Media Release

9 November 2016

CYBER HEALTH CHECK FOR ASX 100 COMPANIES

ASX and ASIC have today invited the 100 largest ASX-listed companies to participate in the ASX 100 Cyber Health Check, a survey to benchmark the levels of cyber security awareness, capability and preparedness within Australian business.

Participation by companies is voluntary, with responses sought by mid-December 2016.

Companies that participate will receive a confidential report benchmarking their own cyber security practices. A public report on the themes emerging from the data is expected to be released in March 2017.

The ASX 100 Cyber Health Check is an industry-led initiative that forms part of the Australian Government's Cyber Security Strategy. ASX and ASIC worked with representatives from Government, business and audit firms KPMG, Deloitte, EY, and PwC, to develop a cyber health check survey for the Australian environment, based on a similar exercise in the UK with the FTSE 350.

The ASX 100 contribute significantly to Australia's economy and are well placed to lead a national effort to encourage best practice cyber security for Australian business. Protecting information assets is important for business sustainability and competitiveness.

Cyber security is a strategic risk management issue for Boards, not just IT departments. Effective governance on how business is addressing cyber risks and building resilience is a key enabler for the Australian economy.

Amanda Harkness, ASX Group Executive, said: "The ASX 100 Cyber Health Check has brought together Government, regulators and industry on an issue of critical importance to Australian business and the millions of investors who hold shares in Australian companies. The sharing of best practice, and increased awareness and engagement by directors of listed companies are important steps in building the cyber resilience of Australian business.

"The better informed boards become, the more effectively they can assess their cyber security risks and opportunities, including identifying areas where improvement is required. Participation will reassure shareholders and the broader community that boards are actively engaged in addressing cyber issues.

"ASX thanks those who contributed to preparing the ASX 100 Cyber Health Check, including ASIC, the Department of PM&C, CERT Australia, and the big four audit firms, especially KPMG. We now encourage Australia's largest listed companies to play their part", said Ms Harkness.

A copy of the ASX 100 Cyber Health Check survey follows this media release, as does a set of FAQs prepared by KPMG.

Further enquiries:

Media
Matthew Gibbs
General Manager, Media and Communications
Tel: +61 2 9227 0218
Mobile: 0411 121219
matthew.gibbs@asx.com.au
http://www.asx.com.au/about/media-releases.htm

Analysts/Investor Relations
Stephen Hammon
General Manager, Finance
Tel: +61 2 9227 0260
Mobile: 0488 212755
stephen.hammon@asx.com.au
http://www.asx.com.au/about/investor-relations.htm

ASX 100 Cyber Health Check 2016

Thank you for taking the time to participate in the Cyber Governance Health Check Survey, to help benchmark the levels of cyber security awareness, capabilities and preparedness across the ASX 100.

We suggest you set aside between 30 and 60 minutes to complete the survey. Please submit your response by 16 December 2016.

All responses are confidential, anonymous and will be reported in aggregated form to ensure individual responses cannot be identified.

Completion Instructions:

For the benchmarking reports to offer real insight, it is important that this survey is completed only by the Chairman, the Audit Committee Chair or the Risk Committee Chair.

A Partner from your Audit Firm will be interviewing you and assisting with facilitating completion of the survey. They will also hold your unique identifier for the purposes of providing confidential individual benchmark reports.

For more information about this project, please refer to the FAQ's document.

Contact Information:

If you have any queries regarding this survey, you can contact either your Audit Firm or the general inquiries box AU-FMCyberhealthcheck@kpmg.com.au

For any technical difficulties, please contact KPMG's Research Lead, Nicola Hassan on nicolahassan@kpmg.com.au

By clicking on the "Next" button below you acknowledge that you have read and understood all of the information detailed in this notification, and agree to undertake the survey.

Unique Identifier:

Please note, only your audit firm will know what your company name is – that information will not be collected in this survey.

To capture your response you have been allocated a unique identifying number. Your Audit Partner will provide you this number during your interview, or if you are self-completing the online survey, please see the FAQ's to find out how you access your unique identifier from your Audit Firm.

Please enter your unique customer identifier here:

1. Respondent Profile

1.1 In order to optimise results, we request that this questionnaire is not passed to the Chief Information Officer (CIO) or others to complete on your behalf. However, if you have done so, could you please indicate who has supported you in completing this questionnaire?

