectations for employees;

Compliance policies and procedures that explain the requirements of the law and the organization's procedures for complying with them;

Training and education programs that ensure employees are aware of the organization's code of conduct and compliance, including the process for reporting violations.

Defining Your Cloud Compliance Strategy

Once you understand the purpose of compliance and have established your compliance goals, it's time to figure out exactly how you will meet those goals.

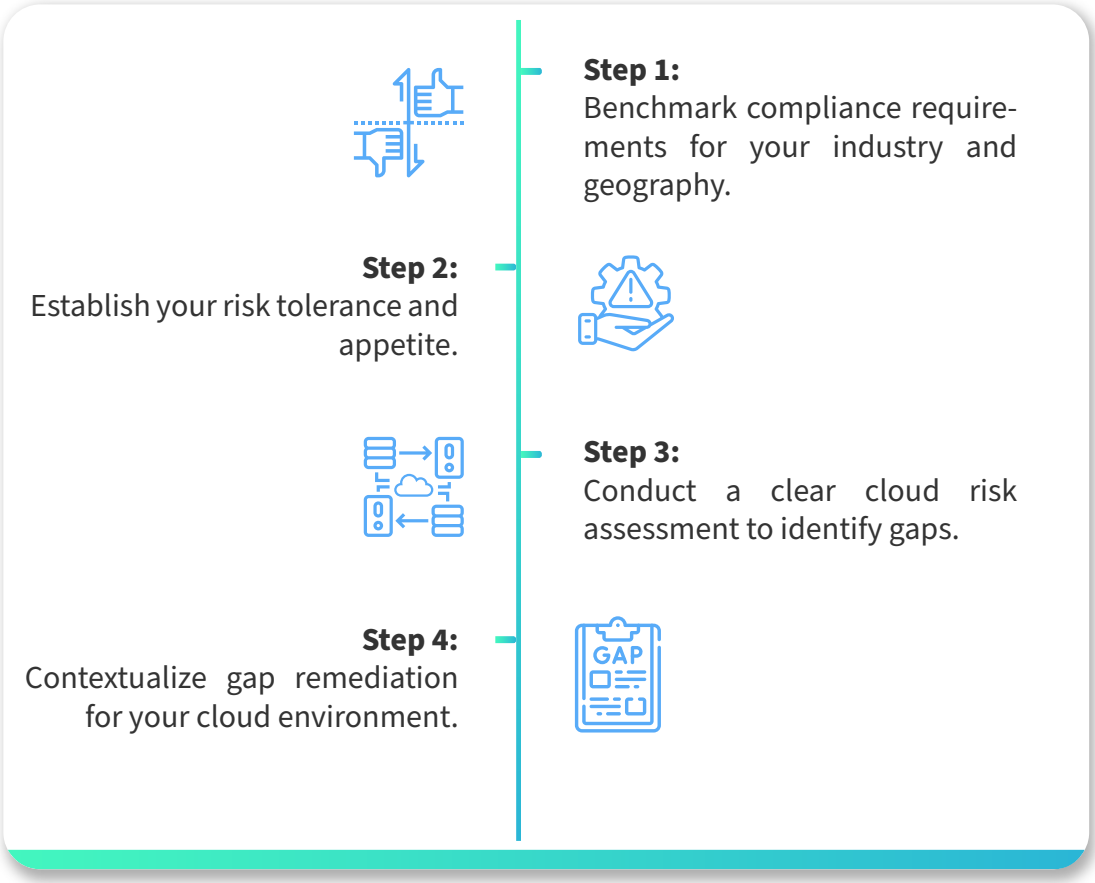
This process can seem daunting, but there are a few steps that organizations can take to ensure they are meeting all of their compliance obligations.

How Do You Know What Policies and Procedures to Put into Place?

If you're responsible for ensuring your company's compliance with cloud computing regulations, you may be wondering what policies and procedures you need to put into place.

The answer depends on the specific regulations that apply to your industry, as well as the cloud services you're using.

However, there are some general guidelines you can follow to make sure you're covering all your bases.



First, take a look at the compliance requirements for your industry. If you're not sure where to find this information, your cloud provider should be able to point you in the right direction.

