Appendix B: Best practices from People, Process, Technology (PPT) Perspective

Usage:

- Definition of PPT:
  - **People**: addresses issues that stem from human error/lack of training.
  - **Process**: addresses issues that stem from lack of guidance or procedures.
  - **Technology**: addresses issues that may arise from improper usage of technological systems and services.
- Examples:
  - An organisation may have a policy where employees must undergo security and awareness training annually – addresses issues arising from *people* aspects.
  - An organisation may have a policy where the communication plan for an incident is established –addresses issues arising from *process* aspects.
  - An organisation may have a policy where system configurations are established – addresses issues arising from *technology* aspects.
  - In other words, the PPT type indicates *what* aspect of PPT the control addresses, not *how* it is implemented.
- **Control Owner**: who is *responsible* for implementing the control.

This is a non-exhaustive list; blank rows have been added for organisations to fill in other controls that they intend to implement or are already implementing.

	Control	Type (PPT)	Control Owner
1.1	**Establish Organisational Policies**		
1.1.1	Develop, communicate, and enforce an asset management policy, covering the roles and responsibilities of key stakeholders and processes for identifying, categorising, modifying, and disposing of assets throughout the asset lifecycle. This should account for both on-premises, off-site and cloud assets.	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.2	Develop, communicate, and enforce a change management policy, covering the roles and responsibilities of key stakeholders and processes for identifying, approving, acquiring, testing, and deploying system, service or environment changes relating to information security.	People Process Technology	▪ Policy owners ▪ Asset owners

1.1.3	Develop, communicate, and enforce a configuration management policy, covering the roles and responsibilities of key stakeholders and processes for documenting configuration of systems and software, establishing baselines as well as detecting, addressing and documenting deviations from the baseline.	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.4	Develop, communicate, and enforce a patch management policy, covering the roles and responsibilities of key stakeholders and processes for identifying, approving, acquiring, testing, and deploying updates to systems and services.	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.5	Develop, communicate, and enforce a vulnerability management policy, covering the roles and responsibilities of key stakeholders and processes for identifying, documenting, evaluating and mitigating risks associated with vulnerabilities in systems and services.	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.6	Develop, communicate, and enforce a network security policy, covering the roles and responsibilities of key stakeholders and processes for identifying, testing, and deploying network security controls.	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.7	Develop, communicate, and enforce an access control policy, covering the roles and responsibilities of key stakeholders and processes for managing, granting, reviewing, and revoking user access, defining access levels, and adhering to the elements of identification, authentication, authorisation, and accountability (IAAA).	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.8	Develop, communicate, and enforce an audit logging and monitoring policy, covering the roles and responsibilities of key stakeholders and processes for collection, analysis, and storage of activity data. This should account for both on-premises, off-site and cloud assets.	People Process Technology	▪ Policy owners ▪ Asset owners
1.1.9	Develop, communicate, and enforce a business continuity plan, covering the roles and responsibilities of key stakeholders and processes for ensuring that the organisation's operations can continue during and after disruption from an incident. This should include strategies for risk assessment, identifying critical functions and assets, backup & recovery procedures, and communication plans during and post-incident. For	People Process Technology	▪ Policy owners ▪ Asset owners

	business continuity aspects specific to DDoS attacks, please refer to section 1.2, Establish a DDoS Incident Response Plan for more details.		
1.1.10	Develop, communicate, and enforce a security awareness and training policy, covering the roles and responsibilities of key stakeholders and processes for educating employees on security best practices and promoting a security-aware organisational culture.	People Process Technology	▪ Policy owners ▪ Asset owners
	Blank rows for any additional controls		
1.2	**Establish a DDoS Incident Response Plan**		
1.2.1	Develop a robust organisation DDoS incident response plan for identifying, mitigating, and rapidly recovering from DDoS attacks. This may include classifying incidents by severity with corresponding response measures (e.g., geo-blocking, request rate limiting) to balance between maintaining business operations and denying DDoS attack traffic. The incident's severity should also inform the level of notification required, i.e., who needs to be informed and how frequently.	Process	All stakeholders, including: ▪ Policy owners ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, System administrators) ▪ Service providers
1.2.2	Ensure that all stakeholders including leaders, operational and application teams, extended IR teams (legal counsel, HR, public relations etc.) and service providers understand their roles and responsibilities at every stage in response to a DDoS attack.	People	All stakeholders, including: ▪ Policy owners ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
1.2.3	Clearly document incident reporting and escalation procedures, inclusive of defining triggers for escalation, defining escalation paths for who needs to be informed at each stage of the incident, and clarifying the decision-making authority at each level of escalation.	Process	▪ System owners ▪ Incident Response (IR) team

