5 pillars of IT that can help to keep your business running when the unexpected occurs

Achieving IT Resilience

getronics

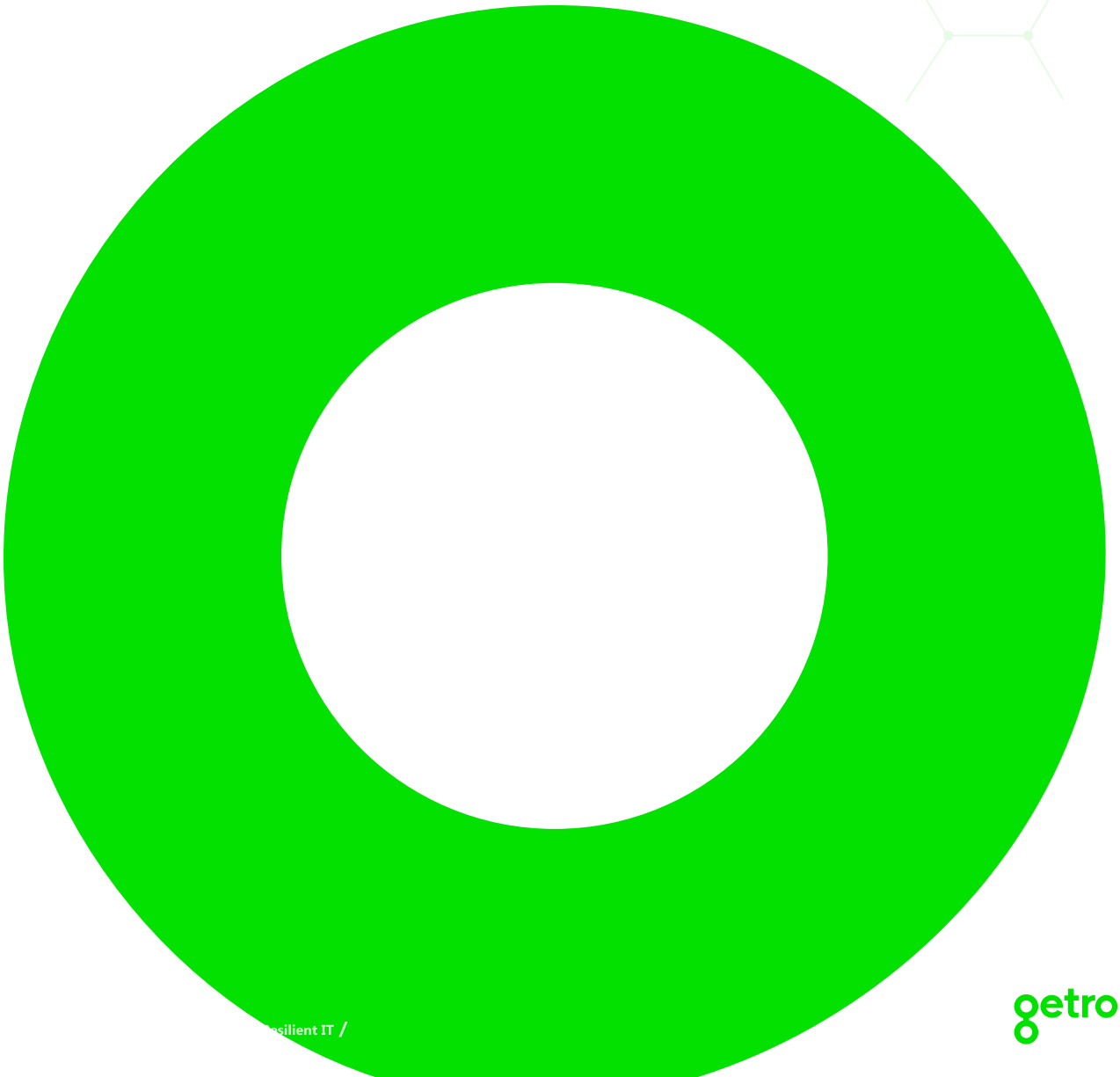
What's inside

Executive summary

Global investment in IT is expanding amidst growing risks like geopolitical tensions, climate change and cybercrime. Organisations increasingly recognise technology's crucial role in ensuring business continuity when a disruptive event occurs. While IT is a major target for threats such as a ransomware, it also protects your organisation's valuable data and assets. Strategic IT investment enhances resistance to threats (including human errors) and improves recovery capabilities.

Resilient IT starts with robust cybersecurity. In addition, it encompasses a broad range of practices and technologies that ensure a rapid response and recovery. At Getronics, we advocate developing a strategic, data-driven disaster recovery (DR) plans and a comprehensive business continuity management system (BCMS), aligned with international standards such as the ISO 22301 and the Business Continuity Institute's Good Practice Guidelines. Integrating these measures from the design stage ensures efficiency and long-term cost-effectiveness.

