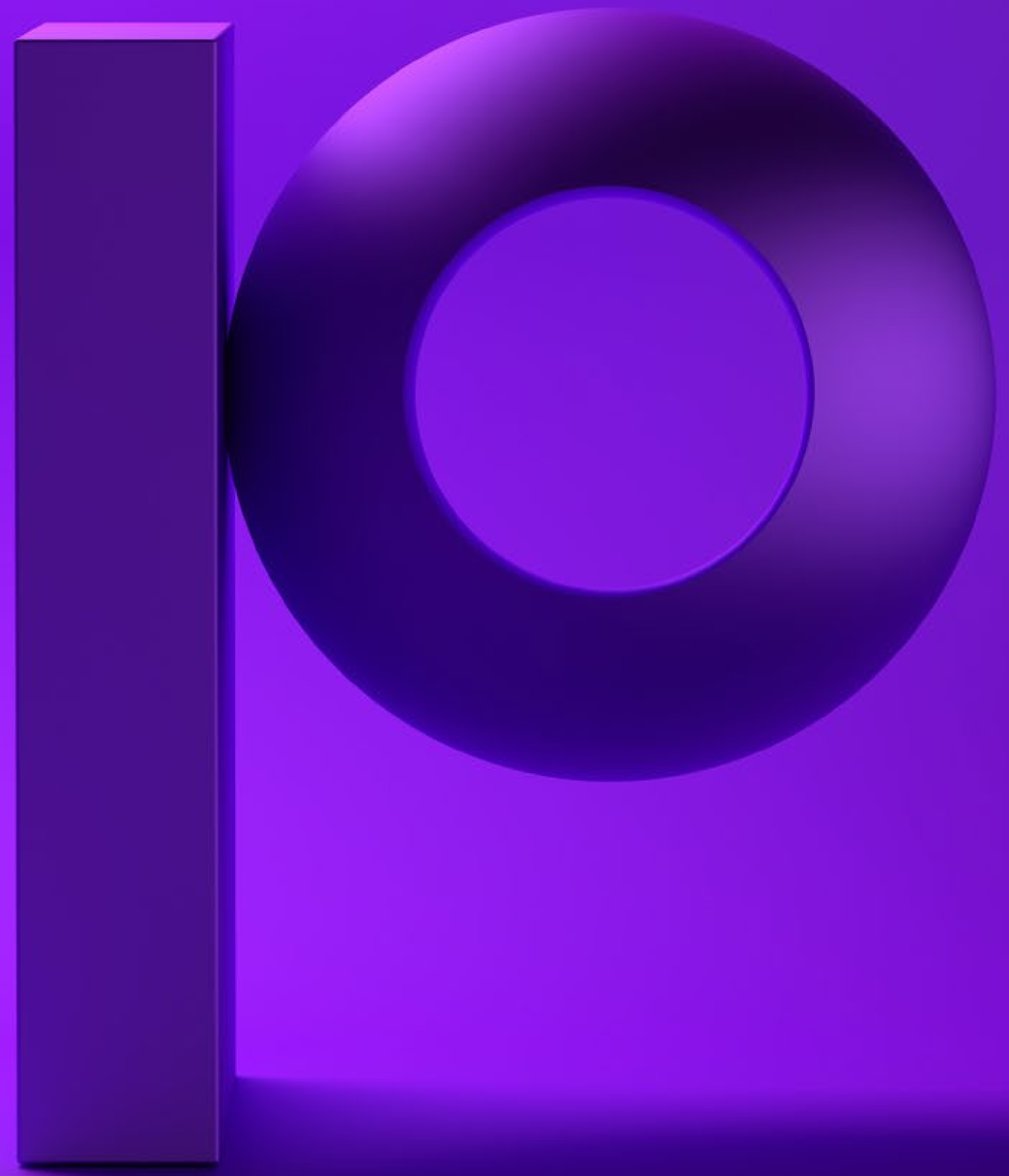
precisely

Secure Your IBM i Today to Meet Tomorrow's Compliance Challenges

New compliance regulations are coming your way. The time to prepare is now.



Introduction

Another massive breach is in the news. Another regulatory entity is rolling out new cybersecurity regulations. Another company executive is spending sleepless nights worrying about IT security vulnerabilities. Sound familiar? It's no wonder that security is the number one IT priority today, at least according to **a recent Precisely survey** of IT professionals at companies with IBM i environments who were asked about their top IT priorities.

