SPANNING
A Kaseya COMPANY

EBOOK

# IT RISKS:

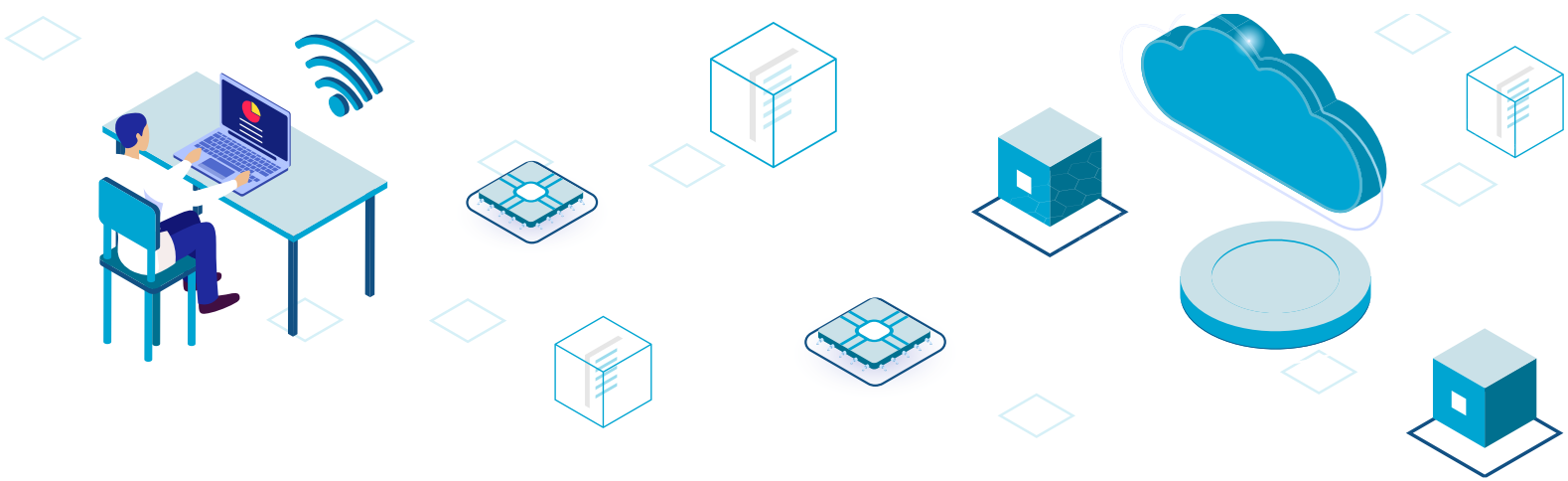
## BACKUP AND RECOVERY BLUEPRINT

# INTRODUCTION

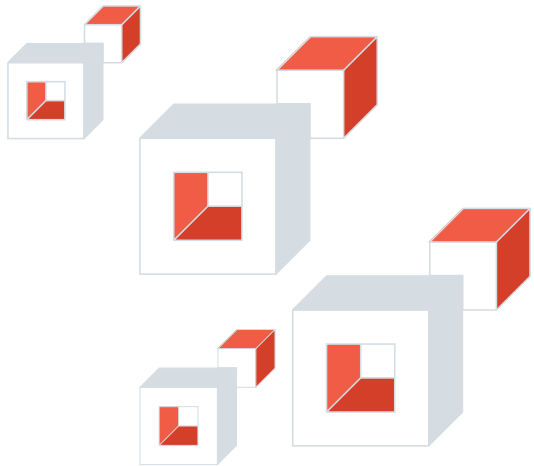
***Modern enterprises are reimagining the traditional work models and transitioning to the hybrid model — the workplace of the future — due to its many benefits. Both employers and employees are increasingly embracing this futuristic model.***

However, in the quest to address this growing hybrid workforce and fuel digital transformation, organizations have been undergoing radical changes, both from an IT and business perspective. For instance, organizations' data footprints are increasingly expanding beyond the conventional on-premise infrastructure to hybrid and multicloud environments. As a result, business-critical data now lives in more places than ever before, from on-premise data centers and multiple clouds to SaaS applications and remote endpoints. A widely dispersed workforce and data footprint also mean that businesses now heavily rely on their information and communication technology (ICT) infrastructure. With the advent of remote and cloud workloads, ICT systems have become the backbone of modern businesses that ensures collaboration and operational continuity.

