

Dieter Schutte  
Head of Cyber Security  
Super Retail Group Services Pty Ltd  
6 Coulthards Avenue  
Strathpine QLD 4500

21<sup>th</sup> September 2022

Dear Dieter,

## Re: RFQ Penetration Testing Services

Thank you for providing Deloitte Risk Advisory Pty Ltd ("**Deloitte**") with the opportunity to assist Super Retail Group Services Pty Ltd ("**SRG**") with security testing services to assess & identify potential exposure to cyber threats. This engagement letter sets out the scope of the services and the terms and conditions (enclosed with this letter) under which we will provide the services to you.

We understand that you, Dieter Schutte, will be your nominated contact and will instruct us in relation to the Services.

### 1 Background

We understand that SRG requires a penetration test for their web applications. The objective of this security assessment is to identify security weaknesses within SRG web applications and provide the opportunity to achieve security in depth.

The security assessment will assist SRG in determining security weaknesses and their root causes and whether current security controls are appropriately designed and operating to mitigate risks associated with web applications.

### 2 Our Engagement

Deloitte will conduct the following activities ('Services'):

To ensure that you can effectively protect against cyber threats, we will structure and tailor our testing to fit your environment. In line with this approach, the activities proposed for this security assessment will cover the following areas:

- Web Application Penetration Test

This will allow Deloitte to assist SRG in identifying and understanding the key risks and security vulnerabilities associated with its current environment. The scope within which we will conduct these activities is detailed in the sections below.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organisation"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

The Australian partnership of Deloitte Touche Tohmatsu is a member of Deloitte Asia Pacific Limited and the Deloitte organisation. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, risk advisory, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at <https://www2.deloitte.com/au/en.html>.

Liability limited by a scheme approved under Professional Standards Legislation.

**Confidential - this document and the information contained in it are confidential and should not be used or disclosed in any way without our prior consent.**

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

© 2022 Deloitte Risk Advisory. Deloitte Touche Tohmatsu

**CONFIDENTIAL**

## 3 Scope of Services

The following outlines the scope of our engagement which is limited to the matters set out in this letter. So that we can assist you effectively, please ensure that you are satisfied that the scope of our engagement and the Services we will provide is sufficient for your needs. If you wish to discuss this with us further, please let us know.

As part of the security assessment, the activity will cover the following areas:

### 3.1 Web Application Penetration Test

The primary purpose of web application penetration testing is to identify and exploit vulnerabilities present in a web application and its components, including the associated infrastructure, and recommend practical solutions to make applications and systems under the scope of engagement more secure.

During testing, we will use a web browser and penetration testing tools that mimic normal client activity as well as generate malicious traffic. Our penetration testing assessment methodology incorporates the suggested testing techniques from standard methodologies, such as the Web Application Hackers Handbook (WAHH) and the OWASP Security Testing Guidelines v4.1.

These methodologies will cover many aspects of a web application, and any customisation of further testing will be evaluated during the testing period. The use of these methodologies also covers those common vulnerabilities as highlighted in the OWASP Top 10 2017 and OWASP Top 10 2021, OWASP Top 10 2021, NIST SP 800-115, PTES.

Some of the specific test cases that will be covered for this testing are listed below:

- **Privilege escalation via forceful browsing** Performing administration actions using lower privileged accounts or as unauthenticated users.
- **Insecure upload functionalities** Uploading malicious executables via insecure file upload functionalities, such as firmware updates or configuration deployments.
- **Authentication & password policy** Enumerate default usernames and passwords within management consoles.
- **Input validation** Issues such as SQL injection, HTTP request header manipulation, HTTP GET and POST parameters, Insecure Deserialization, etc., may lead to sensitive information disclosure or account compromises.

Furthermore, besides manual testing, we will use a number of automated tools that are designed to detect vulnerabilities in web applications such as Burp Suite and Nikto.

Application	Comments
<ul style="list-style-type: none"> <li>• BCF Web Application <b>URL: TBD</b></li> <li>• Macpac Web Application <b>URL: TBD</b></li> <li>• Super Retail Group Web Application <b>URL: TBD</b></li> <li>• Careers Super Retail Group Web Application <b>URL: TBD</b></li> </ul>	Testing to be performed in a non-production (i.e. staging) environment.

### 3.2 Exclusions

For the avoidance of doubt, the Services:

- Do not include the implementation of any recommendations contained in our report

- Do not constitute a source code review. However, during this engagement, we may reveal and analyse underlying application code (through reverse engineering) for the identification and exploitation of vulnerabilities or weaknesses.

Further, the following areas are specifically excluded from the test:

- Business as Usual ("BAU") processes, such as patch management, change management, and access control.
- Test or review of any control, feature, software package, or operating system not defined in the Services.
- Configuration review of any feature, device, software package or operating system not defined in the Services.
- Source code or development processes security review.
- Denial of Service ("DoS") exploitation, physical security and social engineering.
- Business partner systems or transmission security within any service provider's network; and
- Any other test not explicitly defined in the Services.
- Assess any other applications or back-end systems (e.g., ERP) not defined in this letter.
- Deliver formal training or develop training materials as part of the inclusive consulting hours.
- Implement any recommendations contained in our report.

### 3.3 Requirements for Testing

To complete the specific tasks in the most effective way, the following information is required prior to the start of each activity. Additional information may be required during the project execution, and Deloitte will contact your designated contact as soon as possible to facilitate the activities.