Regulations are a big driver of this increased prioritization of security. When respondents to the same Precisely survey were asked to choose their biggest IT security challenges, their number two choice was "growing complexity of regulations." In addition to growing in complexity, regulations are multiplying. In 2018, GDPR was regularly in the news as it had companies across the globe scrambling to get their systems and processes prepared to meet the impending compliance deadlines. And the cost of doing so wasn't cheap. **A survey conducted in 2018** by the International Association of Privacy Professionals (IAPP) and Ernst & Young found that on average a company spent nearly $1.3 million (including salaries/benefits) to prepare for GDPR. Despite the money being spent, the same survey showed that 34% wouldn't even be ready to demonstrate compliance until 2019—more than six months past the deadline. And an astonishing 19% that said they may never be ready! Meanwhile, countries in the European Union are sending a strong message that companies need to step it up. The first GDPR fines are being levied, with the most notable coming from France, which recently hit Google with a fine of 50 million euros (Google is currently contesting the ruling).

Another strong new cybersecurity law that went into effect during 2018 was New York State's 23 NYCRR 500 regulation that affects most financial services companies operating in the state. Now other states are talking about following suit. The California Consumer Privacy Act goes into effect on January 1, 2020, and will compel most companies that do business with California residents to protect sensitive consumer data in ways that are similar to GDPR. On top of this, there is increasing talk in Washington, D.C., of possible legislation at the national level to address data protection and privacy concerns.

It's important to remember that complying with regulations doesn't equate to rock-solid security since regulations don't always focus on all of the layers of security required for total confidence; however, a strong security program that addresses all aspects of security definitely supports compliance. Bottom line: your company can no longer be complacent about IT security. Strong regulations will, one way or another, affect your company and the way your systems are secured. If you're not doing so already, it's critical to start making efforts now to get prepared for this eventuality. To help, Precisely has created this ebook that outlines the key aspects of IBM i security that are typically required by regulations and the various approaches to addressing those needs.

IT Security Policies

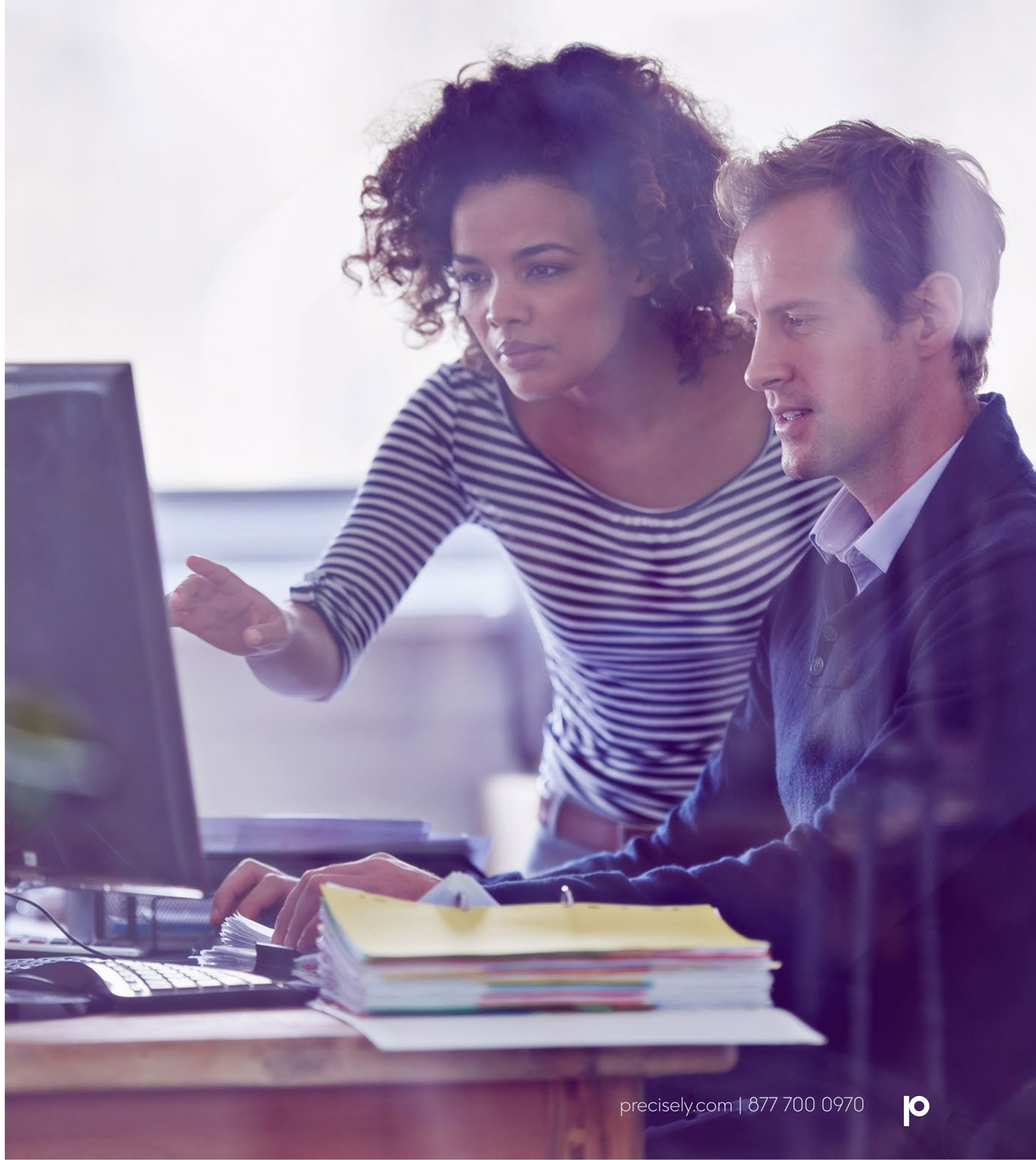
Numerous compliance regulations require companies to define and maintain clear IT security policies. Most notable of these regulations are Sarbanes-Oxley (SOX) and 23 NYCRR 500, which require that you specify how your IT systems are to be secured so as to reduce the risk of unauthorized system access and data breach, as well as the steps to take should a breach occur. Beyond regulations, however, best practices dictate that every company running IBM i should not only have well-defined, well-communicated IT security policies, but these should be based on a formal, documented IT security risk assessment that takes a methodical approach to finding IT vulnerabilities. We'll talk more about security risk assessments in the next section.

