Deloitte Risk Advisory Pty Ltd
ACN 611 748 184

477 Collins St
Melbourne VIC 3000
Australia

Tel: +61 (03) 9671 7000
Fax: +61 (03) 9671 7001
www.deloitte.com.au

Eric Yee

Coles Information Security Intranet

L4 M1 800 Toorak Road

Hawthorn East Victoria 3123 Australia

19th September 2023

Dear Eric,

Re: Coles - Pen Testing - Project STEP upgrade

Thank you for providing Deloitte Risk Advisory Pty Ltd ("Deloitte") with the opportunity to assist Coles ("Coles") with penetration 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 under which we will provide the services to you.

1 Background

Coles MDM Stibo is defined as a business-critical operation system. MDM platform's key role is to manage the product data and provide the capability to update product information in real-time.

Coles upgraded the Stibo (Stibo Systems Enterprise Platform (STEP)) application from version 10.0 to version 11.1 since the current version of STEP was out of support. To ensure continued support from the Vendor STIBO and for the MDM and PLM programs, an STEP application upgrade was required.

We understand that Coles requires a penetration test to be performed on the STEP application in the TEST1 and PERF environments. The objective of this security assessment is to identify security weaknesses within Coles's STEP application and provide an opportunity to achieve security in depth.

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

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
- Infrastructure Penetration Test

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

Deloitte.

2.1 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 are 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:

2.1.1 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 common 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, 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 several automated tools that are designed to detect vulnerabilities in web applications such as Burp Suite and Nikto.

Application in Scope	URL	Comments

Stibo Systems Enterprise Platform (STEP)	https://teststepatlas.coles.com.au/
	https://mdm-perf.azr.cmltd.net.au/
		• Security testing will be conducted on the non-prod environment
		  • TEST1 env - Internet facing
		  • PERF env - internal facing
		• Two user roles in-scope
		  • Administrators
		  • Business Team
		  • Only web UI URL's are in scope of this application penetration testing

	• Resources and workbench are out of scope (as these are in use by Developers).

2.1.2 Infrastructure Penetration Test

With an infrastructure penetration test, we simulate an attack by a malicious person on the network that can be accessed from Coles's internal network. As part of the testing STEP application's underlying infrastructure, we will try to identify vulnerabilities in security measures on the level of network and operating system of selected systems.

Our methodology incorporates the suggested testing techniques from standard methodologies, such as the OSSTMM (Open Source Security Testing Methodology Manual), specifically Data Networks Security Testing, and the testing techniques within the MITRE ATT&CK framework, which is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations (https://attack.mitre.org/).

Environment	System	Description
TEST	Database servers: - ltmdmdb01 Application Servers: - ltmdmapp01, ltmdmapp02 Database name: - ORTSTEP DB version: - Oracle Database 19.11.0.0.0 Application server OS: - RHEL8.8 Database Server OS: - RHEL 8.8	• STEP version 11.1 • External/Internet facing non-prod environment
PERF	Database servers: - lvmdmdb01 - lvmdmdb02 Application Servers: - lvmdmapp01 - lvmdmapp02 - lvmdmapp03 - lvmdmapp04 Database name: - ORVSTEP DB version: - Oracle Database 19.11.0.0.0 Application server OS: - RHEL8.8 Database Server OS: - RHEL 8.8	• STEP v11.1 • Internal network facing only. Not accessible from the Internet

Deloitte.

2.2 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 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.
- 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.
- Assess associated or supporting web services that also reside on the Coles server(s).
- Deliver formal training or develop training materials as part of the inclusive consulting hours.
- Implement any recommendations contained in our report.

2.3 Requirements for Testing

To complete the specific tasks most effectively, the following information is required before 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 for Coles

General Requirements	• Provide project manager and technical contact details (email and phone number).
	• For any assets hosted by a third party (i.e., Hosting/Cloud provider), Coles to raise the necessary third-party penetration testing and obtain approvals.
	• External Testing will be performed from Deloitte Melbourne Lab IP. Whitelist Deloitte's Melbourne Lab IP
	  ○ 123.103.205.58
	  ○ 3.24.249.150

Web Application Penetration Test	• Provide two user accounts for each role in scope.

	• Ensure the environment is provisioned with test data before testing commences. • Specify any maintenance windows that might apply to the environment.

3 Deliverables & Outcomes

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

3.1 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 major 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 Coles 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 explain 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.

3.2 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

3.3 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 Coles and Deloitte.

3.4 Additional Services

During the term of this engagement, Coles 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 Coles 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 Coles.

Deloitte.

4 Our Team

Ashish Mahajan is the partner who is primarily responsible for the Services. Avneet Kaur 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, wireless, and maintain a variety of the most valuable industry-recognised certifications from the Council of Registered Ethical Security Testers (CREST), Offensive Security, and SANS.

5 Fees

The fixed fee payable for the Services is **$17,000** (excluding GST, Expenses, *and retesting*), and **$22,100** *including retesting* (excluding GST, Expenses,). The estimated costs and duration for each service are described in the table below:

Service	Estimated duration (days)*	Total Onshore (excl. GST)
Web Application Penetration Test (time-boxed)	10 days (timeboxed)	$17,000
Infrastructure Penetration Test (web application's underlying infrastructure)		
Total (excl. GST & re-test)	**10 days**	**$17,000**
Optional with Retest		
Web Application Penetration Test (time-boxed)	13 days	**$22,100**

5.1 Billing Schedule

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

6 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.