Activity	Information requirement
<b>General Requirements</b>	<ul style="list-style-type: none"> <li>• Provide project manager and technical contact details.</li> <li>• Testing will be performed from Deloitte Melbourne Lab IP. Whitelist Deloitte's Melbourne Lab IP <ul style="list-style-type: none"> <li>◦ 123.103.205.58</li> </ul> </li> </ul>
<b>Web Application Penetration Test</b>	<ul style="list-style-type: none"> <li>• Provide the URL for testing.</li> <li>• Specify any maintenance windows that might be applicable to the environment.</li> <li>• Request authorisation for penetration testing if targeted systems are managed by a third party.</li> <li>• Provide testing products and card information for the e-commerce websites in-scope.</li> </ul>

## 4 Deliverables & Outcomes

We will provide you with the advice and materials, including reports, documents, advice, e-mails, notes, or other deliverables ("Work") described below:

### 4.1 Security Assessment Report

We will provide you with a report detailing the results of the testing performed. This report will include the following key sections:

- **Executive Summary:** Directed at executive management – A general overview of the security level of the systems tested, including significant vulnerabilities and areas where the general approach to security needs to be improved. We explain the implications of our findings within the business context of SRG and provide an overall rating of security within the environment tested.
- **Summary of Findings:** Directed at operational management – A more detailed breakdown of the vulnerabilities and weaknesses identified for each portion of the engagement. We provide an explanation of the finding, as well as the associated risk to your business.
- **Detailed findings:** Directed at operational management and technical staff – A detailed description of exposures and their context, together with supporting documentation. We assess the impact and associated business risk of each identified exposure and make prioritised technical recommendations to be implemented to address the identified exposures. The priorities and 'Detailed findings' section will also be supported by technical appendices where required.

## 4.2 End of Test Debrief

On completion of the engagement, we will hold an end-of-test debrief with you to allow us to present our preliminary findings and answer any initial questions or concerns that you may have relating to the security weaknesses identified. The session would also provide an informal opportunity to demonstrate any specific findings (where possible) or discuss any recommended remediation activities that could be implemented to mitigate the identified risks.

This session will also assist us in better understanding the business risk and help us rate the risk levels appropriately. This is particularly important for any critical risk security weaknesses or areas where a quick tactical fix may be required.

## 4.3 Use of Deliverables

Our Work is for your exclusive use and must be used only by you and only for the Purpose set out in this engagement letter. We accept no responsibility to anyone (apart from you) who is provided with or obtains a copy of our Work without our written agreement. We reserve the right to include in our Work a statement limiting the use to which the report may be put, any limitations on the scope of the Services performed, and setting out the respective responsibilities of SRG and Deloitte.

## 4.4 Re-Test of Critical, High and Medium Findings

Re-testing of any Critical, High and Medium Findings that have been remediated within 8 weeks of the End of Test Debrief will be provided. The original Assessment Report will also be updated to highlight the re-test results.

## 4.5 Additional Services

During this engagement, SRG may request that Deloitte perform additional Services that are not encompassed by this engagement letter. Deloitte may perform such additional services subject to the approval of a representative of SRG either under a variation to this letter, or, if necessary, on receipt of a separate signed engagement letter with terms and conditions that are acceptable to SRG.

## 5 Our Team

Henry Peens is the partner who is primarily responsible for the Services. Andy Yang will oversee the day-to-day running of the Services, with assistance from an experienced team. From time to time, we may need to include other partners and staff to assist us in providing our Services to you. Our penetration testers have extensive experience in the security assessment of web applications, infrastructure, network, mobile application, and maintain a variety of the most valuable industry recognised certifications from the Council of Registered Ethical Security Testers (CREST), Offensive Security, and SANS.

## 6 Our Fees

The fixed fee payable for the Services is **\$24,800** (excluding GST and Expenses), including one re-test (section 4.4). The estimated costs for each service are described in the table below:

Service	Effort (days)	Total (excl. GST)
Web Application Penetration Test	16	\$ 24,800
Re-test	2	Invested
<b>Total (excl. GST)</b>		<b>\$24,800</b>

### 6.1 Billing Schedule

We will send you our final invoice for all outstanding services provided upon the delivery of our final report.

## 7 Standard Business Terms and Conditions

This letter and our standard terms and conditions (the "Terms"), which are enclosed, set out the basis on which we will provide our Services to you. Where an inconsistency arises between this letter and the attached Terms, the terms set out in the letter will prevail.

### 7.1 Assumptions

We will provide the Services on the following assumptions:

1. Our services:
  - i. Will be purely advisory and consulting in nature,
  - ii. Cannot be relied upon to disclose fraud, other illegal acts, or errors which may exist; however, we will inform you of any such matters as come to our attention in the performance of our Services.
2. External testing against the SRG environment will be conducted locally from the Deloitte penetration testing labs in Adelaide, Brisbane, Melbourne, or Sydney.
3. Where testing is agreed to be performed in a non-production environment, SRG will provide a test environment that is close to production for the testing. Additionally, the test environment will have some test data populated to emulate how the application normally behaves.
4. SRG will obtain the necessary written authorisations from their Cloud Services / Third Party Hosting provider for Deloitte to conduct testing against the SRG -owned applications/infrastructure on SRG's behalf.
5. Deloitte security testing activities will be time-boxed and sample-based, and as such, not every control, page or field within the systems in scope will be tested.
6. SRG will provide Deloitte with a dedicated contact to allow Deloitte to notify SRG in the event that the provided environment or application becomes unresponsive during testing.
7. SRG must provide Deloitte with details of any critical or fragile systems that should not be included in security testing activities and must inform Deloitte of any critical periods where testing should not be undertaken.
8. Once the test dates have been agreed, any alteration to the test window must be communicated to Deloitte in writing at least 5 days in advance. Failure to provide adequate notice of delays or alterations may result in additional charges.