Sound IT security policies must address these key areas across all platforms, including IBM i:

- Physical security of data centers and IT equipment
- Network security
- Password strength and expiration
- Local and remote authentication controls
- Limits on powerful user authorities
- System, data, and command line access controls
- Privacy for data at rest and in motion
- Monitoring of how data is changed or viewed
- Logging of changes to system settings or data
- Mobile-device security
- Frequency and depth of security risk assessments
- Procedures and reporting responsibilities in the event of a breach (incident-response plan)

Monitoring for Deviations from Policies and Compliance Requirements

Third-party solutions are available that help IBM i administrators and security officers compare system and object configurations to the policies their organization has defined for achieving security and regulatory compliance. These solutions can be very helpful as you workto ensure your system configurations align with the requirements of various regulations. In other words, if you were to manually compare configurations to policies, it would be an extremely time-consuming process since there are often hundreds if not thousands of objects and configuration settings within a typical system. When properly configured, the customizable templates these solutions provide can also be used to generate alerts that go to key people should any deviation from policies occur. But templates are just the start. Comprehensive monitoring and auditing of the IBM i system audit journal and other logs and queues is also essential to achieve robust security and maintain compliance. More about this in the Security Auditing and Reporting section.



Security Risk Assessment

Compliance regulations such as PCI DSS, HIPAA, 23 NYCRR 500, and others require periodic risk assessments to proactively seek out and address security vulnerabilities. IT environments are not static and neither are threats. Without conducting periodic security risk assessments that closely examine systems, networks, and peripherals, the odds of a damaging breach increase substantially. Regulations may require that risk assessments also include penetration tests that attempt to breach your system defenses.

Some regulations also require a "separation of duties" when formal risk assessments are conducted. This means that the party assessing the system cannot be the same party that's responsible for managing the system. Typically, this means hiring a risk-assessment expert from outside of the company whose sole focus is to stay up to date on IT vulnerabilities and the evolving nature of external threats. Of course, when assessing IBM i for security risks, it's important to choose an outside entity that understands the unique characteristics of the platform.

As mentioned earlier, it is prudent for any comprehensive IBM i security program to include risk assessments, regardless of regulations. For IBM i, there are third-party tools that can give you a head start with your assessments as they are typically designed to compare the system configurations of your IBM i with known security best practices and produce reports containing actionable information.