You can also contact a business that specializes in helping other companies easily and affordably achieve and maintain cloud compliance through automation procedures, such as Scrut Automation.

Once you know what regulations you need to comply with, you can start putting together your policies and procedures.

Second, your organization's tolerance for risk should be considered when determining which cloud compliance policies and procedures to put into place. The amount of risk your organization is willing to take on will dictate the level of compliance required.

For example, if your organization is willing to take on more risk, you may not need to implement as many compliance policies and procedures. However, if your organization is not willing to take on much risk, you will need to put into place more compliance policies and procedures.

The best way to determine your organization's tolerance for risk is to consult with your legal team and/or your compliance officer (if applicable). They will be able to advise you on the level of compliance required based on your organization's risk tolerance.

Third, your level of cloud compliance as well as the regulations that apply to your cloud environment are dependent upon which type of cloud environment you use. Will you be utilizing a public cloud system, a private and proprietary system, or a hybrid?

Public Cloud Security vs Private Cloud Security Risks and Benefits

Security is always a primary concern when it comes to cloud computing. When deciding between public and private cloud options, it is important to consider the security risks and benefits of each.

Public cloud security risks include data breaches, malicious insiders, and account hijacking. However, the benefits of public cloud security include economies of scale, increased security features, and improved security compliance.

Private cloud security risks include data leakage, unauthorized access, and loss of control. However, the benefits of private cloud security include increased control, improved security, and reduced costs.

Public Cloud Security

The public cloud is a shared environment, meaning that cloud security is a shared responsibility between the cloud provider and the customer.

Did you know?

Three of the most well-known public cloud computing providers are:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

There are a number of advantages that public cloud security has over private cloud security risks and benefits. One advantage is that public clouds are **generally more scalable** than private clouds, meaning that they can **more easily handle large workloads and spikes in traffic.**

Additionally, public clouds typically offer better uptime and availability than private clouds, meaning that your data and applications will be more accessible when you need them.

With a public cloud, you benefit from the economies of scale and the expertise of the cloud provider. The provider is responsible for the security of the infrastructure and you can take advantage of their security controls and procedures.

They tend to have more robust security features than private clouds, including advanced firewalls and intrusion detection/prevention systems.

The main security risks of these public clouds are data breaches and loss of data due to malicious activity. Since they are more well-known and public-facing, they sometimes present an irresistible target to cyber criminals. These risks can be mitigated by using strong security controls and ensuring that data is encrypted at rest and in transit.

One disadvantage is that public clouds are often less secure than private clouds because they are shared among many users. This means that if one user has weak passwords or fails to use two-factor authentication, all users are at risk, and the only users you can monitor are the ones in your employ.

Another disadvantage is that public clouds are often less reliable than private clouds because control is in the hands of a third-party. This means that if public clouds experience outages and downtime, there is little a company can do other than wait for services to be restored, and try to mitigate any business problems in the meantime.

Finally, public clouds can be more expensive than private clouds because they require more infrastructure and resources to maintain, but this can vary depending on numerous factors such as size, bandwidth, and number of users.

Private Cloud Security

Private cloud security offers many benefits over public cloud security, including increased oversight over data security, compliance, and privacy. They are single-tenant environments where the customer has **complete control over access, policies and procedures, and necessary maintenance and repair.**

Private clouds also offer **greater flexibility and customization**, which can be critical for businesses with specific security needs.

However, private clouds can also be more expensive and require more expertise to manage. With a private cloud, you are responsible for the security of the infrastructure and must maintain your own security controls and procedures, as well as provide a physical location for equipment as well as both hardware and software upgrades. This can be costly and time-consuming.

Private clouds also can be less secure than public clouds, as the strength of their security is largely dependent on the budget and compliance knowledge of the company.

Compliance may be harder to prove to vendors, customers, or regulatory agencies; many risk assess-

ments are easier to complete if the company is using a public cloud service, as many of the answers are provided by the public cloud provider. A risk assessment is a much more involved process when analyzing a private cloud environment.

Ultimately, **the decision comes down to a balance of security and convenience**. The public cloud is more convenient and, depending on the number of users, can be more cost-effective; however, the private cloud is often secure and offers more control.

Regardless of which platform you choose, it's important to implement a sound cloud security strategy that is tailored to the specific needs and functions of your organization.

