Implementing World Class Business Continuity in KSA

Dhiraj Lal/Daman Dev Sood

CONTRIBUTE TO THE ACHIEVEMENT OF THE KSA VISION 2030

Many countries that had relaxed COVID-19 curfews and lockdowns and are now starting to re-impose them. Businesses may struggle again. This document recommends that all entities in the Kingdom, big and small, government and private, must quickly implement Business Continuity Management (BCM), which is already mandatory by regulation in many industries, sectors and geographies across the world. This would help ensure that come what may, the entity should be able to smoothly respond, without loss of reputation or financials, regardless of what caused the disruption. The value and the assurance that BCM provides would directly help KSA achieve its 2030 vision of being a reliable and preferred location to do business.

The authors of this whitepaper are both highly experienced and practicing BCM professionals. In this whitepaper, what they cover is:

1. What is Business Continuity
2. How the COVID-19 Pandemic is different from a typical BCM situation
3. The need for holistic BCM in the Kingdom
4. The SAMA Minimum Business Continuity Framework – A KSA Best Practice
5. How to implementing world class Business Continuity in the Kingdom

Section 1

What is Business Continuity

Within KSA also, as across the world, the COVID-19 Pandemic has been a wake-up call. In general, those entities that had an effective Business Continuity Management System (BCMS) in place experienced much lesser downtime and were able to protect their reputation and quickly recover and deliver their critical products and services to their stakeholders and interested parties. Most unprepared organizations struggled. Many entities that have since shut down, never to reopen - typically those that did not have an effective Business Continuity Management System.

Business Continuity Management is defined as a "comprehensive management process, which highlights possible threats and the impact of such threats on the business operations of the organization." The rationale is that advance identification of threats assists organizations to proactively implement controls and develop resilience toward these threats. These organizations would be able to also keep ready their backup plans, to continue to provide their time-sensitive and urgent services within reasonable timelines, in the event of a disaster. This advance preparedness helps protect the interests of stakeholders, brand name and reputation.

To give an example, most of us would expect our telecom provider to provide uninterrupted service at all times. We would simply not accept it that our internet or mobile services be "down," for any reason whatsoever. This is one reason why STC, Mobily, Zain and others have dedicated staff trained and experienced in Business Continuity, so that if there was any incident that caused a disruption (such as fire, a data corruption, breakage of equipment, default by a key supplier, loss of key staff, inability to operate from their office, Control Room or Data Centre, any other reason), they would very quickly be able to restart delivery.

The zero downtime expectation is also the case with other industries such as Power, Water and Electricity, Airlines, Airport, Govt Online payments, Banking, Insurance, and many others, such as Oil & Gas, Manufacturing, Trading, Retail and other sectors. In fact, there may be no industry at all where customers would normally happily accept downtime. Also, those organizations that are often "down" who suffer due to loss of reputation and transaction volumes. For example, if there was any airline whose flights were frequently cancelled or delayed, then customers would most likely stop flying that airline even at the cost of paying more for a better airline. If so then the "delayed" airline may lose market share and revenues, and may even have to shut down.

Based on the above example, which is backed by common-sense and human nature, it is well agreed that Business Continuity readiness helps organizations to effectively respond to unforeseen disaster situations, without losing reputation or market share. As is very logical, there is every chance that organizations that are unable to quickly or professionally respond, may:

- Lose customer trust, faith, confidence and goodwill
- Fail to meet legal, regulatory, national or customer contractual commitments
- Let down their customers, employees, partners and the community, and any others who depend on them

- Be faced with reputation issues with customers and the public, and be exposed to embarrassment, and the need to give explanations to explain their unprofessionalism
- Find their critical and valuable assets destroyed or damaged, leading to needless expense and time delays which may further disrupt operations
- Be levied with fines, penalties, lawsuits and other undesirable actions
- In a truly competitive situation, lose market share, revenues and profits
- Eventually have to shut down, as was the experience of around 550 of the 930 organisations that were directly affected by the 9-11 disruptions.