9. Should testing occur on a third-party or externally hosted system or application, a letter of approval will be required from the third-party/vendor prior to the commencement of testing.
10. Our services will be subject to the limitations inherent in any test of the vulnerability of networks and applications set out below.
11. We will at our own cost, ensure that Deloitte and its employees, agents and contractors comply with your [Responsible Sourcing Policy](#) & [Responsible Sourcing Code](#).

## 7.2 Inherent Limitations

Security testing has a number of limitations that must be understood to ensure the correct interpretation of the results:

- a) Testing is usually restricted to a number of discrete tests which are performed during a small window of time. Where possible, Deloitte will identify additional tests which could be performed, but will not perform these without agreement from you.
- b) Vulnerability testing is often performed in isolation, with very little background information on the nature of the system or systems that are tested (also referred to as “blind” testing). In this case, the tester will make a number of attempts to obtain information about the systems and any associated vulnerabilities.  
  
This type of information is usually cryptic and incomplete, requiring the tester to interpret the data available in order to state their findings. The results are therefore a skilled interpretation of incomplete information and not a statement of fact. We cannot warrant that the information obtained is accurate or complete. The tester’s results should not be relied on in isolation but as an important and necessary factor in your overall assessment of your security measures and the application’s potential vulnerabilities.
- c) Testing in live or production environments will require a modified approach and restriction the use of tools or techniques that may cause an adverse impact to the environment. More restricted testing may result in gaps or areas of the environment, which cannot be properly evaluated.
- d) The tester will be unaware of the composition of your network, and whilst this may increase the risk of damage to your software and data, this is an aspect of the testing.
- e) We do not perform destructive tests during a vulnerability test; however, if we identify potential vulnerabilities to require such an attack and the nature of the vulnerability, we will inform you.
- f) The information obtained and the results provided are only current at the time of testing (results represent a snapshot in time). New vulnerabilities will arise continually. It is therefore critical that patches are kept current, and security audits and vulnerability tests are performed regularly.
- g) We will assume that Information provided by you is complete and accurate, and will not subject such Information to testing except as described in this engagement letter.

## 7.3 Impact of Testing

You acknowledge that our Work within the scope of this Agreement may cause disruption to your network, systems, and processes. We will make reasonable efforts to limit the impact of testing on your network, subject to which you acknowledge and agree that we will not be responsible for network or other disruption from testing which falls within the scope of this Agreement.

You agree to defend, indemnify and hold harmless Deloitte, its partners, and employees from and against any and all third party costs, expenses, demands, actions, suits, or proceedings paid, incurred or suffered by or made or initiated against them or any third party arising out of or in connection with our Services.

## 7.4 Your Responsibilities

1. In addition to the responsibilities set out in section 11 of the attached Terms, you acknowledge that SRGp is, and will continue to be, solely responsible for:
  - a) Making all management decisions and performing all management functions, including but not limited to authorising the Deloitte Services described herein.
  - b) All decisions in connection with the implementation of any advice and recommendations raised as part of the Services.
  - c) Establishing, maintaining, and enforcing appropriate procedures and associated access controls and other technology measures over its systems and operations, including, without limitation, systems designed to achieve its control objectives, financial reporting, monitoring of ongoing activities, and systems designed to achieve compliance with applicable laws and regulations.
  - d) Providing in a timely manner all network, environment, programs, information, and data as required by Deloitte to perform the Services and its obligation under the Terms.
  - e) Informing Deloitte in a timely manner of any need to change the testing schedule.
  - f) Obtaining all authorisation, consent from, and notifying third parties that may be directly affected by this engagement of Deloitte's activities.
  - g) Taking the necessary precautionary steps to ensure that the vulnerability testing will not, or will not be likely to, interfere with the functioning or availability of SRG systems prior to the testing commencing. Such steps should include but may not be limited to:
    - I. Preparing backups of all data, configurations, programs, networks, and systems that could be exposed to the vulnerability testing to enable your staff to restore your systems to the state in which they were prior to the vulnerability testing.
    - II. Updating and patching systems in accordance with current manufacturer and vendor recommendations.
    - III. Having your key support staff available during the vulnerability testing.
  - h) Designating a competent employee with substantial computer systems, network and project management experience, preferably within senior management, to oversee the Services hereunder on behalf of SRG and act as a point of contact for Deloitte.
  - i) Ensuring its personnel fully cooperate with Deloitte personnel to enable Deloitte to perform the Services.
  - j) Evaluating on behalf of SRG, the adequacy and results of the Services.
  - k) Approving all assumptions underlying the performance of the Services as identified in this letter and as may arise during the provision of the Services.
  - l) Accepting responsibility for the results of the Services provided they are properly performed by Deloitte.
2. You warrant that any IP addresses provided to Deloitte for testing are owned by, or licensed to, and used exclusively by SRG.
3. In connection with the Services, Deloitte shall be entitled to rely on all decisions and approvals by SRG.
  1. You acknowledge and agree that:
    - a) Our ability to perform the Services and to meet any reporting deadlines is dependent on you meeting your responsibilities, obtaining all required authorisations and consents, as well as you providing us with reasonably detailed instructions, and making timely decisions
    - b) Our testing Services may cause disruption to your systems and processes. While we will make every reasonable effort to limit the impact of our testing on your network, you acknowledge and agree that we will not be responsible for network or application disruption from testing, which falls within the scope of this Agreement. We will

immediately suspend the Services if we become aware of disruptions to your network or applications as a result of the Services and will notify you to obtain instructions on whether or not to continue testing.

