Inquiry into the Treasury's Budget related Information Security Systems

27 February 2020

Table of Contents

EXECUTIVE SUMMARY

BACKGROUND

1. Two days before Budget Day in May 2019 excerpts from embargoed Budget Sensitive documents accessed from the Treasury's website were publicly released. As a core function of the Treasury, it is fundamental that the integrity of the Budget process is preserved. As a consequence of the unauthorised disclosure, the then Secretary to the Treasury asked the State Services Commissioner to conduct an Inquiry to address concerns raised by the incident, and the security of Treasury's Budget process. The focus of the Inquiry is on what happened, why it happened, the lessons learned, and the actions Treasury needs to take to ensure a similar incident does not occur again.

2. A previous Inquiry in relation to this matter commenced on 11 June 2019 and was terminated on 13 November 2019 due to an undeclared conflict of interest within the Inquiry team. It should be noted that to ensure the integrity of the second Inquiry, the Inquiry has not accessed any of the previous Inquiry's documentation and has gathered information independently.

3. The Inquirer wishes to acknowledge the professionalism and manner with which the Treasury and its staff have engaged with the Inquiry. It is regrettable for all involved that as a consequence of the matter outlined above this Inquiry has not been able to be concluded before now.

4. The passage of time since the incident has allowed the Treasury to progress a number of initiatives intended to address a number of the contributing factors to the incident some of which the Inquiry has referenced later in the report.

THE CIRCUMSTANCES AND CAUSES OF THE INCIDENT

The Genesis of the Incident

5. In the Inquiry's view the genesis of the incident goes back a number of years starting in 2014 and has a number of contributing factors and events.

6. In June 2014 the Treasury owned and operated Central Agencies Shared Services (CASS) function initiated a procurement process for a new web hosting platform for the CASS group of agencies to replace the existing, and near end-of-life Plone platform. The scope of the Request for Proposal (RFP) was both the replacement of the platform and subsequent development of 5/6 agency websites. A key requirement of the new system was that it have increased content management and search functionality.

7. The initial RFP Tender process was unsuccessful with none of the tender pricing being acceptable to CASS.

8. A second RFP was issued in November of that year with a slightly modified scope. This resulted in a preferred vendor being identified and negotiations entered into to supply the

Drupal web hosting platform. During this process the scope was further reduced including the removal of the Budget Day Scenario (BDS) from the core scope of works negotiated with the vendor and was "parked" by CASS for later consideration.

9. The Treasury's Budget Day Scenario is a collection of business processes used to publish the final Budget documents and other Budget content (in both printed and digital formats) and to set-up the physical arrangements for publishing and distributing the Budget on Budget Day each year. The digital delivery includes publishing the Budget publications on Budget Day to the Treasury website (www.treasury.govt.nz), to a stand-alone Budget website (www.Budget.govt.nz) and delivery of an electronic version for the media delivered via a physical lock-up on Budget Day. In addition the Treasury produces the printed version of the Budget documents. Preparing and delivering the Budget is a critical requirement of Treasury and is a core function.

10. A Statement of Work was issued in May 2015 to undertake further workshops to clarify the scope of the project. This concluded with the production of a 12-month Implementation Roadmap for the 2015-16 period and during this time a number of websites for other agencies were developed on the Drupal Platform.

11. The Treasury website was deemed to be the most complex site of all the in-scope agencies due to the volume of site content, so this was left until 2017 for commencement. The Treasury Website Project was scheduled to commence in January 2017 but did not get underway until mid-2017 and operated under a business requirement to be live by the end of March 2018. In order to deliver the project within cost and timeframe parameters, the Treasury Website Steering Group excluded the BDS from the project scope in mid 2017 and revised the scope of the project to a migration project. The project subsequently became known as the Treasury Website Migration Project (TWMP).

12. Excluding the BDS scope from the Treasury website project meant the Treasury Website Project team (subsequently renamed the Treasury Website Migration Project team) was not required to consider how the Treasury's Web and Publishing function could deliver against its obligations to publish the Budget on Budget Day on the new website. Since there were existing challenges in engaging the wider organisation in the website project, it is unclear what information was provided to other Treasury teams regarding the now "orphaned" BDS business requirements.