While this transition offers many advantages, it's not all sunshine and roses for modern enterprises. As the amount of data created and stored across these multiple environments continues to grow, monitoring mission-critical data and its protection has become a Herculean task. More than 40% of cloud engineering and security professionals revealed that cloud-native services increase complexity and further complicate security efforts. The rapidly expanding data footprint and the growing reliance on new ICT systems — or cutting-edge technology — have introduced novel threat vectors and galvanized some others, which are waiting to leap at the opportunity to wreak havoc in your IT landscape.



The latest reports from the cybersecurity landscape underscore these growing risks. According to IBM Cost of a Data Breach Report 2024, the global average cost of a data breach surged to $4.88 million, marking a 10% increase from 2023 — the sharpest spike since the pandemic. This spike was primarily driven by the rising costs of business disruption and post-breach remediation activities such as regulatory fines and customer support. Another survey by Semperis reports that around 83% of businesses were victimized by ransomware in the past year. This ever-increasing and ever-evolving threat landscape can be a death knell for businesses if not tackled properly.



***The global average cost of a data breach surged to $4.88 million, marking a 10% increase from 2023 — the sharpest spike since the pandemic.***

Failure of ICT systems due to security issues, such as systems intrusion or malware infection, will impact business continuity because the critical functions that ensure business continuity are usually dependent upon ICT systems. So, how can modern organizations protect their business-critical data and ICT systems from these rising security threats and keep them readily available? Organizations must weave together plans to create a holistic strategy, which includes:

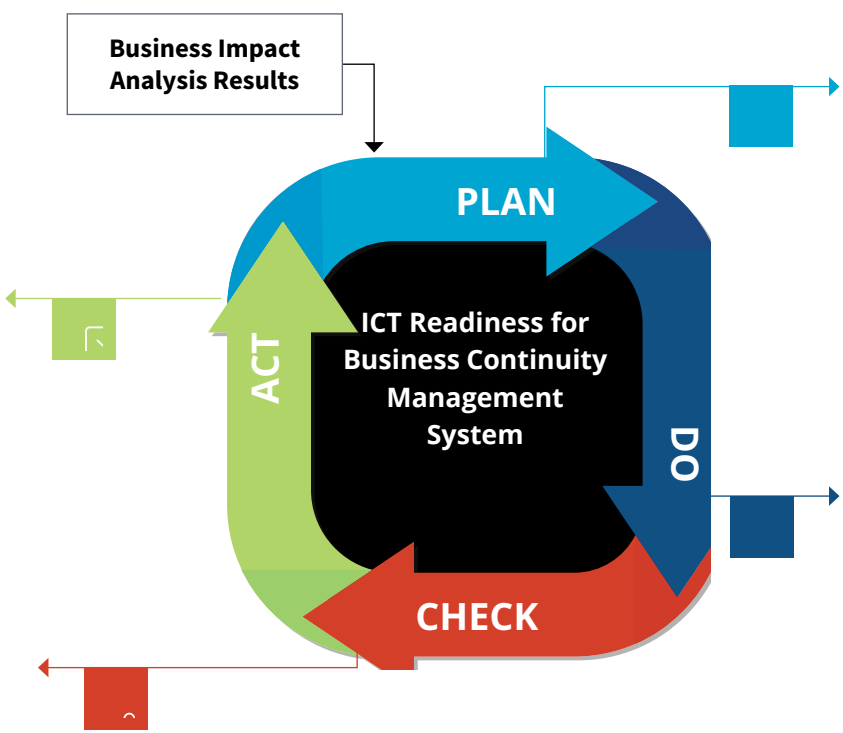
- **A risk mitigation plan that reduces the impact of potential security risks.**
- **An incident response plan that gives clear guidance on what to do during an adverse incident.**
- **A business continuity plan that details how operations will be maintained during the event.**
- **A disaster recovery plan that restores operations to normalcy after the disaster.**