2. SRG represents and warrants that any access or use of SRG's network, environment, programs, information (including but not limited to personal information as defined under the Privacy Act 1988 (Cth)), and data as required to perform the Services will not:
  - a) constitute unauthorised access or otherwise breach the Terms; or
  - b) contravene the *Criminal Code Act 1995* (Cth), the *Crimes Act 1900* (NSW) and equivalent State or Territory legislation.

## 8 Term

The estimated dates on which this testing will take place are:

- **Test Commencement:** To be updated
- **Estimated Test Completion:** To be updated

We will use reasonable efforts to ensure that our Representatives named in the Letter are available to provide the services. However, if we need to, we may replace or reassign any Representative at any time on reasonable notice to you.

## 9 Acceptance

The scope of our engagement is limited to the tasks set out above. If the scope of the Services do not meet your needs, please let us know so that we can vary this letter and our fees accordingly.

Please confirm that you agree to these terms by signing, dating and returning the enclosed copy of this letter to us. Please contact me at +61 433 710 434 or Ashish Mahajan at +61 428 280 129 if you would like to discuss this letter and the terms of engagement with us.

We look forward to working with you.

Yours sincerely,



**Henry Peens**

Partner

Deloitte Risk Advisory Pty Ltd



Sign off by recipient:

Super Retail Group Services agrees to the terms of this Agreement. Signed for and on behalf of Super Retail Group Services by its duly authorised representative:

  
\_\_\_\_\_  
Signature

*10 . October, 2022*  
\_\_\_\_\_  
Date

*KEVIN FIGUEIREDO*  
\_\_\_\_\_  
Name

*GM RISK, SAFETY & SUSTAINABILITY*  
\_\_\_\_\_  
Title

## Standard Terms and Conditions

### 1. This Agreement

This Agreement sets out the terms on which we will provide the Services to you. Where the Letter is addressed to more than one Addressee, each Addressee is a party to, and is bound by, the terms of this Agreement. We will treat you as having accepted this Agreement if you continue to instruct us after you receive it.

### 2. Term

This Agreement starts on the date you sign and return the Letter to us or when we first start work on the Services for you, whichever is first. Unless it is terminated earlier, this Agreement terminates when we have completed providing the Services to you and you have paid us our Fees.

### 3. Our Services

- 3.1 We will provide the Services to you in accordance with this Agreement and with the degree of skill, care and diligence expected of a professional providing services of the same kind.
- 3.2 We will use all reasonable efforts to complete the Services within any agreed time frame.

### 4. Our team

- 4.1 We will use reasonable efforts to ensure that our Representatives named in the Letter are available to provide the Services. However, if we need to, we may replace or reassign any Representative at any time on reasonable notice to you.
- 4.2 Each of us agrees that, during the term of this Agreement and for a period of six months after it ends, neither of us will directly or indirectly solicit for employment any Representative of the other who is involved with the Services. However, both of us may advertise or recruit generally.

### 5. About Deloitte

- 5.1 We are a Member Firm of DTTL. Accordingly, you acknowledge that:
  - (a) each of the Member Firms is a separate and independent legal entity operating under the names “Deloitte”, “Deloitte & Touche”, “Deloitte Touche Tohmatsu” or other related names;
  - (b) the Services are provided by us and not by DTTL or any other Member Firm; and
  - (c) neither DTTL nor any of the Member Firms is liable for each other’s acts or omissions.
- 5.2 Sometimes we may use other Member Firms to help us to provide the Services to you. Where this happens, we will be responsible for any work undertaken by another Member Firm and you agree that:
  - (a) none of the Member Firms, apart from us, will be responsible to you; and
  - (b) you will not bring any claim or proceedings in connection with the Services or this Agreement against any of the other Member Firms that we may use to provide the Services to you.
- 5.3 Any Member Firm that helps us to provide the Services to you will rely on subclause 5.2 and is, to the extent permitted by the Law of any relevant jurisdiction, an intended third-party beneficiary of, and entitled to enforce this Agreement as if it were a party to it.
- 5.4 If we provide you with Licensed Services, you acknowledge that:
  - (a) the relevant Licensed Entity will provide the Licensed Services directly to you;
  - (b) Deloitte enters into this Agreement as agent for the Licensed Entity; and
  - (c) the terms of this Agreement apply to the Licensed Services.

### 6. Confidentiality

- 6.1 Each of us agrees to protect and keep confidential any Confidential Information that is given to us by the other.
- 6.2 Except as set out in this Agreement, or where both of us agree otherwise in writing, we will only use or disclose your Confidential Information to provide the Services to you or other services you may request.