- ❍ Nobody
- ❍ Chair of the Board
- ❍ Chief Executive Officer
- ❍ Chief Financial Officer
- ❍ Chief Operating Officer
- ❍ Chief Information Officer
- ❍ Chief Risk Officer
- ❍ A mix of the above
- ❍ Partner / director of audit firm
- ❍ Other, please specify _____

1.2 Which of these titles best describes your role? (Note: preference is for the survey to be completed at the Board or Committee Chair level)

- ❍ Chair of the Board
- ❍ Chair of Board sub Committee (e.g. Audit or Risk Committee)
- ❍ Non-Executive Director of Board
- ❍ Chief Executive Officer
- ❍ Chief Financial Officer
- ❍ Chief Operating Officer
- ❍ Chief Information Officer
- ❍ Other Executive

1.3 Which sector classification best applies to the company's main business?

- ❍ Technology, Communications and Healthcare
- ❍ Utilities, Energy and Resources
- ❍ Financial Services
- ❍ Industrials
- ❍ Consumer and Leisure
- ❍ Other

1.4 Indicate which of the following risk factors apply to your company (select all that apply):

- ❍ We deliver services vital to the critical national infrastructure
- ❍ More than 50% of our revenue comes through online interactions
- ❍ We run safety-critical automated systems (e.g. failure can put lives at risk)
- ❍ Our shareholder value is significantly dependent on securing and / or keeping secret our critical information assets
- ❍ We handle high value financial transactions or other assets at high risk from theft or fraud
- ❍ Not applicable

2. Understanding the Threat

2.1 Does the Board have a clear understanding of what the company's key information and data assets are (e.g. IP, financial, corporate, strategic, customer / personal data etc)?

- ❍ Limited understanding
- ❍ Reasonable understanding
- ❍ Clear understanding
- ❍ No, the information has not yet been presented to the Board

2.2 Does the Board have a clear understanding of the value of those key information and data assets (e.g. financial, reputational etc) to the company, a competitor or criminal?

- ❍ Limited understanding
- ❍ Reasonable understanding
- ❍ Clear understanding
- ❍ No, the information has not yet been presented to the Board

2.3 What is the Board's understanding of the potential resulting impact (e.g. on customers, share price or reputation) from the loss of / disruption to those key information and data assets?

- ❍ Limited understanding
- ❍ Reasonable understanding
- ❍ Clear understanding
- ❍ The impact has not yet been presented to the Board

2.4 Does the Board periodically review key information and data assets (especially confidential data) to confirm the risk management, legal, ethical and security implications of retaining them?

- ❍ Never
- ❍ Intermittently
- ❍ Annually
- ❍ Six monthly
- ❍ More frequently

2.5 Does the Board receive regular high level intelligence from the CIO / Head of security on who may be targeting your company, from a cyber-perspective, and their methods and motivations?

- ❍ Never
- ❍ Intermittently
- ❍ Annually
- ❍ Six monthly
- ❍ More frequently

2.6 Does the Board encourage its technical staff to enter into formal information sharing exchanges with other companies in your sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats?

- ❍ Yes
- ❍ No

2.7 Do you understand where the biggest vulnerabilities / risk exposures are in your IT security perimeter?

- ❍ Yes, I am confident in my understanding of key vulnerabilities
- ❍ Yes, however my understanding is limited
- ❍ No

2.8 Does your organisation engage external parties to perform regular vulnerability or penetration assessments?

- ❍ Yes, tests are performed and results reported to the Board
- ❍ Yes, tests are performed
- ❍ No

2.9 What level of understanding do the Directors have regarding the cyber security of the ecosystem (e.g. vendors, suppliers, customers) within which the organisation operates and the risks emanating from the ecosystem?

- ❍ Limited understanding
- ❍ Reasonable understanding
- ❍ Clear understanding
- ❍ Not yet presented to the Board

2.10 What level of understanding do the Directors have of the key controls in operation in the cyber resilience framework?