This white paper outlines five core pillars of IT essential for DR and business continuity (BC) capabilities: security, cloud, infrastructure, digital workspaces, and support. Each section covers technical measures and good practices that ensure resilience, from secure-by-design approaches and privileged access management to advanced cloud storage solutions and resilient digital workspaces. Adopting these practices, organisations do not only **safeguard their operations against interruptions** but also **gain a competitive edge** by ensuring they can **adapt quickly and efficiently to changes** and challenges.



getronics

Definitions

3-2-1 Principle

A data backup strategy that involves creating three copies of data, storing them on two different types of storage media, and keeping one copy off-site or offline. This approach ensures redundancy and resilience against data loss in case of hardware failures, disasters or cyberattacks.

Business Continuity

The capability of an organisation to continue its essential functions and operations during and after a disruptive incident or crisis.

Business Continuity Institute (BCI)

A global professional organisation that promotes the science of business continuity management (BCM) through education, certification, research and collaboration amongst BCM professionals worldwide.

Business Continuity Management (BCM)

The process of planning, implementing, and managing measures to ensure the continuity of essential functions and operations in case of a disruptive event.

Business Continuity Management System (BCMS)

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. The management system includes organisational structure, policies, planning activities, responsibilities, procedures, processes, and resources.

Business Impact Analysis (BIA)

A structured evaluation that identifies potential effects of disruptions on business operations, including financial, operational, and reputational impacts.

Consultative Approach

A method of problem-solving and decision-making that involves collaboration, expertise, and tailored solutions based on the unique needs and circumstances of an organisation.

Disaster Recovery (DR)

The process of restoring systems, operations, and infrastructure to normal functioning after a disruptive incident, minimising downtime and restoring service levels.

Disaster Recovery as a Service (DRaaS)

A cloud computing service model that allows an organisation to back up its data and IT infrastructure in a third-party cloud computing environment and provides all DR orchestration.

Disaster Recovery (DR) Workflow/Runbooks

The IT recovery project plan that considers recovery priorities, application and infrastructure groupings, dependencies and technical tasks that get executed by technical resources as part of a recovery process.

Disaster Recovery (DR) Testing:

The practice of planned and scheduled disruptive and non-disruptive IT recovery exercises often required to satisfy regulatory, compliance and stakeholder requirements.

Failover

A process in which a system automatically switches to a redundant or backup system to maintain continuous operation and prevent downtime in case of a failure or disruption in the primary system.

High Availability (HA) Technology

Systems and solutions designed to minimise downtime and ensure that critical business functions are available 99.999% of the time (less than 6 minutes of downtime per year).

Immutable Backup:

A type of data backup that cannot be altered, deleted or modified once it has been created. This ensures the integrity and security of the backed-up data, protecting it from unauthorised access, tampering or deletion.

Incident

An unplanned event, occurrence or situation that disrupts normal operations and requires a response to mitigate its impact.

Maximum Tolerated Data Loss (MTDL):

The maximum amount of data that an organisation can afford to lose during a disruption or incident without causing significant harm or impact to its operations.

Maximum Tolerated Period of Disruption (MTPD):

Time it would take for adverse impacts, which can arise as a result of not providing a product/service or performing an activity, to become unacceptable.

Penetration Testing (Pentesting):

A proactive security assessment where simulated cyberattacks are conducted on IT systems to identify vulnerabilities and ensure the effectiveness of defences in maintaining business continuity during potential disruptions.

Privileged Access Management (PAM):

A security mechanism that controls and monitors access to critical systems and sensitive information by privileged users to prevent unauthorised actions and mitigate risks in disaster recovery and business continuity scenarios.

Reciprocal Support:

The ability of multiple teams (in various locations) to support each other in times of need or during disruptions. This ensures that essential services can be maintained even if one location faces challenges or outages.

Recovery Time Objective (RTO):

The targeted duration of time within which systems, operations or functions must be restored after a disruption to meet business requirements or objectives.

Resilience:

The ability of a system or organisation to withstand and recover from disruptions, maintaining essential functions and operations.

Resilient IT

IT systems designed to withstand and quickly recover from major disruptions, ensuring continuous business operations.

Response:

The actions taken during and immediately after a disruptive incident to address and mitigate its impact, ensuring continuity of essential functions.

Risk Assessment (RA):

The process of identifying, analysing and evaluating potential risks and vulnerabilities that could impact an organisation's operations and objectives.