It is said that organizations that suffer a significant disruption on an average may witness:

- 7 percent lower sales growth
- 11 percent growth in cost
- 107 percent decrease in net income

This is aside from the possibility of closure. Keep in mind some often quoted statistics that:

- Around 40% of businesses experiencing a disaster never re-open. Of those that reopen, almost 30% close within 2 years
- Of around 930 companies in the WTC towers on Sept 11, over 550 had failed 18 months later (59%)
- Businesses can be destroyed by the loss of a critical resource more than 10 days

Formal implementation of BCM helps force organizations to think what incidents may cause disruption in delivery of their products or services, and be ready with suitable response plans, which can in advance be tested, practised and improved. This would help organizations respond quickly and effectively, thus avoiding many of the negatives pointed out above. As they say, the time to buy an umbralla is not when it rains, but before. If you wait till it rains, it would be too late.

Importantly, Business Continuity is not just a defensive or protective strategy, but is actually a revenue-generator, just like any other. This is because there is every chance that organizations that have effective Business Continuity in place may *gain market share* in a disruption, because they responded more quickly or professionally than any of their less prepared peers or competitors.

Section 2 How the COVID-19 Pandemic is different from a typical BCM situation

Business Continuity typically is characterized by situations where the organization is unable to deliver its key products or services due to lack of availability of some important resource category. For example, if there has been a fire in a factory, then the building may not be available, including all its equipment, technology, hard copy records, raw materials etc. So obviously it may not be able to produce the goods as normal. If their IT is disrupted, then the computing capacity may be limited. If the office records are unavailable or the 2 people who have to open the lock together (dual control) are not available then the vault cannot be opened.

In all the above cases, due to lack of availability of the needed resources, the organization may not be able to deliver its products or services in the timelines or quality as committed.

The above scenarios are what traditional Business Continuity typically provides advance solutions for. But the COVID-19 provides a new BCM scenario, not encountered by many in the recent past, a scenario that most BCM organizations have not practiced actively or tested for on a regular basis. Some differences of a typical BCM situation are that the COVID-19 situation:

- Involves most of their staff often working from an alternate location – in many cases their homes. Whereas in a traditional BCM situation, it has been typically only around 20-30% staff working from the backup site for a few days at most.
- Has lasted for a very long duration – and still more time to go before things come back to Business As Usual (BAU). In fact, things may never come back to BAU – they may come back just to the "new normal"
- Provides currently no clarity on final resolution. Whereas traditional disruption situations often last just for a few hours or days
- Had little use for the typical traditional business continuity solutions (backup site/ backup technology/ backup utilities/backup people)
- Caused severe capacity issues due to limited availability of IT resources, network bandwidth, ergonomic work infrastructure etc.
- Has seen the entire ecosystem impacted, including supply chain, which has been a big cause of service disruptions and outages.
- Has witnessed severe security and legal liability issues, including a huge increase in cyber-attacks, ransomware demands, phishing etc.
- Had to contend with severe mental health and psychological issues, due to the current cooped-up "pressure cooker" environment. This is a new dimension, often not considered – more than just people unavailability.

The above are some factors that make the COVID-19 scenario different from traditional Business Continuity Management. It is clear that while the COVID-19 Pandemic caused huge business disruptions, the need to invoke Business Continuity was triggered initially not by damage to resources, but by the need for social distancing. There was no major resources availability issue.

In fact, while a statement has been made that the COVID-19 is a "Black Swan" event, the reality is that it is not. According to Nassim Taleb, author of the "Black Swan", a Black Swan event has three attributes:

- The magnitude impact of a black swan event could be huge
- It lies outside reasonable regular expectations. Nothing in the past can convincingly indicate to the possibility of it occurring
- Even then, if and when it occurs, we may typically create explanations to rationalize its occurrence, as if it could be easily explained as being predictable and logical.

But contrary to the points above, it is well-known that pandemics have ravaged the world periodically. Probably SARS was the first infectious disease disaster in current memory, though quite a while back, and H1N1 more recently. So clearly, the COVID-19 global pandemic was not an unimaginable, unpredictable "Black Swan" event. Instead, the reality is that most of us chose to ignore this "high consequence, low-probability" event.

Therefore, the COVID-19 is not a "black swan", but we can certainly refer to it as a wake-up call.

So with respect to Business Continuity readiness in the Kingdom, what next do we do?

Section 3

The need for holistic BCM in the Kingdom

Most countries around the world have decided to live with the COVID-19 Pandemic, in an atmosphere of Business As Usual – and the Kingdom is no exception. Many countries had relaxed lockdowns and social distancing, and businesses had started reopening. Some economies are already showing signs of recovery from COVID-19 Pandemic restrictions. All this is due to the challenge – do we protect lives, or do we protect livelihoods? Ideally both!

