For Financial Institutions (FIs):

1. MAS (Monetary Authority of Singapore) TRMG (Technology Risk Management Guidelines) and CH (Cyber Hygiene) gap analysis and recommendations.
2. Provision of missing policies, standards and plans to address gaps in the above regulations.
3. Communication of new policies, standards and plans to customer's personnel (e.g. introduction presentation).
4. In-person or online security awareness training (additional charges will be imposed on a per session basis).
5. Internal audit support (does not qualify as independent external audit):
    a) Regular vulnerability assessment (quarterly up to 50 IP addresses);
    b) Annual internal penetration testing (no more than web app PT of 1 x web application, host PT of 10 hosts and network PT of 50 IPs);
    c) Annual internal configuration audit (no more than 50 audit targets);
    d) Annual internal source code review of customised applications (no more than 500,000 Lines of Code);
    e) Annual internal TRMG or CH audit; and,
    f) Annual risk assessment/threat modelling.
6. Annual cyber simulation exercise (charged separately), including
    a) Post-exercise update of incident response plan and playbooks
7. Security governance role for implementation of technical security controls by 3rd party system integrators or internal IT teams (charged per project. This role is not for project management).
8. Incident response standby and activation services:
    a) Review of adequate logging during pre-incident preparation;
    b) 8x5 phone standby;
    c) Next Business Day onsite investigation (24 x 7 x 4 phone and onsite support is charged separately);
    d) Preparation and regular update of MAS incident report until closure of incident (charged separately);
    e) Triage of logs to analyse the incident (charged separately);
    f) Digital forensic imaging and investigation of affected devices (charged separately); and,
    g) Advisory support to IT operations team on recommended containment, eradication and recovery activities (charged separately).
9. Member of TRM steering committee to comply with MAS TRMG.

For Non-Financial Institutions (Non-FIs) Critical Information Infrastructure (CII):

1. CSA (Cyber Security Agency) CCoP (Cybersecurity Code of Practice) gap analysis and recommendations.
2. Provision of missing policies, standards and plans to address CSA CCoP gaps.
3. Communication of new policies, standards and plans to customer's personnel (e.g. introduction presentation).
4. In-person or online security awareness training (additional charges will be imposed on a per session basis).
5. Internal audit support (does not qualify as independent external audit):
    a) Regular vulnerability assessment (quarterly up to 50 IP addresses);
    b) Annual internal penetration testing (no more than web app PT of 1 x web application, host PT of 10 hosts and network PT of 50 IPs);
    c) Annual internal configuration audit (no more than 50 audit targets);
    d) Annual internal source code review of customised applications (no more than 500,000 Lines of Code);
    e) Annual internal CCoP audit; and,
    f) Annual risk assessment/threat modelling.
6. Annual cyber simulation exercise (charged separately), including
    a) Post-exercise update of incident response plan and playbooks
7. Security governance role for implementation of technical security controls by 3rd party system integrators or internal IT teams (charged per project. This role is not for project management).
8. Incident response standby and activation services:
    a) Review of adequate logging during pre-incident preparation;
    b) 8x5 phone standby;
    c) Next Business Day onsite investigation (24 x 7 x 4 phone and onsite support is charged separately);
    d) Preparation and regular update of MAS incident report until closure of incident (charged separately);
    e) Triage of logs to analyse the incident (charged separately);
    f) Digital forensic imaging and investigation of affected devices (charged separately); and,
    g) Advisory support to IT operations team on recommended containment, eradication and recovery activities (charged separately).
9. Member of CCoP steering committee or senior management to comply with CSA CCoP.

For Healthcare, Non-CII Organisations:

1. MOH HCSE (Healthcare Cybersecurity Essentials) and PDPA protection principle gap analysis and recommendations.
2. Provision of missing policies, standards and plans to address HCSE and PDPA protection principle gaps.
3. Communication of new policies, standards and plans to customer's personnel (e.g. introduction presentation).
4. In-person or online security awareness training (additional charges will be imposed on a per session basis).
5. Internal audit support (does not qualify as independent external audit):
    a) Regular vulnerability assessment (quarterly up to 50 IP addresses);
    b) Annual internal penetration testing (no more than web app PT of 1 x web application, host PT of 10 hosts and network PT of 50 IPs);
    c) Annual internal configuration audit (no more than 50 audit targets);
    d) Annual internal source code review of customised applications (no more than 500,000 Lines of Code);
    e) Annual internal HCSE and PDPA protection principle audit; and,
    f) Annual risk assessment/threat modelling.
6. Annual cyber simulation exercise (charged separately), including
    a) Post-exercise update of incident response plan and playbooks
7. Security governance role for implementation of technical security controls by 3rd party system integrators or internal IT teams (charged per project. This role is not for project management).
8. Incident response standby and activation services:
    a) Review of adequate logging during pre-incident preparation;
    b) 8x5 phone standby;
    c) Next Business Day onsite investigation (24 x 7 x 4 phone and onsite support is charged separately);
    d) Preparation and regular update of MAS incident report until closure of incident (charged separately);
    e) Triage of logs to analyse the incident (charged separately);
    f) Digital forensic imaging and investigation of affected devices (charged separately); and,
    g) Advisory support to IT operations team on recommended containment, eradication and recovery activities (charged separately).

For Non-Financial Institutions (Non-FIs) Non-Critical Information Infrastructure (Non-CII):

1. PDPA protection principle gap analysis and recommendations.
2. Provision of missing policies, standards and plans to address PDPA protection principle gaps.
3. Communication of new policies, standards and plans to customer's personnel (e.g. introduction presentation).
4. In-person or online security awareness training (additional charges will be imposed on a per session basis).
5. Internal audit support (does not qualify as independent external audit):
    a) Regular vulnerability assessment (quarterly up to 50 IP addresses);
    b) Annual internal penetration testing (no more than web app PT of 1 x web application, host PT of 10 hosts and network PT of 50 IPs);
    c) Annual internal configuration audit (no more than 50 audit targets);
    d) Annual internal source code review of customised applications (no more than 500,000 Lines of Code);
    e) Annual internal PDPA protection principle audit; and,
    f) Annual risk assessment/threat modelling.
6. Annual cyber simulation exercise (charged separately), including
    a) Post-exercise update of incident response plan and playbooks
7. Security governance role for implementation of technical security controls by 3rd party system integrators or internal IT teams (charged per project. This role is not for project management).
8. Incident response standby and activation services:
    a) Review of adequate logging during pre-incident preparation;
    b) 8x5 phone standby;
    c) Next Business Day onsite investigation (24 x 7 x 4 phone and onsite support is charged separately);
    d) Preparation and regular update of MAS incident report until closure of incident (charged separately);
    e) Triage of logs to analyse the incident (charged separately);
    f) Digital forensic imaging and investigation of affected devices (charged separately); and,
    g) Advisory support to IT operations team on recommended containment, eradication and recovery activities (charged separately).