Implementing a Cloud Compliance Framework

There are a number of different cloud compliance frameworks that must be considered when developing data security policies, and it can be difficult to ensure that all of the necessary requirements are met.

However, by taking the time to align data security policies with the appropriate cloud compliance frameworks, organizations can be confident that their data is well-protected.

When it comes to cloud compliance, conducting a risk analysis is a critical first step. This will help you identify what policies and procedures need to be put into place in order to keep your data safe and compliant.

There are a number of factors to consider when conducting a risk analysis, such as the type of data you are storing in the cloud, where it is located, and who has access to it.

By taking the time to assess the risks associated with your cloud data, you can ensure that you have the right policies and procedures in place to keep it safe and compliant.

Work with a cloud compliance expert to help conduct a risk assessment and develop your data security policy. They can identify the specific gaps in your security, and ensure that your policies meet all of the requirements of your specific cloud compliance framework.

Familiarize yourself on the different compliance frameworks and what they entail. This will help you understand what needs to be included in your data security policy, and what procedures should be in place in order to align with the framework.

Stay up-to-date on changes to the compliance framework. As the framework evolves, so too should your data security policy and procedures. Technology is moving at a rapid pace, and new cybersecurity measures are being developed almost daily.

Aligning Data Security Policies with Cloud Compliance Frameworks

Administration

The administration of the cloud compliance framework is essential to the security of data. Without proper administration, the framework would be ineffective and could lead to data breaches.

The cloud compliance framework must be administered by a team of experts who understand the risks and controls associated with data security. The team must be able to identify and mitigate risks in order to protect data.

A poorly designed or implemented cloud compliance framework can create serious risks for an organization. To ensure that a cloud compliance framework is effective, it is important to involve all relevant stakeholders in the design and implementation process.

Upkeep

Upkeep of a cloud compliance framework is important to ensure data security. Regular updates to the framework help to keep security posture strong and improve detection and response to threats.

Upkeep includes regular maintenance of both hardware and software, both of your cloud environment (if applicable) and the physical devices used to access the cloud. Security patches should be checked for and installed regularly, ideally daily.

Additionally, regular review of access control lists, user activity logs, and other data can help to identify potential security issues and ensure that the cloud environment is secure.

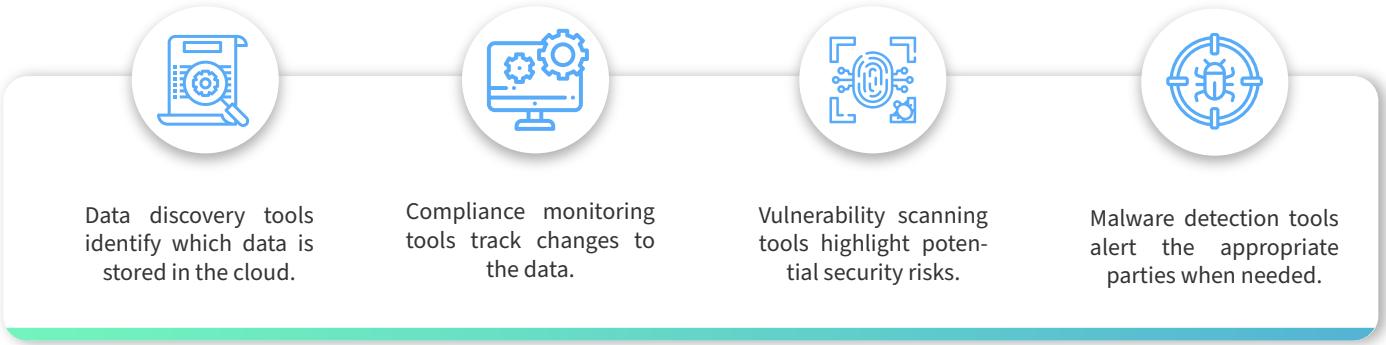
Monitoring

Organizations should monitor their cloud environment on a regular basis to ensure that data is protected and that any potential compliance issues are identified and addressed. Monitoring should take place 24 hours a day, seven days a week, 365 days a year.

Cyber criminals will take advantage of times they perceive security may be lax – for example, weekends and holidays – so every anomaly, no matter how small, should be carefully logged.

