IBM Technology
Lifecycle Services

Driving operational resiliency with IT support and services

Highlights
Infrastructure Support

Visibility and prioritization of IT risks

Managing risk with proactive support services

Managing risk with a consolidated data center support strategy

Operational Resilience Testing

With the continued rise of cybersecurity incidents, it’s not surprising to see legislation emerge around operational resiliency in the finance industry. Whether it’s the Digital Operational Resiliency Act (DORA) in the European Union, regulatory guidance like SR 20-24, Sound Practices to Strengthen Operational Resilience in the US, or Operational Risk and Resilience Guidance in Canada, these regulations are increasing expectations on financial institutes for governance, risk identification, and management as well as operational resiliency and third-party risk management. Of course, the end goal is to ensure that financial organizations are prepared with the right strategies to proactively prevent and recover in the face of a cyberattack, data corruption, catastrophic system failure, or other types of incidents. In many cases, non-compliance and/or failure may result in severe financial penalties for the companies concerned.

IBM has a range of services and solutions to enable financial entities to address security and operational resiliency. IBM Consulting™ provides services for risk assessment, risk governance and controls, and third-party ICT risk management. IBM software solutions cut the time to automate data discovery and governance by up to 90%,[1] helping with compliance and reporting. IBM Data Security helps secure data and automate compliance auditing. IBM Security® helps with incident reporting and management, IBM Security X-Force® offers services for detection and recovery from incidents, and managed detection and response, and IBM Control Desk with Maximo® helps organizations manage and report critical assets.

In addition to these services and solutions, IBM believes that IT support and services can be an important element in the ongoing requirements for operational resiliency. IBM TLS can help clients with services and support solutions that provide proactive identification and remediation for potential issues before they occur.

Infrastructure support

Operational resiliency depends on infrastructure running smoothly and securely. That means constantly balancing between the cost and resources involved in implementing new technologies like hybrid cloud or containerization with the need to maintain at least basic support contracts for hardware and software in production. According to IDC, “Enterprises should prioritize IT support services by workload criticality, viewing them as an investment in preserving the business value of these systems by relying on vendors for optimized performance.” The report also notes that enterprises surveyed are currently saving 290 hours of downtime with server, storage and networking support contracts; more explicitly, they are preventing 79 hours of unplanned downtime thanks to predictive and proactive support tools. [2] It seems that the more critical the workload, the more proactive support should be considered.

To effectively manage 6 Million+ service tickets per year, IBM relies on a global support infrastructure that includes AI-fueled tools like Call Home, Remote Technical Support (RTS), and Cognitive Support Platform (CSP). IBM’s remote support is designed to automatically connect, perform diagnostic analysis, and recover/resolve most problems often within an hour. IBM’s remote support teams resolve 74% of IBM infrastructure hardware and software issues.[3] Client Availability Leaders, Technical & Project Escalation Managers ensure the timely handling of critical situations both remotely and on-site. IBM’s tiered support approach with IBM Expert Care and IBM Multivendor Enterprise Care enables clients to choose the best level of support based on their needs.

Visibility and prioritization of IT risks

One of the key questions organizations should be asking themselves is how they can proactively monitor and assess IT risks to quantify and prioritize the most critical ones. Visibility across the IT estate can be challenging, and IT risks change frequently. Even then, visibility is not enough. Risks need to be understood, assessed, and prioritized into timely action plans to effectively manage the most critical risks early on.

IBM Support Insights, included with IBM infrastructure warranty support and maintenance contracts, provides visibility across the IT estate along with headlights to potential issues and recommended actions for certain vendors. This cloud-based service acts as a single pane of glass, which unifies the support experience across IBM and multivendor infrastructure, providing analytics-driven insights, inventory management, and preventive maintenance recommendations. IBM Support Insights Pro subscription offers additional value with prioritized security vulnerability and lifecycle insights, recommended OS, and firmware levels – focused today on insights for IBM Power and Cisco.

Support Insights provides alerts for different risk factors which include security vulnerabilities, support coverage, operating system/firmware risks, and hardware risks. In addition to ongoing alerts, the tool provides risk scores with an at-a-glance view of the potential threats to the IT environment.

Categories of risk scores are computed using data and insights from a variety of sources and analyses:

- Security: Common Vulnerabilities and Exposures (CVEs) for known OS and firmware levels
- Coverage: Contract and warranty expiration events
- Firmware: Software end-of-support/end-of-life events and OS/firmware diversity
- Hardware: Hardware end-of-support/end-of-life events (IBM Infrastructure only) and vendor field notices (Cisco only)

This helps understand risks and provides information and insights needed for effective targeting and mitigating the possible negative outcomes associated with the assets in question. Alerts include a risk score (High, Medium, Low) that is determined based on the type, priority, and time frame (immediate versus projected) of the risk. This enables organizations to quickly prioritize mitigation efforts based on risk levels. Alerts also come with specific mitigation recommendations which include specific suggestions and options for remediating the issue at hand. Depending on the risk category, the recommendations may include information about patches to apply, versions to upgrade to, advisory replacement options, and others. Not all alerts have specific recommendations, but they generally provide best practice guidance for helping mitigate risk from the alert.