- ❍ Limited understanding
- ❍ Reasonable understanding
- ❍ Clear understanding
- ❍ Not yet presented to the Board

2.11 How confident are you that your company is properly secured against cyber attacks?

- ❍ Very confident
- ❍ Confident
- ❍ Somewhat confident
- ❍ Not very confident

2.12 Do you use public cloud services and, if so, are the risks clearly documented and understood?

- ❍ We used cloud services and risks are documented and understood
- ❍ We use cloud services and risks are understood but not documented
- ❍ We use cloud services and risks have not been assessed
- ❍ We have no cloud services
- ❍ I don't know

3. Leadership

3.1 Is cyber net (residual) risk expected to increase or decrease, in terms of likelihood of occurrence, over the next year or so?

- ❍ Increase significantly
- ❍ Increase slightly
- ❍ Stay the same
- ❍ Decrease slightly
- ❍ Decrease significantly

3.2 In your view, how important are cyber risks to the business?

- ❍ Not at all important
- ❍ Of limited importance
- ❍ Moderately important
- ❍ Extremely important

3.3 Which of the following statements best describes how cyber risk is handled in your Board governance process?

- ❍ It is a technical topic, not warranting Board level consideration
- ❍ We have been briefed about it once or twice but it is not regular Board business
- ❍ We are briefed periodically - e.g. a bi-annual update, plus being told when something has gone wrong
- ❍ We regularly consider cyber risk and make decisions (e.g. investment policies)
- ❍ We actively manage our cyber risk profile throughout the year

3.4 Who is the company's most senior "risk owner" for cyber?

- ❍ Chief Executive Officer (CEO)
- ❍ Chief Financial Officer (CFO)
- ❍ Chief Operating Officer (COO)
- ❍ CIO or Head of IT or equivalent executive position
- ❍ Board Chair
- ❍ General Counsel
- ❍ Company Secretary
- ❍ CISO (Chief Information Security Officer)
- ❍ Other direct report to CIO
- ❍ Chief Risk Officer (CRO)
- ❍ Direct report to CRO
- ❍ Direct report to other C-Suite executive
- ❍ We don't have one

3.5 Where, in governance terms, is the "risk owner" for cyber held to account?

- ❍ The Board
- ❍ Board Audit Committee
- ❍ Board Risk Committee
- ❍ Board Technology or Security Committee
- ❍ Other Board or Committee
- ❍ Executive Committee
- ❍ Standard management operational reporting line

3.6 Does the Board include a Director with a good understanding of Information Security and cyber security in particular?

- ❍ Limited understanding, however a plan is in place to include this skillset
- ❍ Limited understanding and we have no plans to include this expertise on the Board
- ❍ Moderate understanding
- ❍ At least one Board member is well versed in cyber security

3.7 Do you feel the company is doing enough to protect itself against cyber threats?

- ❍ No, there is more we need to do
- ❍ Yes, however there is more we need to do
- ❍ Yes, we're doing enough
- ❍ Yes, standards are excellent

3.8 Do you feel Board colleagues take cyber risk sufficiently seriously?

- ❍ Not seriously enough
- ❍ Very seriously
- ❍ Too seriously

3.9 Have you personally undertaken any form of cyber security / information security training in the last 12 months?

- ❍ Yes
- ❍ No

3.10 Has your Board undertaken any form of cyber security / information security training in the last 12 months?

- ❍ Yes
- ❍ No, but plan to
- ❍ No

3.11 Given the risks you face, how appropriate is the investment you are making around cyber defences?

- ❍ We have over invested in cyber security
- ❍ We have an appropriate level of investment, however plan to do more
- ❍ We have an appropriate level of investment
- ❍ We have underinvested in cyber security, however plan to do more
- ❍ We are underinvesting in cyber security

3.12 How has the Board sought to reassure investors and customers of its robust approach to cyber security?

- ❍ We are not actively engaging with investors or customers about cyber security
- ❍ Passive approach - our risk management approach is clearly outlined in annual reports and on our website
- ❍ Proactive approach - regular discussions with investors and customers around cyber risk management

3.13 When did your Board start receiving incident reports on cyber security?

- ❍ Within the last 12 months
- ❍ We have been receiving reports for greater than 12 months
- ❍ We do not receive reports of cyber incidents

3.14 Does your organisation have a specific cyber security budget?

- ❍ Yes, it is a standalone security budget
- ❍ Yes, it is included in the overall IT budget
- ❍ No, there is no specific budget for cyber security

3.15 Does your organisation have an information security policy that complies with a global standard?

- ❍ Yes - ISO 27000
- ❍ Yes - ITIL
- ❍ Yes – CoBIT
- ❍ Yes - NIST
- ❍ No
- ❍ I Don't know
- ❍ Yes, other, please specify: _____

3.16 Do you have a good understanding of the legal and regulatory requirements regarding cyber security, including reporting and privacy obligations?