6.1 Assumptions

We will provide the Services on the following assumptions:

1. Our Services
    a) Will be based purely on advisory and consulting in nature
    b) Cannot be relied upon to disclose irregularities, including fraud, other illegal acts, or errors that may exist; however, we will inform you of any such matters as come to our attention in the performance of our Services
    c) Will be subject to the limitations inherent in any test of the vulnerability of networks and web-based applications set out below

Deloitte.

2. Our testing is scheduled to be performed in accordance with the below timetable. If your systems are unavailable for testing during a scheduled testing period, testing for that period will not be performed. If you are aware of system downtime during a scheduled testing period (for example due to systems maintenance) you should notify us in advance to make alternative arrangements.

6.2 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) Penetration 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 of 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 penetration 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.

   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.

6.3 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.

Deloitte.

6.4 Your Responsibilities

1. In addition to the responsibilities set out in section 11 of the attached Terms and Conditions, you acknowledge that Coles is, and will continue to be, solely responsible for:
    a) Among other things (a) making all management judgements and decisions, and assuming all management responsibilities, (b) designating an individual, preferably within senior management, to be responsible for your decisions and to oversee the Services, (c) providing oversight of the Services and evaluating the adequacy and results of the Services, and (d) accepting responsibility for the actions, if any, to be taken arising from the results of the Services.
    b) Establishing and maintaining an effective system of internal control over its operations and financial reporting, including, without limitation, systems designed to achieve its control objectives and its compliance with applicable laws and regulations, including, without limitation, monitoring of ongoing activities
    c) Provision of information and data
    d) Informing Deloitte in a timely manner of any need to change the testing schedule
    e) Obtaining authorisation from and notifying all third parties that may be directly affected by this engagement of Deloitte's activities and the timings of such activities.
    f) Taking the necessary precautionary steps to ensure that the penetration testing will not, or will not be likely to, interfere with the functioning or availability of your systems prior to the testing commencing. Such steps should include but may not be limited to:
        a. Preparing backups of all data, configurations, programs, networks and systems which could be exposed to the penetration testing, to enable your staff to restore your systems to the state in which they were prior to the penetration testing
        b. Updating and patching systems in accordance with current manufacturer and vendor recommendations
        c. Having your key support staff available during the penetration testing
2. In connection with the Services, Deloitte shall be entitled to rely on all decisions and approvals of Coles.
3. You warrant that the IP addresses and URLs provided by Coles to Deloitte for testing are owned and used exclusively by you.
4. You acknowledge that:
    a) Our ability to perform the Services and to meet any reporting deadlines is dependent on you meeting your responsibilities, as well as you providing us with instructions and making timely decisions

7 Term

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

- **Test Commencement**: Monday, 25 September 2023
- **Estimated Test Completion**: Friday, 6 October 2023

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.

8 Special Conditions

The Terms are amended as follows:

Deloitte.

a) Clause 8.2 is amended by inserting the words "Upon obtaining your written Consent," at the beginning of the sentence.

b) Clause 10.6 is deleted.

c) Clause 10.7 is amended by replacing the words "14 days" with the words "30 days".

d) Clause 10.9 is deleted.

e) Clause 11.1 is amended by replacing the word "appropriate" and inserting the words "approved by you".

f) Clause 13.3 is amended by replacing the word "we" with "neither you or us" before the words "will be liable for any Consequential Loss".

g) Clause 16.1(a) is amended by replacing the word "30" with "60".

h) The following new clause 29 is inserted:

"29.1 Your Responsibilities

In addition to any responsibilities you may have that are set out in the Agreement, you are responsible for:

(a) informing us in a timely manner of any need to change the testing schedule;

(b) obtaining authorisation from and notifying all third parties that may be directly affected by this engagement of our activities and the timing of such activities, as well as obtaining a signed letter in the form agreed to by both parties. We will not be able to proceed with the Services until it has these authorisations;

(c) taking the necessary precautionary steps to reduce the likelihood that the vulnerability testing will, or will be likely to, interfere with the functioning or availability of your 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 or per your policies and procedures, and

(iii) having your key support staff available during the testing.

taking whatever steps are necessary to protect your data programs and systems throughout the testing.

29.2 Services outside of Australia

(a) We may use other member firms outside of Deloitte Touche Tohmatsu Limited, outside of Australia, to help us provide the Services to you.

(b) We remain responsible for any work undertaken in the delivery of the services and none of the member firms, apart from us, will be responsible to you.

29.3 Liability

(a) You acknowledge that the Services within the scope of the Agreement may cause disruption to your network, systems, and processes. You 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 the Agreement.

(b) You agree to defend and indemnitfy us from and against any reasonable third party claims, incurred or suffered by or made or initiated against them or any third party arising out of or in connection with the Services."

9 Acceptance

The scope of our engagement is limited to the tasks set out above. If the scope of the Services does 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 +61 428 280 129 or Avneet Kaur at +61 455 055 622 if you would like to discuss this letter and the terms of engagement with us.
We look forward to working with you.

Yours sincerely

Ashish Mahajan

Partner

Risk Advisory

Incl. Standard Terms and Conditions

Deloitte.

Sign off by recipient:

Coles agrees to the terms of the engagement. Signed for and on behalf of Coles by its duly authorised representative:

Signature	**Date**
Name	**Title**