Chapter 1

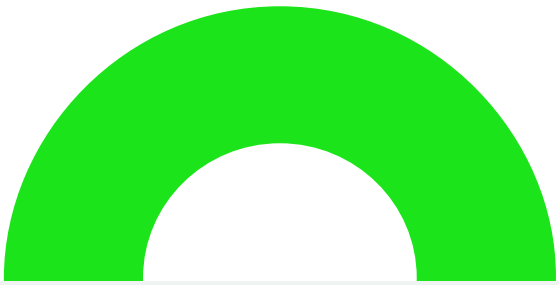
Why resilient IT matters

Despite turbulence throughout the global economy, organisations in every industry continue to invest heavily in maintaining and updating their technology ecosystems. Recent reporting predicts that IT spending will grow by 8% in 2024, reaching a new record of $5.1 trillion globally[1] This prioritisation of IT expansion – even during tough economic times – underscores the importance of technology in the modern business world.

IT has always been a target for attack when it comes to those who want to cause disruption. This means that modern IT services have needed to be vigilant, responsive, and strategic in the way that these disruptions are tackled. This need for innovations offers great opportunities to optimize and transform protection methodologies, and recovery strategy. More and more organisations need DR testing, and strong cyber-security, by constantly evolving these services we are always at the forefront of IT protection.

New regulations are driving the need to revise protection methodologies and recovery strategies, clients who have previously relied on DC failover testing are requesting new and improves ways to recover from cyber-compromised scenarios. We're seeing a circle where updates in regulation lead to industry evolution.

To promote resilience, modern organisations require a data-driven disaster recovery (DR) plan and business continuity management system (BCMS) in place. When the unexpected occurs, companies must be able to rely on their IT systems to efficiently recover. That is why it is vital to invest in building resilient IT systems that are designed to withstand a major disruption, whether it is a disaster (flood, earthquake), a human error or a cyberattack. These systems must be designed with DR strategies in mind, ensuring simple, reliable and effective recovery processes, while incorporating safe testing practices.



A strong, IT-based BCMS presents key advantages:

- **Reduction in downtime, resulting in major cost savings**

Companies that invest in resilient IT systems experience significantly lower downtime in the event of a disruption. This offers a major financial advantage, considering the staggering cost of downtime. Studies show that the average cost of IT downtime is approximately $5,600 per minute – or $300,000 per hour – depending on the organisation and context.[2]

- **Compliance and risk management**

Resilient IT also helps organisations comply with various regulatory requirements, which demand certain standards of data protection and system availability. Regulations like General Data Protection Regulation (GDPR), DORA, and NIS2 in the European Union require companies to ensure the integrity and availability of personal data. In the event of a disruption, this level of compliance can only be achieved through IT that is designed for resilience.

- **Innovation and competitive advantage**

Businesses with resilient IT frameworks are better positioned to adapt to market changes and incorporate new technologies, such as GenAI, augmented reality and off-premise infrastructure, while also mitigating risks. This adaptability not only helps in maintaining continuous operations, but also provides a competitive advantage by enabling quicker integration of innovative solutions.

In this white paper, we explore how the right IT measures contribute to your organisation's business continuity by ensuring preparedness and allowing for a more effective response and recovery. If you would like to learn more about how to embed business continuity throughout your organisation's facilities and workforce in addition to your IT, please also read our full white paper on the topic: "Building Business Continuity into Your Organisation".

[1]Source: IDC
[2]Source: OHV Cloud

Designing IT for preparedness

Robust IT security and risk management are at the heart of any modern BCMS. Security is interconnected with all areas of any organisation's IT. However, to make your company's IT resilient, **business continuity should be enshrined not just in your security, but in all aspects of your tech** landscape. That is why we focus in this white paper on 5 core pillars of IT that require business continuity planning:

1. **Security**
2. **Cloud**
3. **Infrastructure**
4. **Digital Workspaces**
5. **Support**

Strategic investment in these areas is crucial to achieving resilient IT, because poor investment decisions lead to vulnerabilities that put your organisation at risk. At Getronics, we conduct comprehensive DR testing to generate numerous post-test recommendations, highlighting recovery expectations and in some cases the need for a solution redesign if the achievable recovery time objectives (RTOs) fall short of your organisation's business requirements. DR is fundamentally about optimising recovery and setting business recovery expectations. It asks the question: how swiftly can operations be restored? While testing provides opportunities for improvements, the critical limiting factor remains the strategic technical IT design and deployment. By getting this right, you establish a stronger foundation to optimise recovery processes, minimise business disruption and ensure compliance with a BC strategy that accounts for your organisation's specific, predefined Recovery Time Objective (RTO).

In the chapters that follow, we include a list and description of key technical capabilities that help ensure resilience across each of the 5 areas listed above. We also show how these capabilities lead to better business outcomes. The good practices we emphasise in each section are based on our experience of fully integrating business continuity into our own operations and those of our clients around the globe.