- ❍ Yes
- ❍ No

4. Risk Management

4.1 Does the company's Risk Register include a "Cyber Risk" category?

- ❍ Yes
- ❍ No, however plans are in place to include cyber risk in the risk register
- ❍ No, not considered a specific requirement for the risk register

4.2 In the Risk Register, how well described are cyber risks, and the potential consequences for the business?

- ❍ Cyber risks do not appear in our risk register
- ❍ Poorly described: the implications for the company of the risks identified are not clear
- ❍ Reasonably described: the implications for the company of the risks identified are described in a basic manner
- ❍ Clearly described: the implications for the company of the risks identified are comprehensive

4.3 To what extent has your Board explicitly set its appetite for cyber risk, both for existing business and for new digital innovations?

- ❍ Cyber risk appetite has not been defined
- ❍ Cyber risk appetite is partially defined / has not yet been communicated
- ❍ Cyber risk appetite is clearly defined and understood

4.4 Where risk is a product of likelihood and magnitude, how significant or important is cyber risk, when compared with all the risks the company faces?

- ❍ Top risk
- ❍ Medium risk
- ❍ Low risk
- ❍ Not important

4.5 Does the Board have an understanding of where the company's key information or data assets are shared with third parties (including suppliers, customers, advisors and outsourcing partners)?

- ❍ Limited understanding
- ❍ Reasonable understanding
- ❍ Clear understanding
- ❍ No, not yet presented to the Board

4.6 Has the cyber resilience of key third party providers (e.g. vendors, suppliers) and clients / customers that connect to your organisation been assessed?

- ❍ Yes
- ❍ No
- ❍ Not applicable, we don't have any third party systems connecting to our organisation

4.7 Do cyber risks form part of the assessment of risk for all new projects and significant transactions (e.g. mergers and acquisitions)?

- ❍ Yes
- ❍ No

4.8 Does your organisation conduct testing of staff to determine the security risk culture (e.g. sending phishing emails to staff requesting a document to be opened)?

- ❍ Yes
- ❍ No
- ❍ I don't know

4.9 Does your organisation have sufficient skilled resources to deal with cyber risks?

- ❍ Yes
- ❍ No, however there are plans in place to engage additional resources
- ❍ No

4.10 Is the organisation's assessment of cyber risk tolerance informed by the role of the organisation in the sector (e.g. critical infrastructure)?

- ❍ Yes
- ❍ No

4.11 How often is the cyber resilience framework independently assessed?

- ❍ Annually
- ❍ Every 2-3 years
- ❍ It has been assessed but is not on a regular schedule
- ❍ It has never been assessed

4.12 Does the organisation assess its cyber security culture?

- ❍ Yes, annually
- ❍ Yes, every 2-3 years
- ❍ Yes, but not on a regular schedule
- ❍ It has never been assessed

4.13 Do you have a clear understanding of your company's disclosure requirements regarding a cyber breach?

- ❍ Yes
- ❍ No

4.14 How frequently does the Board review the cyber security strategy or roadmap?

- ❍ Multiple times during the year
- ❍ Annually
- ❍ Less frequently than annually
- ❍ The Board has not seen the cyber security strategy

5. Awareness of Help

5.1 The Australian Signals Directorate suggests that 85% of threats can be mitigated by implementing the ASD top 4 strategies. Have you implemented the ASD top 4 mitigation strategies *(i.e. Application whitelisting, patching common applications (e.g. MS Office), patching operating systems and restricting administrator privileges)*?

- ❍ Yes, fully implemented
- ❍ No, we use other frameworks
- ❍ No, however we are almost there
- ❍ No, however we plan to
- ❍ No, we have no plans to implement
- ❍ We are not familiar with the ASD mitigation strategies
- ❍ I don't know

5.2 Does your organisation perform benchmarking or self-assessment against a recognised standard?

- ❍ Yes
- ❍ No, however we plan to in the next 12 months
- ❍ No

5.3 Are the results of the benchmarking or self-assessment discussed at the Board, including the identified gaps?

- ❍ Yes
- ❍ No

5.4 Have you considered using cyber insurance?

- ❍ Yes, we have considered it and decided not to implement a policy
- ❍ Yes, we are implementing a policy in the next 12 months
- ❍ Yes, we have a cyber insurance policy
- ❍ No

5.5 Does your organisation's Internal Audit (or other independent assurance function) team conduct cyber resilience audits?