There should also be a process in place for quickly and efficiently responding to any compliance issues or security threats that are identified.

One way to ensure adequate monitoring is the use of various tools available for this purpose. For example:



Reporting

Monitoring for threats won't do much if you don't follow up by reporting any issues to the appropriate party. That could be the company's IT team, the cloud service administrator, the CISO, or even the CEO.

Depending on the severity of the issue, you may need to contact your local law enforcement, the Federal Bureau of Investigation (FBI), or the United States Secret Service (USSS). In some cases, you may also need to contact your state's attorney general or consumer protection office.

If you are unsure who to contact, you can always start by contacting your local law enforcement. They will be able to help you determine if the issue is serious enough to warrant contacting the FBI or USSS. Remember, it is always better to err on the side of caution when it comes to data security issues.

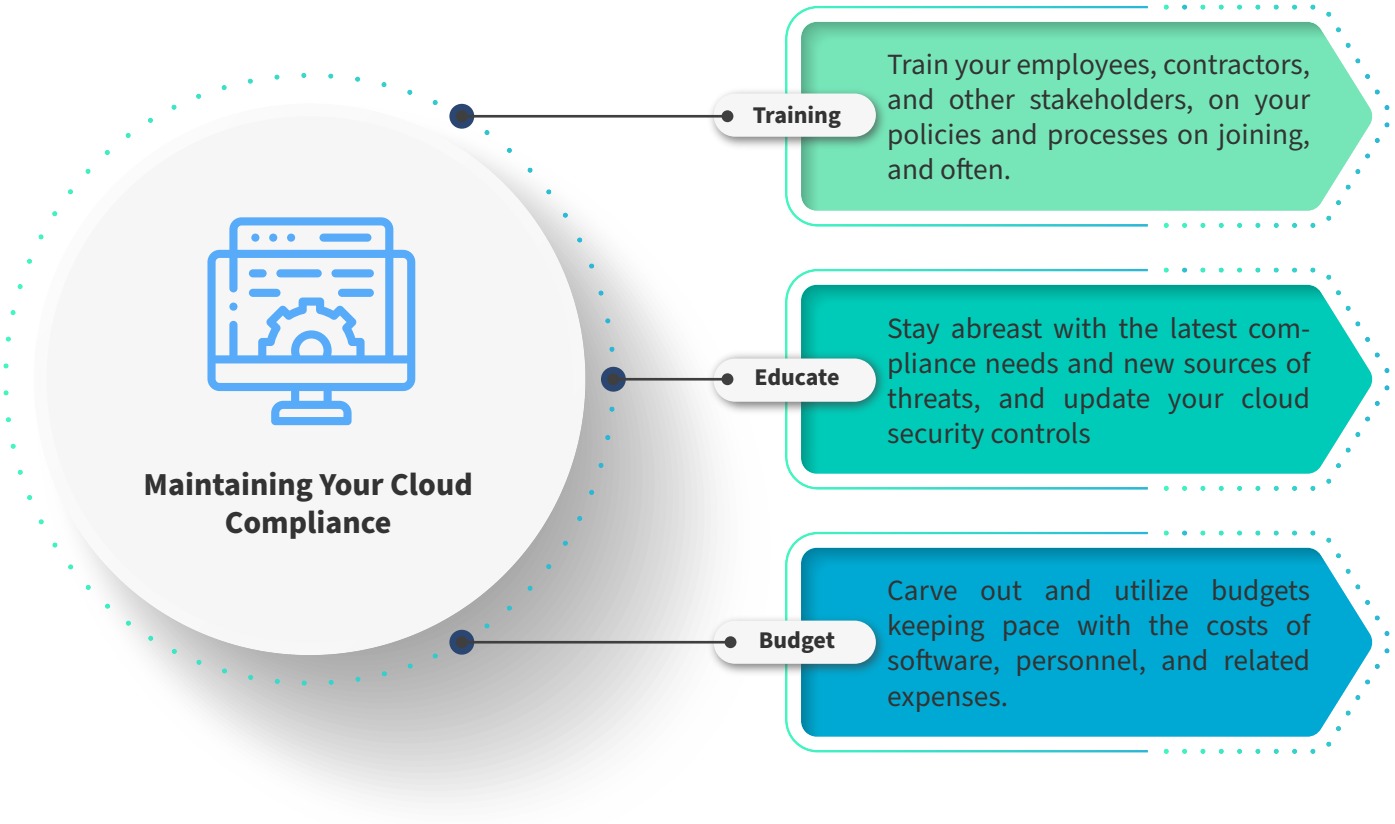
Some of the things that should be included in a report on a data security issue include:

- A description of the issue
- The date and time that the issue occurred
- The location of the issue
- The names of any individuals who were involved in the issue
- The name of the person or organization who reported the issue
- A contact number for the person or organization who reported the issue
- Any other relevant information that could help to identify and resolve the issue.

By now, you should have a pretty good understanding of how to manage your cloud compliance framework. Just remember to keep your monitoring tools up to date, set up alerts for when changes are made to your compliance framework, and document everything so you can easily refer back to it later.

With these tips in mind, you should be well on your way to keeping your cloud compliance framework in check.

Maintaining Your Cloud Compliance



Cloud compliance is a daunting task for any organization. There are many moving parts and it can be difficult to keep up with the ever-changing landscape. However, there are some key things you can do to help maintain your cloud compliance framework. Training and education are critical for keeping up with the latest changes. Budgeting for compliance can be a challenge, but it is important to ensure you have the resources you need.

Training

A chain is only so strong as its weakest link. If you neglect adequate training of your employees, the best cloud compliance framework in the world won't keep you compliant or your data safe.

Your staff should be aware of the compliance requirements for the cloud platform you are using. They should know how to access the compliance documentation and where to find the compliance controls.

Make sure that all new staff members receive training on the cloud compliance framework as part of their

onboarding process, and hold regular training sessions for all staff members on utilizing cloud compliance framework.

Institute procedures, both automated and manual, to ensure that employees are adhering to compliance protocols, especially identity and access management. Establish password management protocols so that strong passwords are always used and frequently changed. Enable two-factor authentication for all external access.

Keep the training materials for the cloud compliance framework up-to-date and easily accessible, so that staff members can reference them as needed.

By following these guidelines, you can be sure that all staff members are properly trained in the use of the cloud compliance framework, and that your organization can maintain its compliance posture

Education

It is important to educate yourself on the topic of cloud compliance in order to maintain a strong compliance framework.

First, be sure to stay up-to-date on the latest compliance requirements. The cloud compliance landscape is constantly changing, so it is important to keep abreast of the latest developments.

Second, take advantage of cloud compliance tools and services. They can be extremely helpful in ensuring compliance with the newest requirements.

Finally, make sure to develop and maintain strong policies and procedures. This will ensure that your organization is able to meet the compliance requirements in a consistent and effective manner.

Budget for Compliance

Compliance with regulatory requirements can be a costly endeavor, but it is important to make sure you have a budget in place to cover the costs associated with compliance, and that this budget keeps pace with the costs of equipment, software, personnel, and related expenses.

When cutting corners, compliance is not an area to reduce. If you perform comparison shopping in order to find a cloud provider or vendor that offers similar services for less cost, ensure that they provide the same or superior service as your current provider, and that they comply with your data security plan in all respects.

Working with your cloud provider and ensuring that they have the appropriate controls in place can help to minimize the cost of compliance while still maintaining a high level of security. In the end, spending a little bit more on data security can end up saving you millions, as Colonial Pipeline, Lakeview Loan Services, and Beetle Eye – as well as thousands of other organizations – can attest.

Conclusion

Acquiring best-in-class compliance in the cloud is not an easy task, but it is achievable with the right mindset and approach.

- Start by understanding the cloud and its unique compliance landscape.
- Build a solid foundation for your compliance program by implementing governance, risk management, and controls.
- And finally, continuously monitor your compliance posture and tune your program as needed.

By following best practices for cloud compliance, you can help ensure that your data is secure and your organization is compliant with regulations.

If you need help with your cloud compliance framework or procedures but don't know where to start, contact Scrut Automation. Our cloud security system, Scrut Octopus, is a unified cloud security solution that can detect and flag cloud misconfiguration and other issues before they snowball into a dire situation. We're happy to help in any way we can.