Cyber Security Reporting award criteria

Reports will be assessed against the following security metrics:

Organisation is aware of its exposure

- Acknowledgement of major risks and threats to operations.
- Evidence of data discovery, infrastructure and access control initiatives within the organisation.

Organisation regularly measures security assurance within its infrastructure, staff and threat landscape

- Mention of ongoing activities, including awareness training, threat intelligence, security testing, policy reviews, patch management and perimeter scanning.

Organisation is safe in the face of cyber incidents and disasters

- Mention of business continuity and disaster response plans.
- Mention of capabilities of incident response team.
- Positive indicators of incident response performance (e.g. low median response time; low percentage of critical incidents that took longer than 48 hours to resolve).
- Mention of capabilities in place to perform disaster recovery in the face of a ransomware attack.

Security team has strong executive buy-in, and has oversight within the organisation

- Mention of board involvement in security (including executive security officers).
- Mention of successful security initiatives fully adopted by the organisation.

Organisation is capable of anticipating and responding to global security events, including major regulations and cyber disasters

- Positive indicators of how organisations reacted to recent cyber incidents (e.g. WannaCry, Petya).
- Positive indicators of how organisations are prepared to respond to currently prominent cyber threats, including ransomware and supply chain attacks.
- Mention of compliance to topical major regulations (e.g. GDPR).
- Mention of methods involved to improve response to these events (e.g. steering committee for regulations, lessons learned from incidents).

Organisation has appropriate investments, tools and expertise dedicated to information security

- Mention of security team size, budget, sub-departments and tools – preferably with rationale behind choice.

Organisation has adopted a holistic framework

- Mention of any security control framework used by the organisation.

Security controls are subject to independent review and test

- Mention of external review of security controls and vulnerabilities.

Organisation has a well-informed security strategy with clear and attainable milestones

- Action plan to transform security, accompanied by clear goals.
- Rationale behind security strategy.
- Mention of drivers and principles of security strategy.

pwc

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

2021-05-10_RITM5237606