- ❍ Yes, in the last 12 months
- ❍ Yes, but not for over 12 months
- ❍ No, however it is under consideration for inclusion in future audit plans
- ❍ No

5.6 Has your organisation implemented an ongoing cyber awareness training program for staff?

- ❍ Yes, in the last 12 months
- ❍ Yes, it has been in place for over 12 months
- ❍ No, however we plan to implement a program in the next 12 months
- ❍ No

5.7 What is the primary source of information for Directors to stay informed and current on cyber security topics?

- ❍ Management briefings
- ❍ Peer discussion
- ❍ Government agency briefings
- ❍ External firm briefings
- ❍ Conferences
- ❍ Other
- ❍ Directors do not receive regular cyber security briefings

5.8 Does the Board ratify the cyber security strategy and framework?

- ❍ Yes
- ❍ No, however the Board relies on senior management to approve and the Board is notified
- ❍ No, the Board is not involved in the cyber security strategy and framework

5.9 Does the Board encourage the cyber security team to engage in data sharing arrangements with other organisations in its environment? (Select all that apply)

- ❍ Yes, Government agencies
- ❍ Yes, peer organisations
- ❍ Yes, competitor organisations
- ❍ Yes, customers, vendors and suppliers
- ❍ No

5.10 Does the organisation perform regular internal vulnerability scans (e.g. by the security team)?

- ❍ Yes
- ❍ No
- ❍ I don't know

5.11 Does the organisation perform regular external penetration testing?

- ❍ Yes
- ❍ No
- ❍ I don't know

5.12 Does the organisation use a set of standard metrics to quantify or trend the cyber risk?

- ❍ Yes
- ❍ No, however they are under development
- ❍ No
- ❍ I don't know

5.13 Has your organisation established a partnership relationship with the national Computer Emergency Response Team (CERT)?

- ❍ Yes
- ❍ No, we don't consider it necessary as we are not essential services / critical infrastructure
- ❍ No, however I think we should
- ❍ No
- ❍ I don't know

6. Cyber Incidents

6.1 From reporting provided to the Board, has the company experienced more or fewer cyber attack attempts over the last year?

- ❍ Significantly more
- ❍ Slightly more
- ❍ Steady state / no change
- ❍ Slightly less
- ❍ Significantly less
- ❍ There is no reporting provided to the Board
- ❍ There have been no cyber attack attempts

6.2 From your own recollection, how well did the company respond to those compromises and occurrences?

- ❍ Poorly / to an unacceptable level
- ❍ OK / average
- ❍ Quite well
- ❍ Very well
- ❍ Board reporting does not include information on cyber incidents
- ❍ Not applicable – there were no cyber attack attempts

6.3 Where, in governance terms, were these compromises and occurrences considered? (Select all that apply)

- ❍ The Board
- ❍ Board Audit Committee
- ❍ Board Risk Committee
- ❍ Board IT or Security Committee
- ❍ Other Board or Committee
- ❍ Management Committee
- ❍ They were not considered at a governance level
- ❍ Not applicable – there were no cyber attack occurrences

6.4 Have you considered how you would notify your customers or clients of a breach of their confidential data?

- ❍ Yes
- ❍ No

6.5 Are you confident in your organisation's ability to detect, respond and manage a cyber intrusion to minimise impact to your business?

- ❍ Very
- ❍ Somewhat
- ❍ Limited
- ❍ No

6.6 Does the organisation have a documented and approved response, recovery and resumption plan and is the plan tested?

- ❍ Yes, the plan is tested
- ❍ No, a plan is in place however it has not been tested
- ❍ No, there is no documented plan
- ❍ I don't know

7. Investment and Customer Data

7.1 Does the board review and challenge reports on the security of your customer's data?

- ❍ Yes
- ❍ No

7.2 What are the drivers for the priority of the Board's review of security reports?

- ❍ Upcoming legislation or regulatory reporting
- ❍ Concern about reputation with customers
- ❍ Investor concern
- ❍ The Board does not review security reports
- ❍ Cyber security is a key risk
- ❍ Other, please specify _____

Finally, please use this space if you would like to add any further comments about cyber security within your organisation:

Please click on the "Submit" button below to ensure your response is counted.