- 6.3 Where relevant, we may use, disclose and transfer your Information to other Member Firms and our Representatives, who will use and disclose it only to provide the Services to you.
- 6.4 We may disclose your Information to our own professional advisers and insurers on a confidential basis.
- 6.5 Subject to subclause 6.6, either of us may disclose any Confidential Information to the extent that it is required to be disclosed by Law, order of any court, tribunal, authority or regulatory body, rules of any stock exchange or any professional obligations or requirements.
- 6.6 A party disclosing any Confidential Information under subclause 6.5 must, where practical and to the extent permitted by Law, notify the other of the requirement to disclose and only disclose the minimum Confidential Information required to comply with the Law or requirement.
- 6.7 You agree that we may aggregate your Information and use and disclose that information in de-identified form as part of research and advice, including, without limitation, benchmarking services.
- 6.8 We will return your Information to you at any time at your request. We may also destroy it if you ask us to. However, we are entitled to retain a copy of any Information you provide to us or which forms part of our Work or our Working Papers, provided that we will continue to keep this Information confidential in accordance with this Agreement.

### 7. Personal Information and privacy

- 7.1 We will handle Personal Information in accordance with the Privacy Act and our privacy policy available at [http://www.deloitte.com/view/en\\_AU/au/privacy/index.htm](http://www.deloitte.com/view/en_AU/au/privacy/index.htm).
- 7.2 You agree to work with us to ensure that both of us meet any obligations that each of us may have under the Privacy Act including, where relevant, notifying the individual to whom the Personal Information relates of who we are and how we propose to use and disclose their information.
- 7.3 Where you provide us with any Personal Information, you confirm that you have collected the Personal Information in accordance with the Privacy Act, that you are entitled to provide the Personal Information to us and that we may collect, use and disclose the Personal Information for the purpose of providing the Services to you or as otherwise permitted by this Agreement.

### 8. Intellectual Property

- 8.1 Unless we agree otherwise, we will retain ownership of the Intellectual Property in our Work. We give you a royalty-free, non-exclusive, perpetual, world-wide licence to use and reproduce any Reports for the Purpose for which the Report was prepared and any related incidental internal purposes in accordance with the terms of this Agreement.
- 8.2 You agree we can use your logos and marks on our Work, unless you tell us otherwise.

### 9. Our Work

- 9.1 Our Work is for your exclusive use and must be used only by you and only for the Purpose.
- 9.2 Unless we give our Consent:
  - (a) our Work must not be used or disclosed for any other purpose or made available to any other person, except your Professional Advisers and Auditor, on the terms discussed in subclause 9.3, or except to the extent permitted by subclause 6.5;
  - (b) our Work and the Services may not be relied on by anyone other than you; and
  - (c) you must not name us or refer to us, our Work or the Services in any written materials (other than to your Professional Advisers and Auditor), or any publicly filed documents, except as required by Law.
- 9.3 You may provide a copy of our Report to:
  - (a) your Professional Advisers and Auditor, provided that you ensure that each Professional Adviser and Auditor:
    - (i) is aware of the limits placed on the use of our Report by this Agreement, including that they may not rely on the Report;
    - (ii) for the Professional Adviser, uses our Report only to advise you in relation to the Services or, for the Auditor, uses our Report only in conducting the Audit; and

- (iii) treats our Report as confidential and does not use or disclose our Report in a manner that is not expressly permitted by this Agreement;
  - (b) any other person who is acceptable to us, with our Consent, but only where that person has first executed an agreement provided by us.
- 9.4 We are not responsible to anyone (apart from you) who is provided with or obtains a copy of our Work without our Consent.
- 9.5 If we give you our Work in draft form or orally, we do so only on the basis that you may not rely on it in that form. Accordingly, we will not be responsible if you or anyone else relies on our draft Work or oral comments or advice.
- 9.6 You acknowledge that the final or signed copy of our Report is the definitive version.
- 9.7 Sometimes, circumstances may change after we have provided our final Work to you; unless we agree with you otherwise, we will not update any final Work we have provided to you.
- 9.8 You acknowledge that any use of or reliance on our Work that is contrary to this Agreement may expose us to a claim from someone with whom we have no relationship or whose interests we have not considered in providing the Services.
- 9.9 Accordingly, you agree to indemnify us against any Loss we may suffer or incur in respect of any claim or action by a third party that arises as a result of:
  - (a) any use or distribution of, or reliance on, our Work that is contrary to the terms of this Agreement or a Consent; or
  - (b) any access to or use of our Work, by any of your Professional Advisers or Auditor.
- 9.10 This indemnity does not apply to any Loss incurred in defending a claim or action by a third party:
  - (a) that results from any wilful misconduct or fraudulent act or omission by us;
  - (b) where that third party has signed an agreement with us that provides that it can rely on our Work; or
  - (c) where we have agreed in writing that our Work may be included in publicly available documents.

## 10. Our Fees

- 10.1 The Fees and the basis on which they are calculated are set out in this Agreement. We may review the Fees where:
  - (a) an Unexpected Delay occurs;
  - (b) there is a change in the scope of the Services we agreed to provide to you; or
  - (c) you do not accept this Agreement within three months of the date of the Letter.
- 10.2 You agree to pay us the Fees for the Services in accordance with this Agreement.
- 10.3 Unless we state otherwise, our Fees exclude GST. You agree to pay any GST imposed on us, now or in the future, in relation to this Agreement. Where GST is payable on any taxable supply made under this Agreement, you agree that the Fee payable for this supply will be increased by an amount equivalent to the GST payable by us in respect of that supply.
- 10.4 We will charge you at cost for any expenses we incur in providing the Services to you. We will tell you what these expenses are before we incur them if they are anything other than incidental.
- 10.5 Unless we agree with you otherwise, we will use business class (or equivalent) for travel overseas and between the east and west coasts of Australia, and economy class for travel within the rest of Australia.
- 10.6 We will also charge you an administration, overhead and telecommunications charge, which is calculated at 5% of our Fees. This charge covers all our out-of-pocket expenses such as telecommunications, stationery and postage.
- 10.7 We will invoice you monthly in arrears for the Fees (unless we agree with you otherwise) and you agree to pay our invoice within 14 days of receiving it. You agree to pay any undisputed portions of an invoice even if there is a dispute between us about that invoice or another invoice. Where amounts remain due and unpaid we may charge you interest at an annual rate of 2% over the Bank Bill Swap Rate published in the Australian Financial Review on the date payment is due.
- 10.8 Without limiting any other rights we may have, we are entitled to suspend or terminate the Services, in whole or part, or to retain or withhold any Information we may hold in relation to the Services or any Work we have done for you if you do not pay our invoices on time.