How the Information was available to be accessed

13. In the weeks leading up to the launch of the new Treasury Website in 2018, it became apparent to the Treasury Web and Publishing team that the way the Treasury had previously published Budget information and content would not work on the new website and that the Budget Day Scenario (BDS) scope of works was required to enable the Treasury to securely upload and publish Budget Information on Budget Day 2018.

14. In previous years the practice had been to use the two weeks prior to the Budget Day to load material into the website content management system to a "draft state" mostly using a bulk upload tool. On Budget Day the Treasury website would be taken off-line so that material could be moved into a "published" state. This approach could not be used in 2018 on the new website for two reasons, firstly because of the lack of bulk import functionality and secondly, the concern that the increased volume and complexity of content would

require more time to index (to enable user searches) using the new platform functionality than the time available on Budget Day.

15. In mid-March 2018 a series of workshops considered options for delivering the BDS for Budget 2018. The preferred solution developed was to create a "vaulted clone" - a complete off-line replica of the new Treasury website. In doing so the project would create a secure duplicate site where Budget information could be uploaded and published securely on the Treasury website over a number of days prior to Budget Day 2018 and then the clone site could be swapped with the "live" Treasury website at 2pm on Budget Day 2018. CASS IT had previously designed and deployed a vaulted clone approach in 2017 to manage Budget information upload onto one of the other Budget deliverables - the www.Budget.govt.nz. The Inquiry was told the design did not consider a shared index.

16. When the 2017 clone design (as applied to www.Budget.govt.nz) was deployed to the Treasury website in 2018 and the clone website subsequently created approximately 2 weeks before Budget Day 2018, it was linked to a shared index function used for the live website, thus breaking the "vault". The Treasury has not been able to provide any documentary evidence to indicate whether the 2017 Budget.govt.nz and 2018 Treasury.govt.nz clone design and deployment processes were identical.

17. The use of a shared index for both the cloned and live Treasury websites meant that when a search term was entered by a user, the index returned not only document headings and snippets (micro descriptions) from the "live" Treasury website but also any relevant document headings and snippets from the clone website if the documents held in the clone site had the setting of "published". If the user then clicked the headings information, a "404" error message from the clone website would be returned to the user indicating that the page was "not found ".

18. From interviews with relevant Treasury staff it is apparent that the ability to view Budget Sensitive 2018 document headlines and snippet information accompanied by an Error 404 script in response to specifically worded searches was known by the individuals involved in determining to deploy the clone to address the BDS. While it was contemplated not sharing the index, the common belief amongst CASS technical staff based on testing conducted was that it would not be practical to re-index the clone site on Budget Day and meet business requirements for publication of Budget information on Budget Day. This assumption was subsequently proven to be false and was not tested with the platform vendor.

19. The Treasury has not been able to provide any documentary evidence that the 2018 clone was subject to any robust internal review process prior to deployment. In addition the 2018 design was not referred for review to the Information Technology Security Manager despite there being a known issue regarding visibility of Budget document headline and snippet information through the Treasury's website search function. This was inconsistent with commonly accepted practice and with the CASS Certification and Accreditation Framework in place at the time.

20. This planned solution was applied to the 2018 Budget publication process and snippets and document headlines would have been visible had a user searched for Budget 2018 information. There is no information to suggest Budget Sensitive information was accessed prior to Budget Day 2018 although no monitoring of search activity was undertaken.

21. In 2019, based on the apparent success of the 2018 Budget solution, the same clone solution was deployed, with the same potential for document headline and snippets to be displayed to users for Budget 2019 content.

22. Search activity log analysis on the Treasury Website shows that between 6.48pm on 25th May and 12.49pm on 28th May 2019 three IP addresses were used to conduct 1923 searches using specific search terms to access headline and snippet information relating to Budget 2019 information from the cloned website. It is apparent that information gathered through this activity was the basis for the documents publicly released ahead of Budget Day 2019.

23. In considering the issues that contributed to the incident, it appears there were a number of areas where the Treasury either didn't follow either its own policies or best practice guidelines. The Inquiry considers there were a number of failures to follow commonly accepted public sector practices that contributed to the incident.