1.2.4	For internal communications, establish communication protocols for the appropriate level of notification as required by the incident's severity, inclusive of upward reporting from frontline staff to senior leadership for visibility and downward reporting of directives or strategic information.	Process	▪ System owners ▪ Incident Response (IR) team
1.2.5	For external communications, ensure established communication protocols and Point-of-Contacts with Managed Service Providers are documented and reviewed periodically to ensure timely activation of DDoS services when required.	Process	▪ System owners ▪ Incident Response (IR) team
1.2.6	For any communications, plan for alternate communication protocols in case of a situation where the established communication mechanism is ineffective or unavailable.	Process	▪ System owners ▪ Incident Response (IR) team
1.2.7	Ensure that any backup mechanisms used for system and service recovery are regularly maintained and tested for reliability and integrity.	Process	▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators)
	Blank rows for any additional controls		

	Control	Type (PPT)	Control Owner
2.1	**Identify Critical Assets and Services**		
2.1.1	Identify critical assets and services of the organisation that are exposed to public internet, such as through a scanning with analysis tools, and generate a Bill of Materials (BOM).	Process	▪ System owners
2.1.2	Prioritise assets and services based on service's criticality.	Process	▪ System owners
2.1.3	Identify the network access path to each critical assets and services from public internet.	Process	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators)
2.1.4	Identify potential network/application chokepoints to each critical assets and services both within and external to the organisation's network (i.e., from public internet).	Process	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators)
2.1.5	Establish a baseline of typical and peak network activity and traffic patterns of the organisation's critical assets and services from public access on normal days and days coinciding with activities that might increase the traffic e.g., promotion events such as the redemption of vouchers.	Process	▪ Operational teams (e.g., Network engineers, system administrators)
2.1.6	Determine the appropriate thresholds to activate DDoS mitigation services and measures. These should be set with an appropriate buffer below the maximum operating specifications of the organisation's network appliances while accounting for the estimated network activity established above.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
2.1.7	Ensure that the organisation's network design is capable of handling network traffic spikes to mitigate resource exhaustion. This includes adequate sizing of network appliances with sufficient throughput, considering network redundancy for inbound and outbound network traffic, load balancing and traffic shaping for critical assets. i) As a starting point, organisations may want to consider accounting for 1.5x – 3x of the peak traffic baseline established in 2.1.5 when designing for their maximum traffic capacity, and scale accordingly (in line with their resources).	Technology	▪ Operational teams (e.g., Network engineers, system administrators)

	Blank rows for any additional controls		

	Control	Type (PPT)	Control Owner
3.1	**Design for Resiliency**		
3.1.1	Enforce network traffic inspection with appliances such as a Next-Generation Firewall (NGFW) that includes deep packet inspection (DPI), intrusion detection / prevention, and application control capabilities. With these appliances, organisations may wish to adopt a mixture of positive and negative security models where applicable e.g., allowlisting and blocklisting. Additionally, for Cloud implementation, a Cloud Network Firewall may offer auto-scaling capability.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
3.1.2	Implement a Web Application Firewall (WAF) for inspection and validation of application payload against application security risks referencing industry resources such as OWASP Top 10 or CWE Top 25. Additional capabilities may include rate limiting API requests and blocking traffic from known malicious bots. Firewall thresholds for raising alerts or activating mitigation measures (e.g., rate limiting) should also be established in line with the baselines established in 2.1.5. Organisations should consider the following best practices for firewall thresholds: i) Alerts should be raised if network traffic increases by 10% - 20% compared to baseline traffic. ii) Activation of mitigation measures should be triggered if network traffic increases by 15% - 20% of the alert threshold, or an increase of around 30% - 50% compared to baseline traffic.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)