This eBook aims to describe in detail how organizations can develop a comprehensive approach and achieve ICT Readiness for Business Continuity (IRBC) so that they continue to operate and meet their business objectives during times of disruptions. IRBC defines the capability of an organization to continue its business operations by preventing, detecting and responding to disruption of ICT services.

Aligning with the ISO/IEC 27031:2011 standard that describes the concepts and principles of IRBC, we aim to provide you with a blueprint for ensuring your business continuity plan deals with any security incident and aid you in developing a consistent and confident approach to planning and implementing a disaster recovery (DR) plan.

# BACKUP AND RECOVERY BLUEPRINT

***ISO 27031 provides a framework of methods and processes to guide organizations in identifying and specifying all aspects — such as performance criteria, design and implementation — to improve their IRBC. It guides IT pros on how to effectively plan for business continuity and disaster recovery (BCDR) by helping them recognize, respond to and recover from disruptions to ICT services.***




## PLAN

- Develop business requirements based on BIA results
- Understand critical ICT services
- Develop/update IRBC Policy
- Identify performance gaps
- Develop strategy options

## DO

- Document IRBC processes
- Implement IRBC Strategies
- Implement/update ICT response and recovery plans
- Execute training and awareness activities

## CHECK

**Ongoing**

- Monitor, detect and analyze threats
- Measure IRBC performance

**Annual Review**

- Test and exercise IRBC strategies
- Review and audit by internal and external groups

## ACT

- Management reviews IRBC program
- Management directs IRBC improvement measures

Organizations need to implement a systematic process to prevent, predict and manage disruptions and incidents that can potentially disrupt ICT services, which is best achieved by employing a Plan-Do-Check-Act (PDCA) cycle. The goal of the PDCA cycle is to put into action measures that can improve preparedness and response in the event of an interruption in ICT services. By doing so, you can ensure both information security management (ISM) and business continuity management (BCM) are effectively carried out. Ensuring the continuity of ICT services helps in monitoring, access control, safe transmission and secure storage of confidential information, thereby aiding in ISM. At the same time, by assuring that the ICT services are resilient and recoverable within a pre-determined period, the PDCA cycle also helps support BCM.

## *Plan*

Planning is the first stage in the PDCA cycle, where the overarching governance structure of the IRBC management system is established and maintained. During the planning stage, an IRBC policy is formulated, which defines the best practices to be followed so the business can continue its operations amid an IT disaster and determines the potential IT strategy solutions that will help meet those requirements. The goal here is to minimize the disruptions and losses caused by the incident while also enabling the business to meet its time-bound commitments. Establishing an incident response (IR) plan is critical; businesses without an IR plan incurred, on average, data breach remediation costs $2.66 million higher than those with an IR plan.

To realize operational continuity amid a disaster and swift recovery from it afterward, an organization must have an effective BCDR plan in place. A BCDR plan mitigates the damage and ensures the continuity of vital business processes during a disruptive event. It also includes steps to quickly restore ICT systems and data to resume business as usual after the event.

A major consideration here is the creation of a failback site to replicate/relocate the mission-critical data and ICT systems so that the business can continue its operation without disruption. It would be best if you also considered geographical and infrastructure risk factors, such as the need for multiple sites or backups in the cloud. It's also critical to note that your data within the cloud also needs to be replicated or backed up in an alternative cloud location for comprehensive protection. For instance, data in your SaaS applications like Microsoft 365 and Google Workspace can be at risk from a wide range of threats. Backing up your SaaS data in an alternative cloud location will make you impervious to such attacks.

