ADVISORY GUIDELINES ISSUED BY

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ON

RESILIENCE AND SECURITY OF DATA CENTRES

25 FEBRUARY 2025

ADVISORY GUIDELINES FOR RESILIENCE AND SECURITY OF DATA CENTRES

1 Introduction

1.1 Digital infrastructure underpins Singapore's Digital Economy by:

a. Enabling seamless connectivity that drives Singapore as a global hub, and accelerates our economic growth through digital industries and businesses[1]; and
b. Powering the digital services in our everyday lives, ranging from digital banking[2] to ride-hailing to e-commerce.

1.2 Digital infrastructure, in particular the compute infrastructure such as Cloud and Data Centres ("DCs"), has become integral to Singapore's economy. Compute infrastructure supports our daily work and lives, and our reliance on it will increase with digitalisation. Resilience and security of the compute infrastructure are important given the systemic impact of failure. While compute infrastructure operators already promote resilience and security as part of their core value proposition, service incidents do occasionally occur, which can lead to significant impact on the economy and undermine user confidence.

1.3 The Advisory Guidelines for Resilience and Security of Data Centres ("Guidelines") set out guidance on best practices on the resilience and security of Singapore's compute infrastructure, covering how DC operators ("DCOs") can manage resilience and security risks of DCs by planning for business continuity and adopting appropriate and proportionate mitigation measures. While the Guidelines are for voluntary adoption, DCs are encouraged to adopt the Guidelines, as this will not only uplift their own resilience and security posture, but also distinguish themselves in the competitive market. This will also instil greater confidence in DCs' users that the digital infrastructure that their businesses rely on is resilient and secure. These Guidelines will be updated regularly to incorporate industry and technological development, learning points from incidents, as well as industry feedback.

2 Key risks for the resilience and security of DCs

2.1 The key risks for the resilience and security of DCs are in 3 main areas – DC infrastructure, Governance and Cybersecurity.

2.2 **Infrastructure Risk**. These are risks stemming from insufficient consideration of risk in the design of DCs. The key risk areas are:

a. Power management – e.g., risks of power disruption caused by inadequate power redundancy during planned maintenance or inadequate lightning protection leading to power outage;

[1] Our digital economy is about 17.7% of Singapore's GDP in 2023. Source: Singapore Digital Economy Report 2024 by IMDA.

[2] For example, e-payment transactions in Singapore increased by ~50% from 2017 to 2022, to $127B. Source: MAS Retail Payment Statistics, 2017 and 2022.

b. Environmental control management – e.g., risks of loss of cooling due to inadequate redundancy within environmental control systems to ensure continuous cooling;
c. Cable management – e.g., risks of loss of network connectivity due to insufficient bend radius resulting in damaged cables;
d. Facilities/tenant space protection – e.g., risks of unauthorised access due to inadequate physical controls, and fire due to inadequate fire detection and suppression systems; and
e. Building site and design suitability – e.g., risks of water intrusion into the DC due to lack of protection against environmental risks such as flooding.

2.3 **Governance Risk.** These are risks stemming from insufficient risk oversight of DC operations. The key risk areas are:
a. Operations management – e.g., risks of power or cooling failure due to inadequate monitoring [3] of DC infrastructure elements such as power supply and environmental control systems;
b. Incident management – e.g., risks of prolonged service disruption due to poor incident management response and service recovery processes; and
c. Change management – e.g., risks of unauthorised change[4] due to weak change management processes.

2.4 **Cyber Risk.** These are risks of cyberattacks on DC operating systems and controls – e.g., risks of data centre infrastructure management systems being compromised which may result in unauthorised temperature changes due to inadequate cybersecurity control measures.

2.5 To manage the risks in DC infrastructure, Governance and Cybersecurity, DCOs should plan for business continuity when incidents happen and disrupt critical services to their customers. DCOs should implement a business continuity management system ("BCMS"[5]) to enhance their resilience against unforeseen disruptions and ensure service continuity. DCOs should adopt a continuous process loop of Plan, Do, Check and Act to implement, maintain and continuously improve resilience and security measures. DCOs should establish objectives, policies, procedures and processes to achieve business continuity targets ("Plan"), implement and operate BCMS ("Do"), monitor and measure BCMS' performance and conformance ("Check"), and take corrective and preventive actions to improve BCMS performance ("Act").