3.1.3	Deploy dedicated pathways for serving different organisation functions or functions of differing criticality. This reduces the attack surface for critical services and ensures they receive minimal disruptions when non-critical services are targeted.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
3.1.4	Deploy load balancers to distribute requests for workload processing for each set of critical assets and services.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
3.1.5	Deploy and configure application nodes at each load balancer such that application resources can scale according to workload processing demands.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
3.1.6	For applicable use cases, enable mutual Transport Layer Security (mTLS) to mutually authenticate users and services such that only genuine requests are served.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
	Blank rows for any additional controls		
3.2	**Maintain Good Cyber Hygiene**		
3.2.1	Keep track of new Common Vulnerabilities and Exposures (CVE) records based on the BOM list.	Process Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators)
3.2.2	Regularly scan assets and services for vulnerabilities.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
3.2.3	Deploy patches to critical assets and services in a timely manner.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
3.2.4	Deploy workarounds and detection rules for zero-day CVE if the assets and services cannot be brought offline.	Process Technology	▪ System owners Operational teams (e.g., Network engineers, system administrators)
3.2.5	Reference industry's benchmarks for secure configurations and contextualise to the deployed environment to minimise exploits from the public internet.	Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators)

3.2.6	Ensure that critical assets and services remain aligned to hardening baselines through periodic follow-up assessments and necessary remediations.	Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators)
	Blank rows for any additional controls		

3.3	**Engage DDoS Protection Service Providers**		
3.3.1	Enable network traffic inspection to detect and block illegitimate protocols and volumetric network attacks for network traffic routed through service providers before arriving at organisation's application resources.	Technology	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.3.2	Enable web application traffic inspection or a WAF appliance with rules configured against application security risks referencing industry resources such as OWASP Top 10 or CWE Top 25, rate limit API requests and block traffic from malicious bots.	Technology	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.3.3	Subscribe to highly available and resilient Domain Name System (DNS) hosting service with a global network of servers located in multiple geographic regions to deliver DNS responses efficiently. The service should filter out malicious DNS traffic and enable Domain Name System Security Extensions (DNSSEC) to mitigate DNS-related attacks such as DNS spoofing, man-in-the-middle, unauthorised DNS changes.	Technology	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.3.4	Utilise Content Delivery Network (CDN) with a global network of servers located in multiple geographic regions to offload and cache content from origin servers. Utilising a CDN also hides the IP address of the origin server, obscuring the actual hosting infrastructure and protecting it from attacks. CDNs can also employ captcha challenges, which reduces the risks of application layer attacks.	Technology	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.3.5	Enable bot management solutions that can detect and prevent activities of malicious bots/ botnets often utilised in DDoS attacks. Solutions may leverage detection capabilities such as behavioural analysis and client request or device fingerprinting.	Technology	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
	Blank rows for any additional controls		

3.4	**Understand the Responsibilities between Subscriber and Service Provider**		
3.4.1	The scope of protections offered by DDoS mitigation services: i. Service Provider should clearly define the scope of DDoS protection services, specifying the assets covered, types of DDoS attacks mitigated, the extent of protection (e.g., network, application layer attacks) and support for incident response. Regular communication of updates to the scope based on emerging threats or changes in infrastructure should be carried out. ii. Subscriber should ensure that organisational assets, critical infrastructure, and specific security requirements for DDoS protection are communicated effectively to the Service Provider. If there are changes or updates to the scope of protection, inform Service Provider promptly.	People Process Technology	▪ System owners ▪ Incident Response (IR) team ▪ Service providers
3.4.2	The risks posed by gaps/limitations in coverage. i. Subscriber, in consultation with Service Provider, should conduct risk assessments to identify potential DDoS attack vectors and vulnerabilities in the organisation's infrastructure. ii. Identified risks should be clearly communicated between both parties, and it would be best for subsequent mitigation strategies to be a collaborative effort. Additionally, Subscriber should inform Service Provider if there are any perceived gaps or limitations in the security coverage that may impact organisational assets or compliance.	People Process Technology	▪ System owners ▪ Incident Response (IR) team ▪ Service providers
3.4.3	Thresholds for raising alert for volume traffic and subsequent performance of DDoS mitigation which should be set below the maximum capacity of the agency's network appliances' bandwidth. i. Service Provider should establish clear alert thresholds for different types and magnitudes of DDoS attacks, considering factors such as traffic volume, patterns, and duration. These thresholds should be communicated with the Subscriber to ensure that it suits the Subscriber's needs and should be below the maximum capacity of the Subscriber's network appliance throughput. Response times	People Process Technology	▪ System owners ▪ Incident Response (IR) team ▪ Service providers