- 10.9 If we are required to provide Information about you or the Services to comply with a statutory obligation, court order or other compulsory process, you agree to pay all of our reasonable costs and expenses we incur in doing so.

## 11. What you agree to do

- 11.1 You agree to co-operate with us and provide us with all reasonable and necessary assistance so that we can provide the Services to you. This includes providing us with timely and reasonable access as appropriate, to your premises, facilities, Information and Representatives.
- 11.2 In addition to any responsibilities you may have that are set out in the Letter, you are responsible for:
  - (a) the performance of your Representatives;
  - (b) making timely decisions in connection with the Services;
  - (c) designating a competent employee to oversee the Services;
  - (d) evaluating the adequacy of the Services, as they have been described in the Letter, for your particular purposes and needs;
  - (e) providing us with accurate and complete Information. Where any Information that we require in order to provide the Services is to be provided by someone else, you are responsible for ensuring that Information is provided to us. You will need to give us all Information that is relevant to the Services, even if the same Information has been given to us previously during another engagement; and
  - (f) updating any Information where there has been a material change to that Information, including telling us if any of your circumstances change during the course of the Services.
- 11.3 You acknowledge that:
  - (a) the Services may include advice and recommendations, but all decisions in connection with the implementation of such advice and recommendations will be your responsibility, and made by you;
  - (b) our ability to provide the Services depends on you meeting your responsibilities under this Agreement and instructing us or responding to our requests in a timely and effective manner; and
  - (c) we are entitled to and will rely on Information provided by you, the decisions you make and any approvals you give; and
  - (d) we will not be liable for any default that arises because you do not fulfil your obligations.

## 12. Unexpected Delay

- 12.1 We are not responsible to you or anyone else for any failure in providing the Services caused by an Unexpected Delay. We will tell you if there is a delay that will affect the Services and the cause of the delay, if known. You acknowledge that this Agreement will be varied to include any change to the scope of the Services, the Fees or the timeframes for completion of the Services if any delay requires it.
- 12.2 If we are required to perform additional services because of an Unexpected Delay, then this Agreement will also be varied to include those additional services and any additional Fees that apply.

## 13. Our responsibility to you

- 13.1 We are subject to a limitation of liability scheme approved under Professional Standards Legislation. Our aggregate liability to you is limited in the manner provided by the scheme. Please contact us if you require a copy of the relevant scheme.
- 13.2 Where the law requires it, our liability to you will not be limited. Where our liability is not limited by a scheme our aggregate liability to you for any Loss or causes of action arising in relation to this Agreement, including for negligence, is limited to the amount that is the lesser of ten times our Fees and \$20 million.
- 13.3 We will be liable to you only for that proportion of the total Loss that we have caused or to which we have contributed and we will not be liable for any Consequential Loss.
- 13.4 We will not be liable for any Loss, or failure to provide the Services, which is caused by an Unexpected Delay or which arises as a result of us relying on any false, misleading or incomplete Information.
- 13.5 The limit of liability set out above applies to all Addressees as a group and it is up to you to agree how the limit is allocated between you. You agree not to dispute the limit if you are unable to agree on how it will be allocated between you.

## 14. Conflict of interest

We have relationships with many clients. This means that after this Agreement starts we may identify circumstances that could cause us to have a conflict of interest. If this happens, we will evaluate the potential conflict and, depending on the circumstances, apply appropriate safeguards to manage it. For example, we may notify you of a

relationship that causes us a conflict and ask for your consent to continue to provide you with the Services. However, you acknowledge that we may need to terminate this Agreement if we are unable to resolve or manage a conflict of interest satisfactorily.

## 15. Insurance

We will maintain appropriate insurance in relation to the Services, including professional indemnity insurance in an amount of not less than \$10 million during the term of this Agreement and for a period of seven years after it ends.

## 16. Termination

16.1 Either of us may terminate this Agreement:

- (a) at any time by giving the other 30 days' written notice; or
- (b) immediately if the other suffers an Insolvency Event, is unable to pay all of its debts as and when they become due and payable, suspends payment of such debts or otherwise ceases to carry on business; or
- (c) immediately if the other commits any material breach of this Agreement that is either incapable of being remedied or is not remedied within 14 days of receipt of a notice requiring the breach to be remedied.

16.2 We may terminate this Agreement if:

- (a) you fail to meet your obligations under this Agreement including to pay our Fees within the time specified or to provide us with adequate Information or instructions; or
- (b) there is a change of circumstances beyond our reasonable control (such as auditor independence or regulatory related developments) that prevents us from providing the Services to you.