As you will see, these 5 focal points are not fully separated from one another, rather they are interconnected. Security and Infrastructure, for example, are integral aspects of all IT operations and are the underlying foundation of any successful company. Digital workspaces, cloud and support all work hand in hand to form a modern, resilient user experience for your workforce and customers.

The key is to consider these aspects in combination with one another and to take a proactive, holistic business continuity approach based on industry-recognised good practices, such as the BCI Good Practice Guidelines and the ISO 22301 Business Continuity standard.
By incorporating business continuity and improving your IT strategy from the outset, you enhance your organisation's business resilience while also gaining the maximum value from your investment in IT.

Chapter 2

Business Continuity through security

A robust security posture is your first line of defence against the ever-increasing threat of cyber-attacks, such as hacking and ransomwares. Resilient security also involves protecting your organisation's facilities from physical threats.

Key technical capabilities for a resilient security

While security covers a wide range of technologies and strategies, the following features and capabilities form the backbone of our own security strategy, and are among the most powerful security options we recommend:

Secure by design:
A 'secure-by-design' approach establishes a strong foundation for your organisation's security. This proactive strategy integrates security into all aspects of your business processes, from design to risk management to monitoring and response. By embedding security throughout, you enhance protection for your data, IT infrastructure and applications.

Dedicated security management role(s):
Security requires continuous attention. Designating individuals or teams within your organisation to manage security is essential. These roles are responsible for defining security policies, selecting the right vendors and solutions, advising the board or c-suite level employees, and coordinating and validating security procedures.

Network & device protection methodologies:
This involves practices like regular system patching and timely phasing out of obsolete or unsupported operating systems. Protecting your network and devices also includes implementing robust designs with high levels of firewall protection. Additionally, it is important to ensure secure data centre hosting and resilience measures, such as redundant power and network links, resilient cloud deployments, replication and backup protection measures.

Security monitoring & threat prevention:
This enables you to continuously monitor your organisation's systems, networks and applications for potential security threats. It includes using advanced security monitoring tools and technologies that detect and respond to security incidents in real-time. Threat prevention proactively identifies and mitigates potential security risks before they can harm your organisation.

Best practices for implementing a resilient security strategy

To achieve the best results along your path to resilient security, the following best practices are indispensable:

Consultative approach

Resilient security is never a one-size-fits-all solution. It requires a consultative approach tailored to your organisation's unique risk factors, needs and budget. Work closely with a trusted partner to identify your IT landscape's unique security challenges and develop customised strategies that effectively mitigate risks and enhance resilience.

Supplier management assessments

At Getronics, we proactively evaluate the business continuity management practices of our suppliers to ensure resilience in every link of our supplier chain. We share our knowledge with our clients to enhance their overall security posture and minimise risks associated with third-party dependencies.

We have active experience of dealing with device failures in real time. The IT industry can be limited by reliance on products and service providers, and in doing so open their systems to potential problems. Getronics considers every aspect of OS systems, from Microsoft & Apple, to Linux, all with the goal of creating a stronger platform for users. We know that we can identify issues before they hit, and in times when it's beyond our control we act quickly to resolve them.

Regular security audits

Regularly auditing your IT systems enables you to identify vulnerabilities. The frequency and scope of your auditing depends on your business's compliance risk, industry regulations and other factors. For example, a hospital might perform a security audit every few months to ensure patient data is fully secure, while a small design studio might check in once a year to keep their client files safe.

Security management practices

Implementing security management means having a plan to protect your data and systems. An e-commerce website, for example, might have a robust security management plan that includes everything from employee training to incident response strategies, ensuring they can fend off attacks and keep customer data secure.

Penetration testing (pentesting)

This practice involves experts trying to hack into your systems to find vulnerabilities before actual criminals do. A financial institution, for example, might perform these tests regularly to uncover and fix security gaps, whereas a media company might schedule pentesting ahead of launching a new app or service.

Security as a source of resilience

Security isn't just a way to keep your peace of mind, it can also be used as a source of resilience in your operational practices. A strategy that keeps recovery at the forefront of its process **will offer your business key benefits, such as safeguarding your data, infrastructure and operations**. We know that these areas can be a source of anxiety for any business that cares about their operational strength, and security is the answer to maintaining them.

Avoiding data breaches, and compliance issues is a key aim for companies that deal with sensitive information. More and more end-users want to know their data is safe, and Getronics supplies the tools necessary to keep your reputation strong, and your finances low.

The needs of business security is ever evolving. As threats change, we need to change too, so we ensure that we protect against these changes and mitigate risks at the same time.

Our offering is bespoke, and comprehensive.