	and escalation procedures should be discussed so that DDoS incidents are addressed promptly and effectively. ii. Subscriber should in turn understand the established alert thresholds and criteria for severity. Clearly communicate with Service Provider about their infrastructure's maximum thresholds and discuss their needs with the service provider. Regular reviews should be conducted to ensure that appropriate adjustments are made for dynamic environments.		
3.4.4	Communications channel for effective and transparent incident and problem management, covering the following: i. Primary communication channel e.g., mobile call, mobile message, email. Ideally, primary communication channel should allow the other party to verify that the message has been received (e.g., a phone call is answered, read receipts for messages). ii. Secondary communication channel if the primary channel fails. Parties may want to consider using multiple means of communication simultaneously, and not just as a backup option, for greater efficiency of response. iii. Relevant organisation personnel to be notified. iv. Frequency of updates to organisation in the event of an attack.	People Process Technology	▪ System owners ▪ Incident Response (IR) team ▪ Service providers
3.4.5	Definitions of terminology used. i. Service Provider should try to provide a comprehensive glossary of DDoS-related terminologies used in the cybersecurity domain. A common understanding between Service Provider and Subscriber should be established. ii. Subscriber should ensure that users are familiar with key DDoS-related terms and concepts through training programs. Clarifications should be made on unfamiliar terms. Common vocabulary should be used to facilitate effective communication before, during and after any possible cybersecurity incident.	People Process Technology	▪ System owners ▪ Incident Response (IR) team ▪ Service providers
	Blank rows for any additional controls		

3.5	**Conduct DDoS Sustainability Tests**		
3.5.1	Conduct DDoS simulation and load tests to determine the maximum workload transactional capacity for critical assets and services as well as validate the configured thresholds of DDoS mitigation services and measures.	Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.5.2	Engage the assistance of professional service providers, if necessary, and ensure that tests are conducted in compliance with the user agreement of hosting environment providers.	Process Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.5.3	Take note of the metrics and indicators relevant to the organisation's operating environment such as service transactions, network health, application servers' performance (e.g., CPU utilisation, memory usage, network bandwidth).	Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.5.4	Adjust the thresholds and configuration parameters of the environment based on the results and metrics captured from the tests above. These tests should be performed when significant changes are made to the environment, as well as periodically to ensure that the growth of the organisation does not outpace the configured thresholds and parameters.	Process Technology	▪ System owners ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
	Blank rows for any additional controls		

3.6	**Be familiar with the Incident Response Plan**		
3.6.1	Conduct DDoS tabletop exercises and drill tests of the DDoS response plan on a regular basis with all internal and external stakeholders, including support from managed security service providers if applicable. This is to familiarise all stakeholders with the processes involved, as well as to identify gaps and issues before a real attack.	People Process	All stakeholders, including: ▪ Policy owners ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
3.6.2	Conduct an after-action review (AAR) after each tabletop exercise/test and update the DDoS response plan based on lessons learned regarding communication, mitigation, and recovery.	People Process	All stakeholders, including: ▪ Policy owners ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
	Blank rows for any additional controls		