Risk Management

24. The limited organisational application and tailoring of the Treasury's standard risk management framework resulted in the creation of risk registers that were high-level, static and not utilised as active risk management tools in relation to the Treasury Website or Budget projects and core business processes reviewed by the Inquiry.

25. The limited scope of the Budget Oversight Group (BOG) to the preparation of Budget Estimates meant that the Risk Register for this group did not include risks associated with Budget documentation production as this was considered outside the scope of this group.

THE FINDINGS OF THE INQUIRY

26. Based on the information outlined above, the Inquiry finds the following:

27. Despite it being a core function of the Treasury to produce annual Budget documents on its website, the Treasury repeatedly excluded consideration of the Budget Day Scenario, initially from the Drupal Hosting Platform implementation, the Treasury Website Project and subsequently the Treasury Website Migration Project. This exclusion from scope contributed to the Treasury needing to implement a rushed, sub-optimal solution for production of the 2018 Budget which was then applied to Budget 2019.

28. The decision to share an Index between the live Treasury website and the off-line clone did not fully meet the Government Digital Service Design Guidelines for managing information prior to release in a digital environment. Those guidelines require that information classified up to and including Sensitive content, must be held in "draft" status until ready for publishing. While the intent to use a "vaulted" clone was arguably more secure than was required under the Guidelines for Sensitive information, the decision to "publish" the information in the clone and then allow access to headline and snippet information via the shared index, did not fully meet the Design Guidelines.

29. The failure to subject the proposed Budget Day Scenario solution to review, or achieve any formal sign-off of the same, was inconsistent with the Treasury's own information technology security review policies, project management and information security

management processes and with accepted good practice. Furthermore there was no post implementation review of the same to consider how improvements could be made to future Budget production processes.

30. The Treasury did not have effective governance or senior oversight processes or systems in place to oversee the Budget process from end-to-end resulting in known risks such as the proposed visibility of document headlines and snippets and the descoping of the BDS not receiving appropriate consideration. This is consistent with the failure by senior leadership to pay attention to core operational performance as reported to the Inquiry.

31. Poor application of the Treasury's standard risk management tools contributed to the decisions firstly to exclude the BDS from scope and subsequently that visibility of document title and snippet information of upcoming Budget documents was acceptable**.**

32. The devolved nature of management decision-making licensed the CASS teams to make decisions about the appropriateness of the BDS solution without either seeking and/or being able to gain more senior level approvals of the same.

33. The Inquiry considers the senior leadership did not actively consider or promote a view of the Treasury's appropriate obligations in relation to the production of Budget information. The organisation has faced ever increasing demands for greater volume and more complex Budget products. This resulted in:
    a. Managers and teams feeling they had no option but to deliver whatever was requested of them, irrespective of the impact on resourcing and potential organisational risk; and
    b. Critical decisions being made for expediency's sake, in the absence of consideration of the wider organisation and security risk.

34. The Inquiry considers some of the above findings may be indicative of wider issues within the Treasury and invites the current Secretary of the Treasury to consider these matters further.

35. The Inquiry has heard from interviewees that the Treasury has progressed a number of initiatives post the incident intended to address some of the issues raised in the Inquiry. The nature of those initiatives are outlined more fully in the body of the report.

BACKGROUND

36. Two days before Budget Day in May 2019 documents containing embargoed Budget Sensitive information that had been accessed from the Treasury's website were publicly released.

37. Access to this information appears to have been possible because as part of its preparation of Budget Day, the Treasury developed a clone of its website. Budget sensitive information was added to the clone website as and when each Budget document was finalised. On Budget Day, the Treasury intended to swap the clone website to the live website so that the Budget information was available online. The clone website was not intended to be publicly accessible.

38. As a core function of the Treasury, it is fundamental that the integrity of the Budget process and information are preserved. Given the high public importance of the Budget process it was considered necessary that an Inquiry be conducted (under The Inquiries Act 2013) to address concerns raised by the incident, and the security of Treasury's Budget process. The focus of the Inquiry is on what happened, why it happened, the lessons learned, and the actions Treasury needs to take to ensure a similar incident does not occur again.

39. The initial Inquiry in relation to this matter commenced on 11 June 2019 and was terminated on 13 November 2019, due to an undeclared conflict of interest within the Inquiry team. It should be noted that to ensure the integrity of the Inquiry, the Inquiry has not accessed any of the previous Inquiry's documentation and has gathered information independently.