Safeguarding your data, infrastructure and operations

Avoiding data breaches and compliance issues, which can have devastating financial and reputational effects

Mitigating risks and protecting against ever-evolving security threats

Chapter 3

Business continuity through cloud

Cloud-based solutions offer businesses many key advantages but can expose you to business continuity risks. This underscores the importance of choosing the right cloud partner and ensuring they have the credentials to meet your security expectations.

Key technical capabilities for resilient cloud services

To ensure your cloud-based services are resilient in case of a disruption, here are some key capabilities that we recommend:

Cloud storage solutions

Using the cloud can protect important data from local hardware issues. For example, a weather analysis firm might store massive data sets in the cloud to protect against data loss from local disasters, whereas a small startup might use cloud storage for ease of access and collaboration.

Strategic deployment

When selecting cloud partners, we advise that you carefully assess them for failure potential, based on a Business Impact Analysis (BIA) and Risk Assessment (RA). Cloud platforms offer a more secure hosting environment, which helps improve your resilience and create a failover plan for each application, based on how critical it is to your business. A balanced, yet resilient strategic deployment approach can combine various solutions, including hybrid setups, to effectively meet your business needs and budget.

High availability resilience design

This means achieving high availability (HA) and resilience of business-critical apps through a design that minimises downtime and mitigates single points of failure. HA systems incorporate dynamic monitoring and automatic failover mechanisms to quickly transition operations to alternate platforms in case of a failure. For example, fully mirrored systems in the cloud can ensure continuous operation even when primary systems fail, with options for load balancing across geographically separated sites (‘active-active’ configuration) or for fast failover (‘active-passive’ configuration). The Getronics Security Operations Centre (SOC) security service platform, for example, is built on a solution that allows for an ‘active- passive’ failover in just minutes from one data centre to another.

Modular resilience

Cloud services can use modular architecture to enhance their resilience. With a modular design, application stacks consist of decoupled components delivered from separate resilient platforms. If one part fails, the entire application remains operational. This is common in web-based applications, where it helps to maximise uptime.

Extracting and archiving data for SaaS mitigation

Ransomwares cannot affect what they cannot touch. A layered backup approach, including air-gapped backup mediums like backup tape, serves as a last line of defence. Managed backup services ensure comprehensive data and system recovery, incorporating regular restore tests and virtual machine-level backups for efficient recovery during disruptions. Migrating to new immutable backup services offers advantages over traditional tape recovery by eliminating the need for offsite storage and speeding up recovery times. Technologies like immutable backups and hardened backup servers enhance security against cyber-attacks. Businesses should consider both fast recovery and slower, comprehensive recovery scenarios in their disaster recovery planning.

Best practices for implementing a resilient cloud strategy

To help our clients achieve a resilient cloud strategy, we advocate best practices like these:

Continuous monitoring and improvement:
Implement robust monitoring systems to detect and respond to potential threats or failures in real-time. Regularly assess and update cloud infrastructure and procedures based on lessons learned from incidents to ensure ongoing resilience and preparedness. Monitoring aspects like replication status, current Recovery Point Objectives (RPO) and thresholds for delays are crucial. Data replication history typically spans 24 to 48 hours, but longer periods may be needed, impacting storage requirements and costs. If data is corrupted, organisations may need to restore from earlier timestamps using offline backups, as cyber attackers often infiltrate systems undetected for days or weeks. This dual approach ensures both real-time protection and the ability to recover from older, uncompromised data.

Multi-layered security:
Deploy a multi-layered security strategy that includes encryption, access controls and regular security audits to protect your data and systems from unauthorised access or breaches.

Cloud as a source of resilience

A resilient cloud strategy offers key benefits for business continuity: New tools require new applications, and as we integrate cloud into our daily operations, it's time to understand how to use it for multiple benefits. Cloud can reduce the downtime during disruptions, keeping uninterrupted operations ongoing.

It's also the most cost effective way to manage your resources, whilst keeping a robust backup and recovery system.

- **Reduced downtime and uninterrupted operations during disruptions**
- **Robust managed backup and recovery**
- **Optimal, cost-effective resource management**

Getronics provides Managed Backup service alongside our Managed Infrastructure service, taking all aspects of data and systems recovery into account as part of your backup strategy. For example, virtual machine (VM)-level backups provide fast recovery of your entire system whenever an incident occurs without having to reprovision a VM, install apps, reconfigure and recover data, etc. More and more of our clients are benefiting from our 'last line of defence' disaster recovery tests using protected offline backups as well as more conventional data centre failover DR testing strategies. We advocate conducting periodic tests as part of your business as usual (BAU) program. After all, your backup and restore integrity is only as good as the last restore attempt.

Chapter 4

Business continuity through infrastructure

Key technical capabilities for resilient infrastructure

Designing and maintaining a resilient IT infrastructure is essential for enabling your business to recover as quickly as possible to reach its Minimum Business Continuity Objective (MBCO) in case a disruption occurs.