16.3 If this Agreement is terminated:

- (a) you agree to pay us the Fees for any work we have done and any expenses we have incurred up to the date of termination;
- (b) except as set out in this Agreement, and only where relevant, each of us will return to the other any documents or property of the other, except that we may retain one copy of all Information to allow us to satisfy our professional obligations and record keeping requirements;
- (c) the termination does not affect any accrued rights of either of us or any provision of this Agreement that continues to apply.

16.4 The provisions of this Agreement that survive its termination include those relating to clause 5, *About Deloitte*; clause 6, *Confidentiality*; clause 7, *Personal Information and privacy*; clause 8, *Intellectual Property*; clause 9, *Our Work*; clause 10, *Our Fees*; clause 13, *Our responsibility to you*; clause 15, *Insurance*; subclause 16.3, *Termination*; clause 17, *Dispute resolution*; and clause 18, *Disclosure of Tax Advice*.

## 17. Dispute resolution

17.1 Each of us agrees to use reasonable endeavours to resolve any dispute that arises in connection with this Agreement by mediation before bringing a legal claim or starting legal proceedings against the other.

17.2 Nothing in this clause prevents either of us from seeking any equitable relief in relation to our rights under this Agreement.

## 18. Disclosure of Tax Advice

In relation to Tax Advice and in compliance with Disclosure Laws, it is acknowledged and agreed that nothing contained in this Agreement shall be construed as limiting or restricting your disclosure of Tax Advice. It is also understood that none of your other advisers will or have imposed any conditions of confidentiality with respect to Tax Advice. Copies of any Tax Advice provided to others is on the basis that such recipients may not rely on such Tax Advice and that we owe no duty of care or liability to them, or any other persons who subsequently receive the same. Except as set out in this clause, all other terms of this Agreement remain unamended.

## 19. Relationship between the parties

We are engaged as an independent contractor. Neither of us is an agent or representative of or has the authority to bind the other. Neither of us will act or represent ourselves, directly or by implication, as an agent of the other or in any manner assume or create any obligation on behalf of, or in the name of, the other. This Agreement is not intended and will not be taken to constitute a partnership, agency, employment, joint venture or fiduciary relationship between us.

## 20. Entire agreement

20.1 This Agreement is the entire agreement between us for the Services. It supersedes all prior communications, negotiations, arrangements and

agreements, either oral or written between us in relation to its subject matter.

20.2 Any changes to this Agreement must be agreed to in writing by both of us.

## 21. Assignment

Neither of us may transfer, assign or novate this Agreement without the Consent of the other. However, we may assign this Agreement to any entity in Deloitte Australia or any successor to our business.

## 22. Electronic communication

Each of us agrees that we may communicate with each other electronically. You acknowledge that electronic transmissions are inherently insecure, can be corrupted or intercepted, may not be delivered and may contain viruses. Neither of us is responsible to the other for any loss suffered in connection with the use of e-mail as a form of communication between us.

## 23. Severability

If any of the terms of this Agreement are not legally enforceable then that term or the relevant part of it will be either amended as appropriate to make it enforceable or ignored, but in all other respects this Agreement will have full effect.

## 24. Governing Law

This Agreement is governed by the Laws of New South Wales and each party irrevocably submits to the jurisdiction of the courts exercising jurisdiction in that State.

## 25. Your feedback

We value your feedback. We aim to obtain, either formally or informally, a regular assessment of our performance. If you wish to make a complaint, please refer to the Complaints Management Policy available at [http://www.deloitte.com/view/en\\_AU/au/index.htm](http://www.deloitte.com/view/en_AU/au/index.htm) or write to the Complaints Officer at [complaints@deloitte.com.au](mailto:complaints@deloitte.com.au).

## 26. General

26.1 A waiver by one of us of a breach by the other party of any term of this Agreement does not operate as a waiver of another term or a continuing breach by the other of the same or any other term of this Agreement.

26.2 To the extent permitted by Law, we disclaim all warranties, either express or implied, in relation to the Services and the Work other than any written warranty made in the Terms.

26.3 The rights and remedies in this Agreement are cumulative and not exclusive of any rights or remedies provided by Law.

## 27. Reading this Agreement

In this Agreement:

- (a) headings are for convenience only and do not affect how this Agreement is interpreted;
- (b) the singular includes the plural and conversely;
- (c) the word person includes an entity, a firm, a body corporate, an unincorporated association or an authority;
- (d) a reference to this Agreement or an act or instrument is to this Agreement, or that act or instrument as amended, varied, novated or replaced from time to time;
- (e) a reference to dollars or \$ means Australian dollars;
- (f) an Annexure forms part of this Agreement; and
- (g) if there is any conflict between these Terms and any other part of this Agreement, the following order of priority will apply:
  - (i) the Letter;
  - (ii) the Annexure; and
  - (iii) the Terms.

## 28. Definitions

In this Agreement the following words have the meanings set out below:

**Addressee** means each person to whom the Letter is addressed and includes, where relevant, any additional parties who may agree to the terms of this Agreement.

**Agreement** means the Letter and the Terms.

**Annexure** means a document which is annexed or attached to the Letter and identified as an annexure or attachment to it

**Audit** means an audit under the *Corporations Act 2001* (Cth) or an equivalent Law, conducted in accordance with relevant auditing standards.