KPMG

Frequently Asked Questions (FAQ's)

ASX 100 Cyber Health Check

November 2016

1. *Who is behind this initiative?*

The Cyber Health Check is a key business led initiative that forms part of the Australian Government's Cyber Security Strategy. Participation in this initiative is encouraged by ASX & ASIC, in conjunction with Audit Firms, KPMG, Deloitte, EY, and PwC. A similar program in the UK was very successful in putting cyber resilience on the board agenda of the FTSE 350.

2. *How do I complete the survey?*

A partner from your Audit Firm will be interviewing you and assisting with facilitating the completion of the survey.

However, if you are unable to participate in an interview, you will be able to undertake the survey by contacting your Audit Partner to receive your unique identifier before going to *https://asx100healthcheck.questionpro.com* and completing it online. **Please note**, you will need to ensure you have a unique identifier so your results are apppropriately captured.

3. *What are the roles and responsibilities of the key players in the Cyber Health Check?*

- The Australian Government placed cyber security and resilience on the board agenda and outlined an initiative for ASX 100 organisations to participate in a Cyber Health Check as part of the Australian Government's Cyber Security Strategy.
- ASX will have ownership of the complete anonymised dataset that will be produced as a result of the Cyber Health Check. In addition, ASX will be facilitating the Cyber Health Check with the assistance of KPMG.
- KPMG has provided the online survey tool and is responsible for managing the online survey.
- The Big Four Audit Firms, KPMG, Deloitte, EY, and PwC will be interviewing and assisting with facilitating completion of the survey for their audit clients within the ASX 100 given their pre-existing audit relationship. They will also hold the unique identifiers for their clients for the purposes of providing confidential individual benchmark reports.

4. *Why should I respond?*

Protecting information assets is important to the sustainability and competitiveness of businesses. Cyber security is a strategic risk management issue for the Board, not one to be left solely to the IT Department. The intent of the 2016 Cyber Health Check is to raise awareness of cyber security at the Board level and share best practice approaches so that boards are more informed as they assess their own security capabilities and plans.

The benefits are wide ranging, including the ability to benchmark survey participants, helping other Australian companies see what 'good' looks like, and most importantly – helping to identify areas of where improvement is required. Participation will also reassure ASX 100 shareholders and the broader community that boards are taking the cyber risk seriously.

5. *Why is my company requested to participate in this initiative?*

The ASX 100 is a group of companies that are at threat from cyber risk – be it from IP theft, data destruction, or fraud. The ASX 100 constitutes a key group of companies which contribute significantly to Australia's economy. A focus on and sharing of approaches on cyber preparedness by this group is important leadership for the Australian business sector in addressing the cyber risk.

6. *My company is on top of cyber issues – so, what's the relevance to us?*

Your company will provide an influential data point for a cyber resilience benchmark that other boards might aspire to. The anonymous sharing of best practice is in the interests of Australia's economic prosperity. This survey may also uncover hitherto unknown vulnerabilities which open you up to a variety of new threats.

7. We actively engage with the security and intelligence community on cyber – so, why reach out to us?

You may have existing relationships with Government Departments or Agencies (e.g. Australian Federal Police (AFP), Australian Signals Directorate (ASD), Attorney-Generals Department (CERT Australia), Prime Minister & Cabinet (PMC), etc.), either at a technical or executive level – or both. The Health Check will not duplicate or conflict with any of these engagements. All of your Government cyber stakeholders will be aware of the Health Check and its objectives. If you choose to share the Health Check results with your existing Government cyber partners they may be able to optimise, enrich or complement those relationships.

8. When will the survey be ready? When will the interview take place?

The Survey will be available through a secured online platform on 9 November 2016. Your Audit Lead Partner will be in touch soon to arrange a time in November for the interview to take place. The target date for completing the survey is 16 December 2016. Whilst firms have the option of receiving a hard copy of the survey questions, they must all be completed online at https://asx100healthcheck.questionpro.com

9. What tool is used to collect the results?

QuestionPro is an internet based survey tool that will be used to collect results. As a sophisticated and reliable tool, QuestionPro captures the survey data and provides functionality to perform analysis and benchmarking.