Access Control

The cybersecurity requirements of compliance regulations are largely written to compel companies to put technologies and processes in place that keep unauthorized users out of systems while maintaining tight control over what authorized users are able to do once logged in. Within IBM i environments, comprehensive access control requires three defensive strategies:

Controlling User Authentication

Weak passwords and dormant user profiles create a significant security vulnerability that is easily resolvable by implementing strong password policies and closely managing profiles. To further strengthen login access, a growing number of companies are implementing multi-factor authentication (MFA). In turn, an increasing number of compliance regulations, such as PCI DSS, 23 NYCRR 500, HIPAA, and others, are adding multi-factor requirements for specific roles or situations. In essence, MFA requires users to provide one or more identifying factors, beyond their normal username and password, before access is granted. However, MFA is not only used to control login access to systems. The technology can also be used to control access to specific dzzatabases, commands, and even individual files. To learn more about MFA, read the Precisely white paper Multi-Factor Authentication for IBM i.

Controlling Powerful Authorities

It is one thing to prevent unauthorized users from accessing systems, but it's another to control what authorized users are able to access and execute once they log in. Many compliance regulations require tight controls on users to ensure they only have the ability to perform tasks on the system that align with their job description.

Broad use of powerful profiles quickly raises red flags with compliance auditors. Unfortunately, on IBM i it's all too common for rank-and-file users to have profiles that provide a very high level of authority. These include dangerous capabilities such as *ALLOBJ, *SECADM, *JOBCTL, and others. Certainly, there are times when a user legitimately needs a high level of authority to complete necessary tasks, but rather than giving carte blanche access, the safer approach is to grant the needed authority on a temporary basis and within narrowly defined parameters. Third-party elevated authority management tools simplify granting and revoking temporary authorities while tracking the actions of users in possession of an elevated authority.

Controlling System, Command, and Database Access

Years ago, simply managing object-level security might have been sufficient to control object access on IBM i, but today, given the manyways a typical system is connected to internal and external networks, far more is required. First there are the many system-access points via network protocols that must be secured, including FTP, ODBC, JDBC, OLE DB, DDM, DRDA, NetServer, etc. Then there are the many ways that databases can be accessed using open-source protocols, such as JSON, Node.js, Python, Ruby, etc. On top of this, there are multiple ways in which commands and data files can be accessed that bypass traditional object-level security.

The solution to securing all of these access points is to implement comprehensive, rules-based exit programs that tightly control a wide variety of access points, yet do so in nuanced ways. Exit programs can require a great deal of work to implement and manage, but fortunately, third-party solutions exist that streamline the tasks of creating, deploying, and managing exit programs while also providing the ability to trigger alerts should suspicious activity be detected.

Sensitive Data Protection

Personally identifiable information (PII), payment card information (PCI), and personal health information (PHI) are required to be encrypted by numerous regulations. These include PCI DSS, HIPAA, GDPR, GLBA/FFIEC, numerous state privacy laws, and others. Encryption technologies use one or more publicly available algorithms with a proprietary encryption key to transform human-readable data into non-readable ciphertext. Only permitted users who possess the proper encryption key can decrypt data. If a breach does occur and the data is properly encrypted, some regulations provide "safe harbor" protection from having to disclose the breach.

Encryption relies on the careful management of encryption keys to ensure data stays properly protected. If keys fall into the wrong hands, your encryption efforts are for naught, which is why several regulations such as PCI DSS, HIPAA, GLBA/FFEIC, and others also stipulate how encryption keys are to be managed.

For IBM i, various third-party solutions are available for encrypting data both "at rest" and "in motion." At-rest encryption applies to protecting sensitive database fields (such as credit card numbers) on disk drives and on backup media. In-motion encryption applies to protecting sensitive data as it's being sent across networks, whether as a data stream or as entire files. When sending files, third-party secure file transfer solutions are often used as they not only provide encryption, but also include numerous features that streamline and automate file-transfer processes.

Some companies are able to avoid encrypting sensitive data, yet still demonstrate compliance, through a technology called tokenization. The approach replaces sensitive data, say on a production server, with non-sensitive substitute values called "tokens." This effectively removes the production server from the scope of compliance because the relationship between the sensitive data and its replacement token is kept in a database on a separate server. PCI DSS regulations, for example, allow the use of tokenization for protecting credit card information.

Security Auditing and Reporting

Numerous compliance regulations, including SOX, PCI DSS, HIPAA, GDPR, and others, require some form of system activity logging, and as new regulations come along, it's a safe bet that many of these will also include a logging requirement. As mentioned earlier in this ebook, the regular monitoring of system and database audit logs is an essential, foundational security measure.