Scope of the Inquiry

40. The Inquiry was tasked with investigating and making findings on:

    a. The circumstances surrounding the incident, including security measures taken in response;
    b. The causes of the incident, including whether Treasury adhered to its own internal policies relevant to the security of Budget sensitive information and to applicable government-wide policies and good practice;
    c. The appropriateness and effectiveness of the information security systems the Treasury had in place in relation to the final six-week production phase of the Budget;
    d. Any linkages or implications for the Treasury's wider information security systems; and
    e. Any other relevant matters necessary to provide a complete report on the above.

41. Excluded from the Scope of the Inquiry is investigation into the actions taken by the Secretary of the Treasury in responding to the incident as this has already been the subject of investigation by Mr John Ombler, Deputy State Services Commissioner and reported on 25th June 2019.

42. The full Terms of Reference for the Inquiry are contained in Appendix 1.

Inquiry Approach

43. This Inquiry commenced on 14th November 2019 and was concluded on 27th February 2020.

44. The Inquiry has sought and considered information from a range of sources and applied a "trust but verify" principle to the consideration of that information.

45. Interviews of relevant individuals/parties were conducted between 11 December 2019 and 23 January 2020.

46. Given the length of time since the incident occurrence (28th May 2019) the Inquiry has been mindful of the need to triangulate interview information with pre-existing documentary evidence wherever possible. During the course of the Inquiry a significant amount of documentary evidence provided by the Treasury and other parties has been obtained, reviewed and considered.

47. Consistent with the Inquiries Act 2013, the Inquiry has at all times complied with the principles of Natural Justice. Accordingly, any individual against whom an adverse finding has been made has had the opportunity to review the relevant parts of this report and provide evidence to rebut the finding. The Inquiry has considered any and all such evidence in finalising its report.

48. A timeline of events leading up to the incident is included in Appendix 2.

THE CIRCUMSTANCES AND CAUSES OF THE INCIDENT

THE TREASURY'S WEBSITE

The Genesis of the Incident

49. The Inquiry has reviewed information that indicates the root of the incident goes back to June 2014 when the Treasury owned and operated Central Agencies Shared Services (CASS) function, initiated a procurement process for a new web hosting platform for the CASS group of agencies to replace the existing, and near end-of-life Plone platform. Approximately 5/6 websites from a number of agencies were proposed to be hosted on the replacement platform. A key requirement of the new system was the inclusion of increased content management and search functionalities.

50. The initial RFP process was unsuccessful with none of the tenders complying with CASS's budget expectations for the project.

51. A second RFP was issued in November of that year with a slightly modified scope. This resulted in a preferred vendor being identified and negotiations entered into. During this process the scope was further reduced including the removal of the Budget Day Scenario (BDS) from the core scope. Although not technically descoped at this stage, the BDS was not included in the scope of works negotiated with the vendor and was "parked" by CASS for later consideration.

52. A Statement of Work was issued in May 2015 for the vendor to undertake further workshops to clarify the scope of the core project. This concluded with the production of a 12-month Implementation Roadmap for the 2015-16 period new hosting platform Drupal implementation and establishment of a number of websites for other agencies.

53. In 2016 a Statement of Work entered into between CASS and the Vendor to initiate a discovery process in preparation for the Treasury Website project was cancelled thus delaying the commencement of Treasury Website Project (TWP).

54. The Treasury website was deemed to be the most complex site as a consequence of the high volume of content on the existing site and the requirement to prepare and publish Budget Sensitive information. As a consequence it was deferred until 2017 for development.

55. The TWP was scheduled to commence in January 2017 but was delayed and did not commence until mid-year. The TWP operated under a business requirement for the new website to be live by the end of March 2018 to ensure the Budget process was not compromised in any way.

56. The volume of information on the old Treasury website and challenges gaining engagement from the wider organisation resulted in the TWP re-scoping the project in order to deliver the project within cost and timeframe parameters. The Treasury Website Steering Group considered and approved a Business Case in July 2017 prepared by the Treasury Website Project Manager that:

    a. Re-scoped the project from a website redesign and build to a content migration project onto the new platform; and

b. Excluded the BDS from the project scope.