The planning stage must include a risk assessment and business impact analysis and establish the recovery objectives — recovery time objective (RTO) and recovery point objective (RPO) — accordingly. This stage can also be used to delegate roles and responsibilities, determine communication channels and document all the relevant processes and procedures.

## Do

The “Do” stage focuses on performing activities and implementing solutions that were established in the first stage so that the organization can keep an eye out and get back up and running in the event of an ICT services interruption. The key outputs for this phase are the implementation of determined strategies, the generation of appropriate plans and the execution of training and awareness activities to realize IT resilience and support the continuity of ICT services.

Tabletop exercises are an excellent practice on that front. When an unpredictable incident like a natural disaster or a cyberattack occurs, the more you are prepared, the better the results will be. Such exercises help teams experience firsthand the challenges that may arise and take on the roles they would need to during a real crisis. It also allows them to pinpoint areas that require improvement and prepare a step-by-step plan guideline.

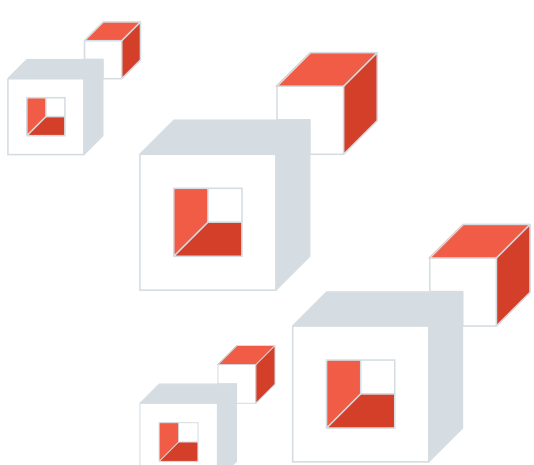
## Check

Imagine discovering that your recovery strategies and plans do not work in the midst of an IT disaster. That’s why it’s critical to have the “Check” phase, where the review and evaluation of your backup and recovery plan and the performance of the IRBC management system take place. The key outcome of this phase includes continuous monitoring of ICT systems for disruptions and periodic reviews of ICT responsiveness and recoverability.

Organizations need to have a comprehensive DR plan and conduct regular testing, failing which they could face devastating consequences while attempting a recovery during an emergency. However, DR testing can eat up your valuable resources and time and drastically impact your productivity if your organization lacks automated testing capabilities. You must be able to automatically test and certify your RTO, RPO and SLAs ahead of time without affecting your production servers.

## Act

In the final phase, the leadership should assess how effectively the whole IRBC strategy is working and consider implementing remedial measures to improve the effectiveness of the initiatives and lessen the likelihood of interruptions to ICT services. This stage ensures the continuous improvement of IRBC and, thereby, the organization’s readiness to handle unforeseeable events that could jeopardize business operations.



# BACKUP AND RECOVERY WITH SPANNING

Today, SaaS applications like Microsoft 365, Google Workspace and Salesforce have become an integral part of the ICT infrastructures of modern businesses. They have become the goldmines where the majority of your business-critical data go in as individual emails and messages, shared files, folders and drives, calendar entries and so on. The widespread adoption of SaaS platforms is rapidly expanding the organizational attack surface, placing increasing strain on security teams to manage and defend a more complex threat landscape. Moreover, the shared responsibility model (SRM) of cloud security places the onus on the respective organizations to secure their data in the SaaS applications. According to SRM, while the SaaS providers ensure the security and integrity of the platform, the onus is on the customers to manage and secure the data generated.

## *That's where Spanning can save the day.*

Spanning provides purpose-built, cloud-to-cloud backup and recovery for Microsoft 365, Google Workspace and Salesforce that is completely secure, surprisingly affordable and exceptionally easy to use. Spanning Backup automates the backup process, eliminating redundant manual tasks to free up your team to focus on more strategic initiatives. With cutting-edge features like granular, end-user self-service restores and integrations like dark web credential monitoring, Spanning makes your backup and recovery a breeze while giving you 100% confidence in your SaaS data protection.