But the pandemic is not yet defeated, and it is too early to sit back and relax. There are many other threats and dangers also, that might come your way. If not today, then tomorrow. Your plan to ensure business continuity during COVID-19 Pandemic might not work for other threats and disruptive events. In this pandemic, your primary objective was to save your people. But are you confident that you would be able to continue your business and protect your other assets in case a different disaster strikes, such as a cyber-attack, water-logging, fire or explosion, missile attack, data breach, or key supplier outage? If not, then it is the right time to put in place a comprehensive BCMS. This is relevant to all KSA entities, such as ministries, governments, businesses, schools, colleges and universities etc. They all have an obligation to be resilient, and it is typically the responsibility of the Board of Directors to ensure this readiness. The question to all organizations is:

- What would happen if a new disruption came along, in addition to the current situation? Would you be able to withstand it without suffering afresh? Have you put in place the needed "horizon scanning" to keep a constant eye on any new and emerging risks or threats?
- Do you have the needed availability and protection for all categories of resources, including People, Data, Value-creating Processes, Vital Records, Communications, Assets, Brand & Reputation – and also ensure financial resilience?
- Have you identified what risks and threats could disrupt your business? Have you established these risk levels as acceptable to you? Have you put in place the needed controls to mitigate and reduce the impact to levels that you are comfortable with?

- Have you determined the timelines for recovery of all your key products and services? Have those timelines been validated with your important stakeholders and interested parties?
- Have you focused also not just on products and services, but also communications? Could the loss of your communications system for even 1 day damage your revenues and business model? Particularly in today's environment where anyone can say anything on social media, which can create a reputation issue for you.
- Do you have documented Business Continuity Plans of how you would respond and recover within timelines, without reputational impact, in the case of any fresh business disruption?
- Have you tested, reviewed, maintained and improved your plans, and are you confident that they give you the holistic ability to anticipate, respond and recover within timelines?

Unless you have comprehensive business continuity plans in place to manage all scenarios, you may struggle again to survive. This is where Business Continuity readiness helps.

Business Continuity Management is typically implemented by identifying potential threats to an organization, and the impacts to the business operations those threats, if realized, might cause. A framework for organizational resilience is then built, with the capability for an effective and timely response. The objective is to safeguard the interests of the key stakeholders, reputation, brand and value-creating activities. This preparation is best done well in advance

Given KSA's leadership in the global economy, implementation of Business Continuity is perhaps even more important in KSA than in some others countries. Already, the Kingdom of Saudi Arabia is the largest exporter of oil in the world and among the 20 largest global economies. By 2030, Saudi Arabia intends to be a global leader in other selected sectors also.

Per its Saudi Vision 2030 document, the Kingdom has already unveiled how it plans to achieve this goal. The Saudi Vision 2030 is built on three pillars, namely a *vibrant society, a thriving economy, and an ambitious nation*. Through its vision of "A Thriving Economy", Saudi Arabia aims diversifying the economy in the country beyond the oil and gas sector, and bringing large investments in other sectors. The Saudi Vision 2030 aspires to make Saudi Arabia the market maker in selected sectors, as well as a leader in competitively managing assets, funding and investment, and to be recognised as a globally preferred destination for businesses to operate in.

Almost certainly, in order to fully support the Saudi 2030 vision, all entities in Saudi will have to demonstrate effective Business Continuity readiness. It would simply not be acceptable for Saudi-based entities to allow unexpected events to cause business disruptions and failure to deliver their committed products and services within reasonable timelines.

So while Business Continuity is not currently mandated across all sectors of the Saudi economy, this is something that should be considered, as some other nations have already done across the world. Making Business Continuity mandatory for all Saudi entities would very quickly ensure that all recognise the need to protect the reputation of the Kingdom through flawless delivery and meeting of commitments.

Section 4 The SAMA Minimum Business Continuity Framework – A KSA Best Practice

The good news is that Business Continuity is not a new concept for KSA . Many entities in the Kingdom have already implemented high quality BCM Programs, and in many cases, that readiness has delivered full value during the COVID-19 Pandemic. Many of these entities in KSA have implemented BCM in line with the global BCM standard ISO 22301, developed by the International Organisation for Standardisation, and have got ISO 22301 certified also, as proof of competence.