Monitoring System and Database Activity

In addition to QHST and system message queues, IBM i provides the powerful, unalterable journaling capabilities of the operating system. The combination of security-audit and data-object journaling makes it possible to log and trace a broad range of activities, including user authentication, system access, data changes, object configuration changes, and more. The downside of journaling is that its output is both voluminous and cryptic. That's why many IBM i shops utilize third-party solutions that simplify the processes of analyzing journals to identify specific events, trigger alerts when suspicious activity is detected, create reports for compliance auditors, and more. Keep in mind that many regulations require saving journals and other system logs for multiple years should they be required for an audit or investigation of some security event.

Monitoring Database-View Activity

Although journaling can log many different kinds of activities, some companies have especially sensitive data that requires security officers and managers to know if an unauthorized user accessed and viewed such data—regardless of whether the data was changed. Although journaling can't provide this information, technologies are available from third parties that make it possible to record these database-view activities, complete with "snapshots" of the precise data the user viewed.

Leveraging SIEM Solutions

For companies that utilize an enterprise-wide security information and event management (SIEM) solution, third-party tools are available that filter and format journal entries and other IBM i log data for integration with a SIEM. The sophisticated predictive-analytics capabilities of SIEM technologies make it easier for security officers to find patterns across multiple systems that may indicate suspicious activity or some other situation that could put a company out of compliance.

The Time to Prepare Is Now

Laws change, threats evolve, and no company can afford to be complacent when it comes to IT security and compliance. The only sensible path forward is to embrace a process of making continual improvements by regularly evaluating risk, hardening access, protecting confidential information, and monitoring activity. Of course, an additional challenge is striking the right balance between improving security, meeting your company's compliance requirements, making it possible for users to do their jobs, and managing the budget and other resources you have to work with. It's a lot to deal with, but what matters most is that you act now.

As a summary to this ebook, below is a brief checklist of key security activities that need to be on your radar:

- Compile and enact policies that reflect relevant compliance regulations and current IT security best practices.
- Map established policies to IBM i configurations so you can detect when settings change that could create exposures.
- Perform security risk assessments (at least annually) to find vulnerabilities. Use a trusted third party that understands IBM i security.
- Lock down access to IBM i by strengthening passwords (add multi-factor authentication where necessary), controlling the use of powerful profiles, and utilizing exit programs to manage access via network protocols, communication ports, open-source database protocols, and commands.
- Encrypt or tokenize particularly sensitive data, both at rest and in transit, so that data is rendered unreadable if a breach occurs.
- Implement comprehensive logging and monitoring to receive alerts of suspicious activity, to trace any activity that's in question, and to create necessary reports for auditors and managers.

Precisely Can Help

With proven security solutions and services for IBM i and a deep bench of experts, Precisely is here to help you strengthen IBM i security and comply with the regulations that impact your company. Our focus is to stay up to date on IBM i security vulnerabilities, best practices, and mitigation technologies.

Precisely Security Software for IBM i

Fortify your system-access security, file and field security, and monitoring and auditing processes with our best-in-class software solutions that cover:

- Model-based compliance management
- Compliance monitoring and reporting
- Security risk assessment
- Control of network access, open-source access, database access, and command access
- Encryption, tokenization, and anonymization
- Monitoring access to critical data
- Secure file transfer
- Elevated-authority management
- Multi-factor authentication
- SIEM integration

Precisely also offers solutions and services for AIX, Windows, and Linux that address security and compliance-auditing needs.

Precisely Professional Services for IBM i

Our security experts are here to assist your team in reinforcing IBM i security and meeting compliance requirements in numerous ways:

- **Security risk assessment** — We perform in-depth, periodic risk assessments on your IBM i environments and then, using our detailed findings as a guide, we sit down with your IT and compliance managers to help formulate and implement a plan for remediating discovered vulnerabilities.
- **Compliance/security audit assistance** — We assist your team during compliance or security audits by generating reports required by your auditors.
- **Managed-security services** — We assign your company dedicated IBM i security experts who, depending on the level of service chosen, regularly check security configurations, deliver status reports, monitor systems for security events, adjust security configurations, and more.
- **Security technology installation and training** — Ensure a successful implementation of your Precisely security technologies and receive all needed training.

To learn more about all of Precisely's security products and services, visit www.precisely.com.

precisely

About Precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely's data integration, data quality, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

www.precisely.com