The top technical capabilities for a resilient IT infrastructure include:

Infrastructure as Code (IaC):
During the COVID-19 pandemic, many organisations embraced IaC as it enabled them to rapidly scale and manage IT infrastructure remotely, enhancing operational resilience and continuity in a predominantly digital work environment. IaC offers many key advantages that contribute to resilience. By automating the rapid provisioning and configuration of infrastructure, IaC ensures consistent and repeatable deployments, which are crucial for maintaining operations during and after disruptions. It also allows for quick scaling and adaptation of resources to changing needs, and its version control capabilities enable swift recovery of previous states, minimising downtime and ensuring continuous service availability.

Scalable backup offerings:
This involves implementing scalable backup solutions that adhere to industry best practices, such as the 3-2-1 rule: maintain 3 copies of your data, on 2 different media, with 1 copy being off-site and 1 copy being offline, air-gapped or immutable. Additionally, a strategy mix of data and system-level backups for virtual machines will allow you to recover faster in case of a disruption.

DR plans and recovery workflows:
Utilise industry-leading tools and methodologies for DR planning and execution with a technology-agnostic strategy. Sophisticated DR management tools are available that support efficient recovery processes by ensuring a data-driven approach to setting recovery priorities, forecasting recovery time objectives (RTO) and managing resources. These tools also centralise DR technical information, preventing delays from siloed data. A structured Crisis Command framework ensures coordinated, effective operational responses, aligned with industry-standard crisis management methodologies for optimised recovery activities.

Disaster Recovery as a Service (DRaaS):
Disaster Recovery as a Service (DRaaS): Partnering with a trusted DRaaS partner provides your organisation with a safety net that catches you if something goes wrong. It helps get services back online fast after issues like a power outage or a cyberattack. It is not a one-stop solution; while DR might involve failover from one data centre to another, if a business's systems are cyber-compromised, a totally different recovery strategy may be required. This could involve recovery from offline data, such as traditional backup tapes, or utilising faster, immutable backups where such an investment has been leveraged. For example, a TV network might use DRaaS to ensure they're always broadcasting, even if a technical breakdown occurs, while a bookseller might opt for a simpler setup that keeps their inventory safe at a manageable cost.

Best practices for implementing a resilient infrastructure strategy

Some of the best practices we advocate for building a resilient infrastructure strategy include:

Data-driven DR with real-time reporting:
Our business continuity planning incorporates data-driven DR approaches that provide accurate insights for informed decision-making. Using best-in-class tools and central portals, we manage recoveries efficiently, provide accurate reporting and forecast for planned DR scenarios. This lets you manage your resources more effectively and meet your RTOs. Additionally, we provide accurate recovery reports which enable you to make confident, informed decisions and strengthen your continuity response strategy.

Efficient DR service delivery:
Using centralised Command and Control interfaces lets you streamline DR service delivery while lowering costs. Real-time recovery updates enable you to make critical decisions with confidence, ensuring minimal impact on operations and maintaining stakeholder trust during disruptions.

IT Service Continuity Management (ITSCM):
A tailored, consultative approach to ITSCM is required. It starts with assessing your needs and developing the right DR solutions. Establishment of a 'Managed DR Service` implementation and recovery process development (runbooks) is required. Managed DR Tests are essential, along with a controlled delivery process and post-test reporting. Managed DR Tests are used to flush out issues that can be remedied to optimize and validate DR strategies. Technical skills required for DR processes and resolving DR testing issues often require specific skill sets not regularly practiced as part of normal technical support operations, so experience and knowledge history in DR testing practices is a considerable asset in ensuring effective and efficient recovery.

Infrastructure as a source of resilience

A resilient infrastructure offers key business benefits. Disruptions are few and far between, but when they hit, they can make customers unhappy – in order to avoid this, Getronics can minimise downtime to technology, giving colleagues and customers alike a supported experience. There's no delay with Getronics either, we operate in real-time, meaning that reporting and forecasting are made as developments happen – you can make informed choices and prioritise our next actions. It's cost-effective, comprehensive and managed efficiently.

Chapter 5

Business continuity through digital workspaces

By embedding business continuity into your digital workspace strategy, you ensure productivity and security in hybrid and remote working environments, making them more resilient while also enhancing your business's resilience as a whole.

Key technical capabilities for resilient digital workspaces

To ensure resilient digital workspaces, here are some key capabilities to consider:

Privileged access management (PAM):

PAM involves limiting and controlling access to sensitive systems and data. This enables your organisation to enforce 'least privilege access' policies, which means users only have access to the systems and applications they need to do their jobs. This limits the risk of unauthorised access and potential breaches.