However, KSA entities have another option, which is the excellent SAMA BCM framework, released in 2017 by the Saudi Arabian Monitory Authority (SAMA). The expectations mandated in this framework are based on SAMA requirements, considering also international standards such as ISO 22301, ISO 27001, and also good practices and professional guidelines from the UK-based BCI (Business Continuity Institute) and the US-based DRII (Disaster Recovery Institute International).

The SAMA minimum Business Continuity Framework is a KSA Best Practice. The SAMA framework is extremely well developed, certainly one of the most comprehensive BCM frameworks in terms of its expectations. The principles advocated in the SAMA framework are based on well-known and appreciated BCM learnings, tried and tested. Its intent has been to ensure 24×7 continuity and availability of business operations in the case of any disruptive event to financial service entities in the Kingdom (primarily Banks and Insurance companies). The SAMA Framework sets expectations both in terms of Business Continuity Planning (BCP) and IT Disaster Recovery (IT DR) Planning. Per the SAMA document, IT DR (which includes policies, standards, procedures and processes pertaining to resilience, recovery or continuation of technology infrastructure supporting critical business processes) is part of Business Continuity.

While the target of the SAMA framework has been to enhance the resilience capabilities of financial institutions in the Kingdom, there is nothing that prevents other entities and sectors in KSA from using this excellent BCM document for their own guidance. The key principles of the SAMA framework are valid for other industries also, not just financial services. While the ISO 22301 is generic and global, so has no option but to be high-level, the SAMA framework is designed to be implemented in the Kingdom, and so is KSA-specific.

It is highly recommended that entities looking to implement BCM in KSA consider implementing their BCMS in line with the SAMA framework, to the extent possible. Those who need can visit http://www.sama.gov.sa/en-US/Laws/BankingRules/BCM%20framework.pdf to access the SAMA BCM framework document. As the name says, this provides the minimum expectation – those who want should consider doing even more.

Section 5

How to implement world class Business Continuity in the Kingdom

For any KSA organization, one logical and immediate step would be to capture their COVID-19 Pandemic learnings and incorporate them into their own BAU, response and recovery plans, where possible. And for those who do not have a formal or comprehensive BCMS in place, it is highly recommended to immediately fix this dangerous gap. The typical cycle for BCM implementation is:

Figure 1: Typical Steps in BCM Implementation

The steps above are reasonably in line also with the SAMA framework document. Some of the key highlights of the SAMA Business Continuity framework document are that it:

- Defines principles, objectives and control considerations for initiating, implementing, maintaining, monitoring and improving business continuity controls in its member organizations.
- Mandates that the Board of directors or a delegated executive member is expected to have the ultimate responsibility for the BCM program.
- Expects that a BCM Committee should be established and mandated by the board of directors.
- Specifies that the audience to ensure BCM implementation is the Board of Directors, CEOs, Chief Risk Officer, Senior and Executive Management, Business Owners, Owners of information assets, CIOs, CISOs, Business Continuity Managers, Internal Auditors and those who are responsible for and involved in defining, implementing and reviewing business continuity controls.

- Is applicable to the full scope of organizations, including subsidiaries, employees, subcontractors, third parties and customers.
- Recognizes the interrelationship with other related areas, such as enterprise risk management, health, safety and environment (HSE), physical security, and cybersecurity (including cyber resilience and incident management).
- Standardizes definitions such as Maximum Acceptable Outage (MAO), Recovery Time Objective (RTO), Maximum Business Continuity Objective (MBCO) and Recovery Point Objective (RPO), to prevent any misunderstanding

Some key expectations mandated by the SAMA BCM framework document are that:

- All Member Organizations are required to comply with these requirements and integrate it formally in their BCM program.
- Senior management, such as CRO, COO, CIO, CISO, BCM manager and other relevant departments should be represented in the business continuity committee.
- A BCM function should be established. A BCM manager/ head should be appointed, and must have appropriate authority to manage the BCM Program
- A business continuity policy should be defined, approved and communicated to relevant stakeholders.
- Organizations should perform a business impact analysis to identify and prioritize the activities (i.e. products, services, business functions and processes).
- The BCM committee should endorse the prioritized list, BIA results, RA and the defined RTOs, RPOs and MAOs.
- Organization should periodically perform a Business Continuity Risk Assessment. It should include, but not be limited to identify potential internal and external threats. The Risk Assessment should identify single point of failures that may cause disruption to critical activities, considering people, process, technology and premises
- The risk assessment should include risks associated with overall organization as well as data centers (primary and alternative), which are not owned by the Member Organization (likely to be third-party owned or outsourced)
- Relevant cyber security requirements, if any, must be included.
- The organization must define a risk treatment plan and implement BCM controls.
- The business continuity strategy should be defined, approved, implemented and maintained.
- Capability of vendors, suppliers and service providers to support and maintain service levels for prioritized activities during disruptive incidents should be assessed at least on a yearly basis.
- A BCP should be defined, approved, implemented and maintained in readiness for use during disruptive incidents, to enable the Member Organization to continue delivering its important and urgent activities, at an acceptable pre-defined level. Procedures should collectively include key resources (e.g. people, equipment, facilities, technologies) and a process to continue the critical activities within predetermined recovery objectives (RTO, RPO and MAO).
- The Organization should define, approve, implement and maintain an IT Disaster Recovery Plan (IT DRP) to recover and restore technology services and infrastructure components (Data, Systems, Network, Services and Applications) in alignment with the Business Impact Analysis.

- Data, system, network and application configurations, and capacities in the alternative data center should be commensurate to such configurations and capacities maintained in the main data center.
- Formal contracts should be signed with third parties to ensure the continuity of outsourced services or delivery of replacing hardware or software within the agreed timelines in case of a disaster.
- Timelines and expectations of contracts signed with external service providers must be aligned with the BIA and RA outcomes as signed off by the organization's Top Management.
- For all critical activities, as determined by the BIA, the Member Organization should ensure that the key service providers have a BCP in place and their plans are tested at least on a yearly basis.
- The Member Organization should define, approve and implement a Crisis Management Plan (CMP) that would facilitate a well-managed response for major incidents, including rapid communication to ensure overall safety to both internal and external stakeholders. Typically the CMT consists of members of Top Management and is their responsibility. Representatives of the critical products, services, functions and processes (including Communications department) should be considered as members of the Crisis Management Team (CMT).
- A formal communication plan should be created to address the communication with the internal and external stakeholders during crisis - including the media response plan. Guidelines must be specified for communicating with employees, relevant third parties and emergency contacts.
- Organizations should define, approve, implement, execute and monitor regular BCP and DRP tests to train their employees and third parties and test the effectiveness of the BC and DR plans.
- BCP simulation test exercises should be conducted at least once a year. The effectiveness of the IT DRP should be measured and should be evaluated on a yearly basis as minimum. IT DR tests should be combined with the BCP test at least once a year. Cyber security scenarios should be considered also. Tests should also cover the activation and involvement of the CMT.
- All BCP and DRP tests results should be reported to the BCM Committee, Top Management and the Board of Directors.
- The Member Organization should identify the improvements based on the tests performed and provide an action plan to SAMA within two months after the submission of the test results.
- A training program should be provided once on an annual basis to employees involved in BCM to achieve the required level of experience, skills and competences. (Note - In today's "social distancing" scenario, a good way to provide this "all employee" annual awareness could be via eLearning. Since eLearning can typically be accessed anywhere and at anytime, this would also facilitate repetitive sessions that would enable the eventual appreciation of the needed BCM concepts, including roles and responsibilities of all in the organization to support effective BCM)
- The Organization's BCM should be subjected to periodically reviews and audits by a qualified independent internal or external party that must report independently the identified gaps along with road map to senior management and the BCM committee.
- The Internal Audit should provide a reasonable assurance on the executed activities, test results and to observe if the executed tests are meeting the Member Organization's overall Business Continuity program objectives.
- The BC and IT DR program, policies, plans and procedures should be reviewed and updated periodically, and in case of (major) change in the critical products, services, business functions and/or processes.

As most BCM professionals would agree, the above expectations are quite comprehensive and well in line with global good practices. This confirms the point made earlier – that the SAMA framework is worth being considered to be used as a guiding document for other KSA entities also - even those not in the financial sector.