QuestionPro ensures multiple layers of data security. KPMG Risk Management and the KPMG National Privacy Officer have recently reviewed the security and privacy aspects of QuestionPro to ensure they comply with Australian privacy requirements. For the purposes of this project KPMG also conducted a detailed IT security review. For detailed information relating to data security please refer to the document *Steps to Secure ASX 100 Cyber Health Check Data.*

10. How long will take it to complete the questionnaire?

We estimate that the interview will take approximately an hour and includes a mix of multiple choice and open questions.

11. How will the data be used? Is this confidential or anonymous?

This will be an anonymous questionnaire. Neither the Government nor the Audit firms will be able to see the identity of participants.

The Government will not host or have access to individual reports or identities. The Government will have an aggregated report which shows results across the ASX 100, but it will be anonymous.

The data will be stored on a secured platform that will be subject to a security review. Security has been tested by KPMG.

The anonymised results will help raise awareness of cyber threats and inform how the Government prioritises and targets its cyber security risk management advice. Once the survey and analysis is completed, the data will be deleted from the QuestionPro platform, and the entire de-identified raw dataset will be sent to the ASX to be the data custodians. Each of the four firms will also hold a copy of the anonymised data set.

12. How can I prepare for the interview? Can anyone assist me?

We encourage open and honest responses about this issue; so little preparation work is required.

The survey focuses on cyber risks and the boardroom. Whilst most of the day to day responsibilities for cyber are managed by a ‘Chief Information Security Officer’ or similar, where possible we seek responses from the Chairman or Audit Committee Chair or Risk Committee Chair.

13. I don't know all the answers, what should I do?

For the benchmarking reports to offer real insight, it is important that the answers to the questionnaire come from the Chairman, the Audit Committee Chair or the Risk Committee Chair. Both the Government and the audit firms are aware that a large section of this audience are not cyber security experts and that the level of discussion of cyber security risk at the Board level will vary between companies. Please remember, your answers will remain anonymous.

14. Would my CIO be the best person to undertake this?

We advise against the CIO or any other representative of the organisation completing the questionnaire. If they do, it will have an impact on the results and the subsequent benchmarking reports – which are solely focused on the governance of the cyber risk at Board level. CIO driven responses will impact on the accuracy of the results for the whole ASX 100 sample. They may also miss a governance link, which exacerbates a specific vulnerability.

15. Will you share the results? If so, when and how?

After submissions are completed, ASX, ASIC and the four Audit firms are targeting to produce a high level aggregate report to draw out the themes from the results of the questionnaire, along with a benchmark for companies that have participated. We expect the aggregated report to be available in March 2017 and released publicly. The individual benchmarking reports would be available to the Boards, via Audit Partners, shortly thereafter.

16. What will Government do with the results?

Government will not host or have access to individual company results data. The ASX is the custodian of the raw anonymised data set. This report will enable Government to see how cyber security is managed by boardrooms of the ASX 100 companies, and help it better target its corporate governance guidance and support as part of Australia's Cyber Security Strategy.

17. How should I deal with media queries?

You are encouraged to be supportive of this initiative. Success will be driven by participation. You may direct any enquiring press to call Matthew Gibbs, ASX General Manager Media and Communications (phone: +61 2 9227 0218, email: matthew.gibbs@asx.com.au) or Ian Welch, KPMG Senior Manager External Communications (phone: +61 2 9335 7765, email: iwelch@kpmg.com.au)

18. What are the next steps?

A partner from your respective Audit Firm will be in contact to arrange a date for the interview. The partner will work with you to clarify questions you may have and assist with completing the survey.

19. What happens after this?

After the interviews, an industry report and benchmark will be produced which will equip boards and audit committees with a greater understanding of where specific vulnerabilities may exist within their companies.

20. Who do I contact if I have problems with the service?

If you experience any problems with the service, you can contact either your Audit Firm, or contact the general inquiries inbox AU-FMCyberhealthchec@kpmg.com.au

For any further information on the survey tool or process, you're welcome to contact KPMG's National Cyber Partner, Gordon Archibald on garchibald@kpmg.com.au or KPMG's Research Lead, Nicola Hassan on nicolahassan@kpmg.com.au