Multi-factor authentication (MFA):

This advanced identity and access management (IAM) feature protects digital workspaces by requiring users to provide multiple proofs of identity (such as a password, a mobile device, or biometrics) before they can gain access to your company's systems. This significantly reduces the risk of data breaches and fraud.

Centralised management:

Adopting centralised and secure methods for application deployments enables you to mitigate risks and reduce support costs compared to using a distributed management model.

Best practices for implementing a resilient digital workspaces strategy

Let's look at some best practices for making your digital workspaces resilient:

Dynamic working practices:
Implement flexible work policies and technologies that support secure remote work, while ensuring seamless collaboration and productivity, no matter if your employees are working in the office, from home or on the move.

Cyber-threat training, awareness, and response plans: Conduct managed training programmes that educate your employees about security and cyber threats. This enables them to identify and handle potential risks more effectively, with clear lines of reporting and best practices to apply.

Outboarding:
Properly outboarding users (systematically removing access and collecting company assets when employees leave) also helps maintain the integrity of the IT environment and ensures compliance with data protection regulations.
This contributes to business continuity by preventing sensitive data from being compromised in the first place.

Digital Workspace as a source of resilience

Embracing resilient digital workspaces is vital to your business's success in the age of remote and dynamic working practices.

Key benefits include:
Getronics can seamlessly collaborate with your workforce, boosting productivity. Colleagues thrive when they can work securely from any device, from any location, offering trust and flexibility. You can centralise management with a digital workspace and do so without massive costs. Digital workspaces are supportive, and technology focused environments, that make the working day run smoothly.

[7]SPOF : Single Point of Failure

Chapter 6

Business continuity through support

Lastly, business continuity should extend to your organisation's IT support. Support plays a vital role in maintaining a consistent user experience for your customers, employees and other stakeholders, even when a disruption occurs.

Key technical capabilities for resilient support

Some of the key technical tools and capabilities you can leverage to make your support operations more resilient include:

Cloud-based service desk and telecoms:
With a cloud-based service desk and telecommunications, you can ensure vital communication channels remain open, even if an on-site failure occurs.

Dynamic and distributed workforce:
Digital workspaces and cloud-based apps for your support teams allow you to implement failover options. In case of an outage in one location, you can seamlessly continue offering support services from other locations.

Augmented reality (AR) remote support:
This emerging technology leverages AR to enable experts to remotely guide on-site personnel or users through troubleshooting and repair processes. It facilitates real-time visual collaboration, allowing field experts to see what the on-site user sees through their device's camera and provide overlaid instructions directly on their view.

By ensuring expert support is accessible regardless of location, solutions like these enhance operational resilience and business continuity whenever critical equipment requires repairs.

Best practices for implementing a resilient support strategy

In addition to technical tools, resilient support relies on the right approach to training and staffing. Here are some best practices:

Continual training and cross-training:
Regularly update your training programmes to equip support staff with necessary skills, but also to be prepared in case of an incident that might impact their work. Cross-training (ensuring support employees have multiple skillsets to fill multiple roles when needed) allows you to operate more flexibly.

Language diversification:
Instead of concentrating all employees who speak a certain language in just one location, consider where applicable the need to ensure you have employees with the right language skills available at multiple locations in case of an outage or labour shortage that might impact client communications.

Understanding technical resource needs:
With pre-planned IT recovery scenarios, DR management tools and data from routine DR testing, it is possible to determine the technical resource pool size needed to respond to a disaster recovery event and meet business recovery objectives (e.g., RTOs).

Key questions to answer include:
What technical skill sets are required? How many people are needed to execute the recovery? Do you have enough technical resources, and are they properly trained and rehearsed in recovery practices? Identifying these needs allows you to address any gaps and enhance the team's resilience in responding to crises.

How support resilience benefits your business

By making your IT Support and operations more resilient, you deliver key business benefits, including:
You gain the ability to respond to events affecting one location in a flexible and effective way. Giving you the power to communicate clearly and in real time. By maintaining customer relations with Getronics support you offer a better experience to customers and team members, making solutions easier to provide.

- **The ability to respond flexibly and effectively to events affecting one location**
- **Ensuring uninterrupted support and communications in case of an incident**
- **Maintaining better customer relations and offering a better customer experience, even under challenging circumstances**

As with all of the best practices described in the sections above, Getronics also applies the recommended support best practices to our own operations. This is why, for example, our EMEA regional team is capable of immediately mobilising to support our APAC regional team in case of an incident affecting their operations. We also implement and routinely test various other reciprocal support solutions to ensure smooth, uninterrupted support and minimise the risk of communication breakdowns.