Other principles worth being followed for world-class Business Continuity in the Kingdom are:

- Once you have implemented your BCM Program, don't stop there. Implement also the rest of the Resilience components – which would include Crisis Management, Risk Management, Information Security, Cyber Security and Data Protection etc.
- Organizations that do not have a formal Risk Management System in place should urgently consider implementing. The ISO 31000 is a good Risk Management framework to use. The pandemic showed us how organizations may suffer if they do not have advance preparedness or horizon scanning in place. The pandemic crept upon the world and paralyzed many organizations. Not many saw this coming. Learning from this mistake, at least you should now make sure that you don't allow other risks, threats and vulnerabilities to cause you business disruptions or loss of revenues, profits or reputation.
- Same is the issue with Crisis Management. The SAMA Framework already mandates organizations to have a documented and tested crisis management plan ready at all times. The fact is that Corporate Governance demands advance planning and preparedness, rather than for Leadership Teams to allow themselves to be surprised by unexpected scenarios or evolving incidents which could eventually break the organization. It is suggested that the BS 11200:2014 Crisis Management Standard could be used to develop a Crisis Management framework that can be used by organizations to be able to anticipate and effectively respond to crisis situations.
- Organisations looking to implement would be smart to allocate their best and smartest people to the BCM initiative. BCM can help your organisation survive a disaster that may otherwise put it out of business. For commercial organisations, BCM can help increase revenues and profits.
- Once your best people have been allocated, do provide effective training in advance of the implementation. Just as you would never allow an untrained driver to drive an ambulance to take your loved ones to the hospital, or an untrained doctor to conduct the surgery, in the same way you would be asking for trouble if you were to ask your teams to implement BCM without being first sure that they have the needed understanding and competencies (evidence of which can be prior training, education or experience). To be more assured, get your people BCM certified – which means that they sit for a BCM exam and pass it. FQA UK, Exemplar, IGC, CORE, DRI and the BCI provide certification cousres that are well-recognised and appreciated. BCM Professional certification exam charges vary widely – those interested can choose the BCM certification course that matches the cost that they are willing to pay.
- Consider also for your organisation to be ISO 22301 certified – as many entities in KSA have chosen to be, such as SABIC, Arab National Bank, and many others.
- Whether certified or not, ensure continual improvement of your BCM, Crisis, Risk and other implementations via the PDCA - Plan, Do, Check, Act cycle. Set a goal that every day, your Management System must be better than it was the previous day.

Summary

Just as many entities have done globally, all entities in the Kingdom, big and small, government and private, would be smart to ensure formal and comprehensive implementation of Business Continuity. This would help ensure not only the survival and growth of the organisation, but also would directly support the 2030 vision of KSA to be a reliable and globally preferred destination to do business.

The SAMA Minimum Business Continuity framework is an excellent KSA Best Practice, which is very detailed and comprehensive. While the SAMA framework is directly relevant to Financial Services, other KSA entities in other sectors can also be guided by it. Others who are looking for an internationally recognised framework may consider the ISO 22301:2019. Organizations that want ongoing assurance of their BCM readiness at all times may choose to get the staff or their organization ISO22301 certified through globally respected entities.

Dhiraj Lal, Executive Director
MBCI, CBCP, ISO27001 & 22301 Technical Expert, Assessor and Lead Auditor, ISO27001, CISA, ITIL
Contributing Author to the "Definitive Handbook of Business Continuity 3rd Edition" – John Wiley & Sons

Daman Dev Sood, Chief Operating Officer
FBCS, FBCI, CBCI, SMIEEE, MAIMA, ISO 22301 LA & Expert, IEEE Ambassador
Author of the "Step by Step guide to the NCEMA 7000: Implement BCM the UAE way"

Tarun Bhandari. Chief Administrative Officer
Lean Six Sigma Certified, ISO 31000 Risk Management Specialist

CORE is in the BCI UK Hall of Fame for being a 4 time winner of the Service Provider of the Year regional award!

BCI MIDDLE EAST AWARDS 2019 WINNER

BCI INDIA & SOUTH ASIA AWARDS 2019 WINNER

For more information, contact:
Email: info@continuityandresilience.com
WhatsApp : +971 50 576 7804
Phone: +971 2 659 4006
+91 9958091880

Continuity & Resilience (CORE) provides services in

- Business Continuity Management (BCM), Information Security
- Cyber Security
- GDPR
- Risk Management
- Crisis Management
- IT Service Management and Disaster Recovery
- Leadership and soft skills

In these areas we provide services like:

- Consulting and Implementation
- Testing, Assessment, Assurance and Annual Audits
- Training and Professional Certification

We provide advisory services in

- Automation Tools (BCM, ITDR)
- Mass Communication
- e-Learning products
- Workplace Recovery
- Documentation Resilience Management and Effective Collaboration