	Control	Type (PPT)	Control Owner
4.1	**Monitor for Early Warnings of DDoS Attacks**		
4.1.1	Monitor for abnormal slowness or abnormal surges in network traffic (e.g., network latency) to critical assets and services from the public internet. i. Keep track of optimal response time and latency time of critical assets and services during business-as-usual period. ii. Set up and fine-tune alarm thresholds to detect abnormal response time and latency time to critical assets and services. iii. Automate notification to operation team and disaster recovery team for immediate diagnostic and investigation upon detection. iv. Upon detection, enable network packet capture to support further investigation and analysis of attack traffic if resources permit.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
4.1.2	Monitor for unusual traffic (reconnaissance traffic) coming from a single or a group of IP addresses.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
4.1.3	Other indicators of DDoS include but are not limited to: i. Slow application performance, ii. High processor and memory utilisation, iii. Websites being unavailable, iv. Unexpected surge in ingress traffic.	Technology	▪ Operational teams (e.g., Network engineers, system administrators)
	Blank rows for any additional controls		
4.2	**Determine the Nature and Scope of the DDoS Attack**		
4.2.1	Verify that the suspicious traffic is a DDoS attack: i. Perform internal checks to assess if service disruptions stem from internal faults or events e.g., organisation's server failure or configuration errors on network devices.	Process	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Incident Response (IR) team ▪ Service providers

	ii. Contact managed service providers through previously established communication channels, if applicable, to verify if observed service disruptions for the organisation's services arose from service provider outages.		
4.2.2	Identify the details of the DDoS attack: i. Identify the critical assets and services that are being affected, including IP addresses of the systems, through available tools and documentation such as network monitoring services or network infrastructure diagrams. ii. Work with managed security service providers, if applicable, to identify malicious packets e.g., destination port number, communication protocol, and determine the DDoS attack vectors. iii. Review logs/critical equipment health status e.g., DNS logs, Router/Firewall CPU and Memory, etc. iv. Ensure that logs are shared among various teams e.g., Apps, Server, Network, Cybersecurity, in a timely manner for a more holistic view of incident. v. Inform managed service providers, if applicable, on the possibility of DDoS attacks such that packet inspection may be enabled for specific network traffic to facilitate subsequent investigations.	Process People	▪ Operational teams (e.g., Network engineers, system administrators) ▪ Incident Response (IR) team ▪ Service providers
	Blank rows for any additional controls		

	Control	Type (PPT)	Control Owner
5.1	**Execute DDoS Incident Response Plan and Other Mitigation Measures**		
5.1.1	In the event of a DDoS attack, follow the established DDoS response plan, adapt, and respond to the situation, inclusive of incident escalation procedures and communication plans to internal and external stakeholders.	People Process Technology	All operational stakeholders, including: ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
5.1.2	The following mitigation strategies to minimise the impact of the attack and restore normal operations may be adopted: i. Identifying and blocking malicious traffic: Once the attack path has been identified, custom rules can be added into network firewall or WAF to block malicious traffic (such as through IP address or geolocation restrictions), reducing the load on the target server or network. ii. Absorbing attack traffic: Managed DDoS protection services and workload scaling can help absorb attack traffic while permitting legitimate user traffic to still be processed. This involves activating redundant systems and resources to increase the network and application load that may be served. iii. Rerouting traffic: Network traffic can be rerouted to other services or networks to avoid overwhelming a single target server or network. iv. Implementing rate limiting: Rate limiting can be used to control the amount of traffic that can be sent to a server or network, preventing it from being overwhelmed. v. Shutting down affected vulnerable service(s)/resource(s) for remediation: For attacks targeting known vulnerabilities of services/resources, organisation may isolate and remediate the vulnerable resources against observed attacks before bringing them back online. Note that, depending on the scale of affected services/resources, this might disrupt the entire system.	People Process Technology	All operational stakeholders, including: ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers

	vi. Preserve essential service(s)/ resource(s): During persistent attacks on non-critical services/ resources that impact business-critical services/ resources, organisation may choose to deny attack paths of the threat actor by shutting down targeted services/ resources and preserve the availability of essential organisation services/ resources. This separation should ideally be accounted for during design and implementation of services.		
5.1.3	Where feasible, automation of the above processes might enable faster response and activation of the response plan, alongside a streamlined incident response process, reducing the impact of the attack. However, human oversight of the automated processes is key to addressing the risk of false positives/negatives, and to make critical judgement decisions.	People Process Technology	▪ Policy owners ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators)
5.1.4	Take note of the following considerations when leveraging automated DDoS mitigation/ incident response measures: i. Not all incidents are suitable for automation and may require human intervention/decision-making. As such, conduct a risk assessment to evaluate the impact of automated response, such as the risk of false positives and negatives, and ensure that there are fallback mechanisms i.e., human intervention to address unintended consequences of the automated solution. ii. Automated solutions should have granular controls for thresholds, triggers, and escalation paths, ensuring that the configuration aligns with the changing needs of the organisation; these should be fine-tuned in accordance with insights derived from DDoS sustainability tests and post-incident reviews.	People Process Technology	▪ Policy owners ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators)
5.1.5	Continue to monitor other network assets for any additional anomalous or suspicious activity that could indicate intrusion attempts into the organisation while the current DDoS attack has diverted the organisation's attention and resources.	Technology	▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators)
5.1.6	Organisations suspected to be a victim of DDoS attacks are strongly advised to report the case to SingCERT via the Incident Reporting Form as the	Process	▪ System owners ▪ Incident Response (IR) team

	information could help alert and assist other individuals and organisations. If monetary loss(es) or criminal activity is involved, organisations may lodge a police report at any neighbourhood police post or online here.		
5.1.7	Organisations that encounter Ransom DDoS (RDDoS), where a malicious actor threatens to conduct DDoS attacks on an organisation unless a ransom is paid, are strongly encouraged not to pay the ransom – doing so does not guarantee that the attack will not happen and will further fund criminal activity. Instead, report the case to SingCERT via the Incident Reporting Form and mobilise your response teams against a potential DDoS attack, taking actions as outlined in your DDoS Incident Response Plan.	Process	▪ System owners ▪ Incident Response (IR) team
	Blank rows for any additional controls		

	Control	Type (PPT)	Control Owner
6.1	**Resume Normal Operations**		
6.1.1	Initiate recovery phase of incident response plan, such as restoring data from backups and other restoration assets and restoring network channels and connections.	Process Technology	All operational stakeholders, including: ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
6.1.2	Verify that services have been restored to the level required for business operations, such as in terms of bandwidth, latency, and application performance.	Process Technology	All operational stakeholders, including: ▪ System owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
6.1.3	Notify internal and external stakeholders on the activities performed for recovery as well as the progress for restoration of operational capabilities.	Process	▪ Incident Response (IR) team
	Blank rows for any additional controls		
6.2	**Review and Incorporate Lessons Learned**		
6.2.1	When the attack has subsided and normal operations have resumed, review and document the incident with managed security service providers, covering at least the following: i. Attack Analysis: assets targeted, attack characteristics (sustained flood, level of sophistication), peak amount of network traffic, length of attack.	Process	All stakeholders, including: ▪ System owners ▪ Policy owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators)

	ii. Impact Analysis: services impacted (extent of impact + length of downtime), indirect damages (e.g., loss of IP, reputational damage), user impact (from both attack and from defensive measures).		▪ Service providers
6.2.2	Update the DDoS response plan to include improvements drawn from lessons learned regarding communication, mitigation, architecture improvements and recovery. Continue to conduct DDoS tabletop exercises and drill test the DDoS response plan.	People Process Technology	All stakeholders, including: ▪ System owners ▪ Policy owners ▪ Incident Response (IR) team ▪ Operational teams (e.g., Network engineers, system administrators) ▪ Service providers
6.2.3	Participate in collaborative threat intelligence sharing partnerships with other organisations to exchange information about cyber threats including DDoS attacks. Collective knowledge can enhance situational awareness to detect recent types of DDoS attacks and mitigate them effectively.	Process Technology	▪ System owners ▪ Policy owners
	Blank rows for any additional controls		