Chapter 7

The path to resilience: A consultative approach to business continuity

If you are an IT leader in the process of enhancing your organisation's technical resilience to ensure business continuity, it can be difficult to know where to begin. Some IT departments may lack the internal expertise, resources and time required to comprehensively identify all potential IT-related continuity risks, which makes it hard to define effective policies and mitigation strategies.
They may also lack experience or training in technical recovery on the scale required during a disaster. As a result, they face challenges outside of normal support practices and lack a planned, organised recovery strategy.

Business impact analysis and risk assessments

Often, organisations do not possess the capability to accurately evaluate the IT risks they face and how these might realistically impact their operations. This is why conducting a detailed business impact analysis (BIA) and risk assessment (RA) with support from experienced consultants is essential.

IT resilience and service continuity compliance

Business Continuity Management (BCM) and IT Service Continuity Management (ITSCM) involves assessing and evaluating your organisation's adherence to established Business Continuity and IT service continuity standards, guidelines and regulatory requirements. A rigorous BCM & ITSCM process helps identify areas for improvement, so you can select effective measures to achieve preparedness, a good response and a smooth recovery.

IT DR plan development and testing

This step involves creating, implementing, and reviewing strategies to ensure your IT systems can sustain operations during and after a disruption. It encompasses identifying potential IT threats, setting recovery objectives, and formulating response protocols. Regular testing of these plans through simulations and drills is crucial to ensure their effectiveness and readiness.

Crisis management and disaster recovery consultancy

Having a proven crisis management plan is vital when an incident occurs. This plan outlines the necessary actions for your organisation and establishes protocols for communication with customers, the public, and other stakeholders. Disaster recovery consultancy is critical to prepare for the rapid restoration of IT operations to normal levels as efficiently as possible.

Continual optimisation and realignment with business needs

An IT resilience strategy must adapt to your actual business requirements. Continuous monitoring and testing of your business continuity plans against real-world scenarios ensure they are robust enough to handle evolving risks and challenges. In IT resilience and business continuity, there is no one-size-fits-all solution. Key investments in IT can improve resilience, but a customised, thoroughly tested plan that addresses your organisation's specific needs is crucial.

DR is a subset of IT Service Continuity Management (ITSCM). An ITSCM plan outlines the preventive and management layers securing an application and infrastructure estate, while a documented DR plan details the strategy for specific recovery scenarios. Both plans provide assurance to auditors and stakeholders, but in practice, they involve implementing a technically detailed execution strategy.

A robust recovery solution also requires stringent change management controls to adapt to new applications, rebuilt infrastructure, migrations and business priority changes. Change management requests should include a risk assessment to determine the impact on the executable DR process and whether ITSCM/DR plans need updating.

Chapter 8 | **Conclusion:**

Resilient IT is the key to business continuity

IT is a frequent target of attacks which needs to be strengthened. At the same time, it is a shield that can effectively protect your organisation, as long as the right elements are in place. Resilient IT systems, along with a well-trained and prepared workforce, enable you to restore order as effectively as possible during disruptions, minimising downtime and ensuring compliance with regulatory standards. In addition to cybersecurity, resilience spans five core pillars of IT: security, cloud, infrastructure, digital workspaces, and support.

By integrating business continuity into every facet of your organisation's tech landscape, you enhance your ability to adapt to evolving challenges. The key to achieving resilient IT is strategic planning, collaboration and continuous improvement. The good news is that, you do not have to do it alone. Working with an expert consultative partner like Getronics helps you identify your organisation's unique risks, develop tailored solutions and implement robust DR plans that align with your business objectives.

By integrating the technologies and good practices outlined in this white paper and choosing suitable, proactive consultative partners, you set your organisation's IT on a path to greater resilience in our increasingly unpredictable world.

About business continuity IT consulting services from Getronics

Getronics is the home of innovation and expertise in Business Continuity Management (BCM), IT Service Continuity Management (ITSCM), and Disaster Recovery (DR). We offer IT consulting services that ensure your organisation is strong, and resilient, facing disruptions head-on, so that problems are solved before you notice them.

Our approach brings together advanced tools, with decades of experience, meaning that no matter which sector you operate in we have a service to uphold your standards. If you're looking for a partner in consultancy, compliance support, framework development, and customised programmes then Getronics is the answer. And we don't stop there either: testing strategies, cloud, IT infrastructure, and digital workspaces are on offer to you too.
Join with Getronics and we will create a diverse and bespoke support system, that keeps your business healthy.

Getronics take pride as a global leader in IT solutions. Our service includes a bespoke collection, made for you, that addresses all of your needs. Explore our extensive portfolios that offer up services like digital workplace which provides a working environment that uses technology to help colleagues work, collaborate, and socialise together. Business applications that build and transform relationships between people and technology. And infrastructure support – to maintain the high standards that you expect, and we deliver.

Getronics is a global leader in technology solutions with a team of over 4,000 colleagues in 22 centres, providing comprehensive end-to-end services across the globe.

getronics