[3] Alternative monitoring should be implemented by DCOs in an event where the primary monitoring system is affected or made unavailable by the planned maintenance. This is to ensure there are no periods of time where important events and alarms from underlying DC infrastructures are masked due to the unavailability of the monitoring system for the duration of the planned maintenance.
[4] Strong adherence to approved changes should be enforced to ensure that no unplanned or unauthorised changes are made in parallel to a planned approved change. Any deviation or modifications made to an existing approved change should be approved by the change advisory board.
[5] BCMS is a management system that encompasses processes, procedures and rules to ensure that critical business services remain operational during planned or unplanned disruptions, and continuously develops and improves them.

3 Managing resilience and security risks of DCs

3.1 The "Plan" process establishes the scope and policies of the BCMS, obtain top management support to be executive sponsors, and identify what critical products and services to protect from business disruptions. DCOs should:

a. Establish clear business continuity policies that outline the objectives, scope and responsibilities. The policies should align with DCOs' organisational goals and regulatory requirements;
b. Determine the scope of the BCMS. DCOs should identify critical business products and services (e.g., power, cooling, connectivity), define the extent of the BCMS, its mission, goals, and internal and external obligations;
c. Obtain support and involvement from top management on the business continuity policies to ensure that resources for BCMS are available, roles are assigned and communicated. DCOs should ensure that BCMS achieves its intended outcomes and promote continual improvements to it;
d. Update the BCMS accordingly when changes (new products (e.g., Lithium-ion batteries), suppliers, business model, etc.) are introduced to the business. This should include the purpose of the change and their potential consequences;
e. Ensure that resources are allocated to support the establishment, implementation, maintenance and continual improvement of the BCMS. People should have the right competency and training to support the BCMS; and
f. Ensure that people involved in the BCMS are aware of the policy, their own roles and responsibilities before, during and after disruption. DCOs should also determine what will be communicated, when to communicate, with whom to communicate, how to communicate and who will communicate for internal and external communications.

3.2 The "Do" process implements and operates the business continuity policy, controls, processes and procedures. This involves several steps to understand, plan and test for business continuity events. DCOs should:

a. Conduct business impact analysis to identify critical business functions and the potential impact of disruptions. DCOs should identify the maximum tolerable time frame in which the impact of service disruption becomes unacceptable to their customers;
b. Conduct a thorough risk assessment to identify potential threats and vulnerabilities, both internal and external. DCOs should evaluate the consequences of those risks occurring as well as their likelihood and apply appropriate risk treatments for each identified risk;
c. Implement a range of business continuity strategies and solutions to reduce the likelihood or shorten the duration of service disruptions. Examples include redundant power supplies, lightning protection systems, fire detection and suppression, cybersecurity measures against ransomware, etc.;
d. Develop detailed response and recovery plans which specify the actions to be taken during and after a service disruption to restore normal operations quickly. DCOs may implement and maintain an incident response structure (assessment, activation, action) to provide an effective response in case of an incident; and

e. Ensure that their employees (and/or suppliers) who are involved in BCMS are trained and prepared to respond effectively during an incident. DCOs should conduct regular testing and exercise to ensure the business continuity plans are effective and relevant. The exercises help to identify any gaps in the plans, improve preparedness, and ensure that employees (and/or suppliers) are familiar with their roles during a service disruption.

3.3 The "Check" process monitors and reviews performance against the established BCMS' goals and objectives. The results of the assessment should be presented to top management for review. DCOs should:

a. Establish key performance indicators to measure the performance and effectiveness of the business continuity strategy and ensure continuous alignment with organisational objectives;
b. Conduct regular internal audits, reviews and feedback sessions to identify gaps and areas for improvements on the BCMS; and
c. Ensure that top management reviews the organisation's BCMS regularly to ensure its relevance, adequacy and effectiveness.

3.4 The "Act" process maintains and improves the BCMS by taking preventive and corrective actions based on the results of management review, and updating it to align to management's expectations. DCOs should:

a. Foster a culture of continuous improvement by addressing non-conformities and implementing corrective actions;
b. Review the effectiveness of any corrective action taken; make changes to the BCMS, if necessary; and
c. Keep abreast on evolving threats and technologies that may cause service disruptions and update their BCMS accordingly.

3.5 DCOs could refer to international standards such as the ISO 22301, ISO 27001/2, ISO 31000, ISO 22237 and TIA-942 for specific measures to adopt as part of their BCMS.

