SIBENCO
LEGAL & ADVISORY

INFORMATION GOVERNANCE CHECKLIST

- Are your leaders embedding IG as a foundation of good corporate governance?
- Do you have IG champions at board level?
- Do you know the IT and cyber risks for your organisation?
- Is the data held within your organisation being used effectively for multiple business value-creating purposes?
- Have you clearly articulated the purpose of a robust IG framework in your business?
- What is your organisation measuring – e.g.:
  - No. of attempted cyber attacks per annum; no. of cyber security breaches of IT systems per annum; and the cost of responding to each privacy breach, business interruption costs etc?
  - No. of privacy breaches per annum and the cost of responding to breaches, business interruption etc?
  - Revenue, cost, profit of new/improved products developed from information derived from analytics?
  - Cost of implementation of new IT systems and software?
  - Percentage of increase in data and percentage of data deleted per annum?
  - Cost of production per page of reviewed documents for litigation and regulatory inquiries?
- Who is the day-to-day leader of IG? Is there a person clearly responsible or an IG steering committee?
- Where there is an existing or contemplated IG steering committee –
  - Are all the relevant senior stakeholders on the committee?
  - Are those committee members able to embed appropriate IG processes throughout the organisation to achieve strategic organisational objectives?
- Are those responsible for information management on a day-to-day basis able to work collaboratively across functions to ensure that IG strategic objectives are met and achieve best practice, with the resulting efficiencies?
- Do you have a clear and comprehensive IG framework that includes:
  - Current policies and processes embedded within the organisation – in particular, is privacy embedded within your organisation?
  - IT policies and plans for disaster recovery and business continuity for cyber security incidents?
  - Policies and processes that comply with current records retention legislation and regulatory requirements e.g, OAIC Data Breach Notification Guide?
  - Training of key personnel to implement policies and processes and execute cyber security plans?
  - Regular reviews and audits of relevant cyber security, privacy, and records management policies and processes,etc?
- Can your IG framework and those responsible for IG adapt and respond promptly to changes in strategic organisational objectives – e.g., to new business opportunities arising through digital disruption or data analytics – or to regulatory change – e.g., changes to privacy laws or records retention requirements?
- Do your policies and processes adequately cover:
  - Employee cyber security education and awareness training?
  - Social media use?
  - Mobile device and BYOD use?
- Do you have external audits to ensure best practice standards in information management and adherence to policies and processes?

For further information, please contact Susan Bennett, Principal
on +61 2 8226 8682 or email susan.bennett@sibenco.com