With customizable retention options and flexible license management, Spanning's industry-leading solution offers the lowest total cost of ownership (TCO) in its class. What's more? Spanning can be set up, installed and made fully functional in minutes, not hours or days — **No** expensive training costs, **No** lengthy installation and configurations, and **No** headaches.

***There are "bad days" in IT. Then there are the "really bad days," which can put the whole business at risk. These are just a couple of examples where Spanning has helped organizations like yours get through their worst days unscathed.***

# MILLAR SAVES LIVES. WE SAVE THEIR DATA

**Founded in 1969, Millar, Inc. is a medical device manufacturer**, world-renowned for their catheter-based sensors and devices that aid in medical research and clinical diagnosis. Since Millar is an FDA-regulated business with strict compliance requirements, they take data protection very seriously. The company needs to keep product-related information backed up and accessible for the lifecycle of their products, which could range from seven to 20 years.

Millar considered various backup solutions before choosing Spanning to protect their data, intellectual property and email communications stored in Microsoft 365. “We looked at a backup solution that was going to be able to indefinitely keep all our data. And that was one factor that really drew us to Spanning,” says Todd Miller, director of IT at Millar, Inc.

Over the years, Spanning has maintained the trust that Millar kept. There had been occasions where the organization had to restore emails that had been mistakenly deleted or missing. “Spanning has a really nice console where we can go into an individual mailbox and actually search for that piece of mail throughout the entire account. And once we’ve found it, we literally just check it, hit restore, and then you can either restore it to the individual user or do a cross-mailbox restore,” notes Miller. Spanning’s quick point-in-time restores have also been especially helpful for the company while accessing and restoring critical information from former employees’ mailboxes. “It was that combination of the simplicity of use and the automation that it offers that really drove us to choose Spanning over other providers,” Miller asserts.

> ***From an IT Director’s standpoint, choosing Spanning has really been kind of a no-brainer. It frees up resources to work on other projects and push other technologies.***

# GLOBAL BRANDS TRUST SENDGRID, AND SENDGRID TRUSTS SPANNING

**SendGrid is a globally renowned cloud-based email service provider** with over 69,000 customers like Spotify, Uber and Airbnb. The company sends more than 40 billion emails every month. The onus of protecting their enormous amounts of valuable customer data made them switch from the manual, weekly export provided by Salesforce to Spanning Backup for Salesforce. “We chose Spanning Backup because our IT team had been using it for Google Workspace and was very happy with it,” says Kerry McDonough, business systems administrator for SendGrid.

Spanning works as a tab right inside the Salesforce application, eliminating the cost and risk associated with manually exporting data for backup. “I live in Salesforce, so it makes sense that the backup solution is in there, too. There’s no manual labor or downloading required with Spanning Backup,” adds McDonough. Since Spanning backs up metadata — including customized reports, dashboards and email templates — SendGrid never has to worry about painstakingly recreating all those customizations in the event of a data loss.

The set-and-forget system of Spanning excites SendGrid and McDonough the most. “A weekly backup is not sufficient when you’re working in a fastpaced startup environment. Things change every day! I love the ‘set it and forget it’ aspect of Spanning Backup; it just runs automatically every day,” mentions McDonough.

> ***Transparency, honesty and trust are crucial to us in all aspects of our business — hiring, working together, working with customers and working with vendors. I trust Spanning with our data because they are so open and transparent.***

More than 20,000 organizations like
Millar and SendGrid have put their faith in Spanning
and reaped the benefits — and your business could be next.

## AUTOMATE YOUR BACKUP AND RECOVERY WITH SPANNING BACKUP AND TAKE COMPLETE CONTROL OF YOUR SAAS DATA AND TIME.

**GET A DEMO TODAY**

SPANNING
A Kaseya COMPANY