4 Additional measures to manage cyber risks

4.1 In addition to the above, DCOs should prepare for and manage the risks of cyber threats (e.g., supply chain attacks, malware attacks, ransomware, etc.) effectively in the key risk areas based on each DC's business and operational needs and ensure adequate cybersecurity control measures are in place for its network and system. DCOs should:

a. Establish, maintain and continuously improve an Information Security Management System that is approved by their management with clearly defined roles, responsibilities and coordination of information security policies and standards. DCOs should ensure that auditable entities are established and updated periodically such as reviewing the scope of audit, determining the effectiveness of the audit scope, etc. There should be designated primary and backup personnel who are information security liaisons as the point of contact with local authorities and are contactable by the customers. DCOs should also establish and document an acceptable use policy for critical and new technologies, services and end-user

devices (e.g., wireless technologies, laptops, mobile devices) in accordance with industry standards, and is communicated to all relevant employees and third parties;

b. Ensure that all employees and third parties are suitable for their roles prior to employment or contract and that they understand their responsibilities, employment and contract and conditions (including termination) to reduce the risk of theft, fraud, or misuse of facilities. DCOs should perform background checks in accordance with applicable ethics and contractual obligations. DCOs should ensure all assets owned by the organisation are duly accounted for and returned by employees and relevant third parties. DCOs should establish and implement an information security training and awareness programme for employees and relevant third parties upon hire and review at least annually;
c. Ensure that they have an effective control framework over their third-party service providers supporting them that includes third party service providers due diligence, agreement, delivery management, assurances over their performance and compliance with internal controls. DCOs should develop and maintain risk management procedures, overseeing the risks and impact arising from third-party service. DCOs should also ensure that open-source components are safe to use, to protect against cyberattacks via software supply chain[6];
d. Ensure that they and their third-party service providers conform to DCOs' information security and risk management policies, standards, procedures and contractual obligations through regular reviews. DCOs should establish procedures, training or awareness, and relevant policy enforcement actions to deter or prevent employees from unauthorised access, and enforcement of commercial agreements with relevant third parties and end users with acceptable use policies or agreements. DCOs should ensure the use of cryptographic controls are compliant to relevant agreements, applicable laws and regulations;
e. Ensure that activities performed, and events occurred in their network and systems are being tracked and maintained for a period of time to allow detection of any unauthorised activities and to facilitate investigation and resolution in the event of security incidents (e.g., access violations). DCOs should ensure that audit trails of network and system activities are logged, protected and reviewed periodically;
f. Ensure that their network and systems are designed and configured securely to prevent against unauthorised entry points or malicious activities through weak system configurations. DCOs should develop configuration standards, implement controls against malicious code threats, ensure timely application of security patches, restrict and control use of utility programs, implement controls to restrict the use of unapproved or unauthorised software, etc;
g. Conduct security testing and implement monitoring controls across its network and systems to detect vulnerabilities and malware in a proactive and timely manner. DCOs should conduct internal and external vulnerability scans, network and application layer penetration testing from the Internet when there are

[6] DCOs should ensure third party open-source components are safe to use, to protect against cyberattacks via software supply chain.

significant changes in the infrastructure, applications or modifications or at regular intervals;

h. Establish policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities to ensure that security is an integral part of the information systems as well as the business processes associated with these systems;
i. Implement encryption and secure cryptographic key management to ensure that sensitive information in transmission or in storage electronically are being protected against unauthorised use or disclosure. DCOs should establish key management procedures to address all components of the key management life cycle (i.e., generation, distribution, utilisation, storage, archiving, replacement and destruction of the keying material);
j. Implement administration controls to ensure the enforcement of policies, standards and procedures relating to the creation, maintenance and removal of privileged accounts. DCOs should establish a formal review and revocation process to review the adequacy of privileges and access levels, and de-provision or remove access in a timely manner. DCOs should segregate duties and areas of responsibilities to reduce opportunities for unauthorised or unintentional modification or misuse of the information assets. DCOs should implement controls (such as changing service authentication credentials at least twice annually) for all creation of service and application accounts and include more than one approver[7] for system configuration changes, especially changes are significant or sensitive; and
k. Implement network segmentation and security controls for its network and systems by dividing them into separate network domains and separating them from the public network (i.e., Internet). DCOs should implement appropriate access controls between network domains based on business needs and security requirements and deploy network intrusion detection or prevention systems to detect/deter abnormal network activities.

5 Designated Officer

5.1 Uplifting and ensuring the resilience and security of digital infrastructure is an important task, and it requires the collective effort of the organisation led by senior management. DCOs are encouraged to designate a senior representative to take charge of this collective effort.

[7] Approver is to authorise changes before the changes are carried out by a separate team of implementer/maker and checker.