Managing risk with proactive support services

Visibility to IT risk is the starting point, but then it's down to organizations' already stretched IT staff to follow up on alerts and take the appropriate mitigation actions in a timely way. In 2022, XForce identified 23,964 security vulnerabilities.[4] Once alerts are published, organizations need to explore them, prioritize the ones to address first, and then start mitigation actions. Supplementing IT staff with vendor-provided proactive support can enable organizations to prioritize day-to-day maintenance actions which can often be delayed by unexpected issues and strategic IT projects.

IBM works with clients to customize their support services to provide both reactive and proactive solutions. Some examples of different support services IBM can execute in place of IT staff include :

- Single point of contact for severity 1 and 2 issues
- Problem determination, problem source identification, and resolution
- Custmized support plans which include operational and maintenance processes, current support structure, critical applications, critical outage scenarios, and envrionment
- Reports summarizing service activity for reported problems with proactive recommendations
- Document and maintain availability requirements
- Performance analysis and recommendations for improvement
- Execution of preventative services

You can count on IBM Technology Lifecycle Services to keep your mission-critical systems running smoohtly 24x7

Managing risk with a consolidated data center support strategy

The proliferation of vendors in the data center has a direct impact on the amount of downtime experienced, according to IDC.[2] With each new product and vendor, interoperability risks are exponential. With separate contacts for each vendor, it becomes more and more difficult to pinpoint a single area impacting performance. The amount of time organizations' IT staff spend on vendor support is also a key concern for many as it takes time away from more strategic activities. Finally, each person who has physical access to your data center is a potential security risk.

Consolidating vendor support to a trusted vendor is one way organizations can address operational resiliency across the data center. Working with IBM as the trusted supplier for consolidated data center support has shown to address the concerns mentioned above. In fact, clients have achieved reduction in mean time to problem resolution, reduction in time spent on hardware support and on vendor management, avoidance of outages as well as cost reductions.[5] Read the Forrester report : The Total Economic Impact of IBM Hybrid IT Support for more details on a consolidated support strategy with IBM.

Operational Resilience Testing

Regularly checking the infrastructure for potential weaknesses is also vital to maintaining resiliency. Organizations need to identify potential single points of failure that may cause or extend outages. They should plan to review machine logs, records, and trends to isolate chronic problems and develop action plans to avoid or minimize the impact of unplanned outages. IBM can provide quick health checks for products in the data center. In addition to rapid health checks, deeper assessments can be conducted to tune for optimal performance or to go deeper into security vulnerabilities.

Given the multiplicity of individual products and vendors in most data centers today, it's not enough to do resilience testing at the product level. Whether an organization has just had a major incident or want to be more proactive about maintaining high levels of availability, an assessment of the environment as a whole can help uncover dependencies and inhibitors to high availability and propose best practices to maintain it. The IBM High Availability Center of Competency can help with assessments, post-incident reviews as well as best practice and knowledge sharing.

Conclusion

Operational resiliency depends on an efficient and effective infrastructure. Keeping that infrastructure current, gaining visibility to potential risks, and aggressively taking action to mitigate those risks are critical to success. Organizations need a trusted partner who understands their business needs and takes a holistic approach to support and services with a focus on resiliency.

Why IBM Technology Lifecycle Services

IBM Technology Lifecycle Services works with organizations to tailor an approach that meets their operational resiliency needs. IBM has over 35 years of experience providing multivendor maintenance and support for approximately 22,000 IBM and other third-party hardware and software products. With a global footprint that extends to over 130 countries, you can rest easy knowing that resources are available when you need them. Finally, per the IDC Marketscape 2022 Worldwide Support Vendor Assessment, IBM's top strengths as a global support provider are our global presence and multivendor capabilities, our proactive care capabilities, and our C-suite relationships which allow us to understand our clients' business needs[6].

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
January 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

[1] "IBM Cloud Pak for Data enhances DataOps services to deliver business agility with cost savings and risk reduction," Aliye Ozcan, May 2020.
[2] IDC Perspective: The Cost of Downtime in Datacenter Environments: Key Drivers and How Support Providers Can Help, Doc # US50240823, March 2023
[3] IBM internal data
[4] X-Force Threat Intelligence Index 2023
[5] The Total Economic Impact for IBM Hybrid IT Support, A Forrester Study Commissioned by IBM, January 2023.
[6] IDC Marketscape 2022 Worldwide Support Vendor Assessment, IDC, March 2022