**Auditor** means an auditor who is appointed to conduct an Audit of you.

**Confidential Information** means and includes:

- (a) the terms of this Agreement and the details of the Services;
- (b) any information or material which is proprietary to a party or acquired by either of us solely as a result of the Services;
- (c) any Intellectual Property and methodologies and technologies that:
  - (i) you use in your business, and to which we are exposed in the course of providing the Services; or
  - (ii) we use to provide the Services;
- (d) any information designated as confidential by either of us; and
- (e) any Work we provide to you,

but excludes any information that:

- (a) is or becomes publicly available, except by a breach of this Agreement;
- (b) is disclosed to either of us by a third party provided that the recipient reasonably believes the third party is legally entitled to disclose such information;
- (c) was known to either of us before we received it from the other or is developed by either of us independently;
- (d) is disclosed with the other's Consent; or
- (e) is required to be disclosed as contemplated by subclause 6.5.

**Consent** means prior written consent which may be granted at the consenting party's discretion and which may be subject to conditions.

**Consequential Loss** means any loss or damage which is indirect, consequential, special, punitive, exemplary or incidental, including any loss of profit, revenue, anticipated savings or business opportunity, loss or corruption of data or systems, or damage to goodwill however caused or arising as a result of the Services or this Agreement.

**Deloitte** means the Deloitte Australia entity or entities entering into the Agreement as identified in the Letter.

**Deloitte Australia** means the Australian partnership of Deloitte Touche Tohmatsu, each of the entities under its control and any of their respective predecessors, successors or assignees.

**DTTL** means Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee.

**Disclosure Law** means Rule 3501(c)(i) of PCAOB Release 2005-014, or US Internal Revenue Code sections 6011 and 6111 and related Internal Revenue Service guidance, or any equivalent legislation, statute or subordinate legislation or guidance in any relevant jurisdiction relating to the disclosure of Tax Advice which applies to you or any Tax Advice we may give you.

**Fees** means the fees for the Services as stated in, or calculated in accordance with, this Agreement.

**GST** has the meaning given to it under *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

**Information** means any information, documents, materials, facts, instructions or Confidential Information provided to us by you or your Representatives or anyone else at your request.

**Insolvency Event** means and includes:

- (a) the making of an arrangement, compromise or composition with, or assignment for the benefit or, one or more creditors of a party;
- (b) the appointment of administrators, liquidators, receivers, a bankruptcy trustee or analogous person to, or over, all or part of a party's business, assets or securities;
- (c) an application being made, or a resolution being proposed, which seeks to effect such an appointment other than for a solvent reconstruction; and
- (d) the existence of a legislative presumption of insolvency in relation to a party.

**Intellectual Property** means all industrial and intellectual property rights throughout the world and includes rights in respect of copyright, patents, trade marks, designs, trade secrets, know-how and circuit layouts.

**Law** includes the *Corporations Act 2001* (Cth) and the rules of the United States Securities and Exchange Commission.

**Letter** means the engagement letter between us to which the Terms are attached.

**Licensed Entity** means a Deloitte Australia entity that holds a licence or registration.

**Licensed Services** means that part of the Services that are required to be provided by a Licensed Entity.

**Loss** means any losses, liabilities, claims, damages, costs or expenses (including interest where applicable and Consequential Loss), judgments or orders however caused or arising as a result of the Services or this Agreement.

**Member Firm** means a partnership or an entity that is a member of DTTL and each of that partnership's or entity's controlled entities, predecessors, successors, assignees, partners, principals, members, owners, directors, employees and agents.

**Personal Information** has the meaning given to it in the Privacy Act.

**Privacy Act** means the *Privacy Act 1988* (Cth).

**Professional Advisers** means your professional advisers who are advising you in relation to the Services but excludes any investor, agent, intermediary, underwriter, syndicate participant, lender or other financial institution or anyone who may provide you with any credit enhancement or credit rating.

**Professional Standards Legislation** means a Law providing for the limitation of occupational liability by reference to schemes that are formulated and published in accordance with that Law and includes the *Professional Standards Act 1994* (NSW) and any similar legislation in each state and territory in Australia.

**Purpose** has the meaning given to it in the Letter or our Work, or where silent on this, the purpose for which we provide our Work to you.

**Report** has the meaning given to it in the Letter or where the Letter does not set out a specific report, means any final form documents, reports or deliverables we provide to you as a result of the Services or this Agreement including those consisting of advice or opinions.

**Representative** means any officer, employee, consultant, agent, contractor or subcontractor of either of us, who is involved in the activities to which this Agreement relates and in the case of Deloitte, includes a partner.

**Services** means the services described in the Letter.

**Tax Advice** means any advice, whether written or oral, relating to tax, tax structuring or tax treatment provided by us as a result of the Services but excludes any tax due diligence Work which we prepare as a result of the Services.

**Terms** means these standard terms and conditions.

**Unexpected Delay** means any delay in providing the Services that is caused or contributed to by an act or event (including the non-performance of your obligations) that is beyond our control or was not reasonably foreseeable by us at the date of this Agreement.

**us** means Deloitte, or both you and Deloitte, as the context requires.

**we** and **our** means Deloitte and, where applicable as the context requires, the members of Deloitte Australia and any of their Representatives.

**Work** means any advice or materials including any reports, documents, advice, opinions, e-mails, notes or other deliverables, whether in draft or final form, in writing or provided orally, that we prepare either alone or in conjunction with you or provide to you as a result of this Agreement and includes any Reports but excludes our Working Papers or any source code.

**Working Papers** means any files or working papers created by us as our record of the Services, in any form.

**you** and **your** means each Addressee, and where applicable as the context requires, each Addressee's Representative.