57. The TWP subsequently became known as the Treasury Website Migration Project (TWMP) and the focus became on migrating the large volume of content from the original Plone platform onto the new Drupal platform website by March 2018. Additionally, in accordance with the revised project scope no further consideration was given by the TWMP team to how Treasury's publishing function could deliver against its obligations to publish the Budget on Budget Day 2018 on the new website.

58. The new Treasury website went live in March 2018.

The Budget Day Scenario (BDS)

59. The BDS was the term used to refer to a series of business processes designed to prepare and deliver the Government's Budget information at set times on Budget Day. There were four key deliverables:

    a. The printed version of the Budget documents;
    b. Digital version published to the Treasury website (www.treasury.govt.nz); a site mainly used by practitioners, banks and analysts
    c. Digital version published to www.budget.govt.nz - a stand-alone website dedicated to Government's communication of the Budget; high traffic volumes are achieved around the time of the Budget announcement;
    d. Digital version and preparation for the physical press gallery lock-up; the embargoed preview to enable the press gallery to prepare for Budget Day announcements.

60. The preparation work for Budget publication had typically been a stand-alone activity managed by the Web and Publishing team. Delivery timelines are rigid, work volumes have increased year on year and the Budget Estimate content and other Budget related documents and content was often changed at short notice late in the delivery process. The traditional BDS was based on a significant preparation phase for all four delivery methods but delivery of the Treasury website is the most pertinent to the Inquiry.

61. Delivering the Budget content to the Treasury website traditionally required intense activity whereby the Treasury website was taken off-line for four hours on the morning of Budget Day to allow for the transfer of published information and bulk upload of the same to the site . This step was risky as there was little to no contingency and the process was described as highly stressful. The Treasury website would be on-line again at 2pm to coincide with the Budget Day announcement.

62. The change of hosting platform in 2018, and the timing of the TWMP go-live in 2018 required a new approach for the BDS for Budget 2018 to be developed. This change is a material factor in the circumstances that led to the incident of Budget 2019. The BDS solution for 2019 was described to the Inquiry as the same as BDS in 2018.

The Lead up to Budget 2018

63. In early 2018 in the weeks leading up to the launch of the new Treasury website, it became apparent to the Treasury Web and Publishing (W&P) team that the TWMP scope did not include the requirements for the BDS and that the way the Treasury had previously published Budget information would not work on the new website.

64. This issue was escalated to the Chief Information Officer (CIO) who directed the establishment of a working group tasked with finding and implementing a solution for publication of the 2018 Budget with specific consideration to be given to the cloning functionality of the Drupal platform as a potential solution. The CASS IT team had previously designed and deployed a clone solution to publishing Budget information on the www.Budget.govt.nz website in 2017.

65. The TWMP Project Manager was asked to assist the CASS team to identify and implement a solution. The scope of work, reporting lines and accountabilities of the Project Manager for this piece of work were not documented or formalised.

66. A short list of desired functions for the BDS solution was created by the W&P team and used as input to two workshops convened in mid-March 2018 to urgently develop a solution for BDS for Budget 2018. The workshops were attended by the TWMP Project Manager, representatives from the CASS IT team, the W&P team and the external platform vendor. One workshop focussed on the "vaulted clone" solution and the second concentrated on a bulk uploader tool that was subsequently delivered and enabled the W&P team to load the Budget 2018 content into the clone site.

67. As stated above the first workshop discussed the "vaulted clone" solution or in lay person's terms, a completely isolated replica of the new Treasury website. The intention was the project would create a secure, duplicate site where the W&P team could develop and publish Budget Sensitive content securely prior to Budget Day. The clone website and the "live" Treasury website could then be swapped at 2pm on Budget Day 2018 allowing all Budget information to be available to the public immediately post the Budget Day announcement. The approach to the clone was described as an infrastructure solution that could be set up by CASS IT without any engagement or dependency on third parties.

68. The Inquiry was told that a design for creating the clone website was first developed by the CASS IT Chief Architect in 2017 for use on the www.Budget.govt.nz site. At the time of the deployment of the clone in 2018 to the Treasury website, the Treasury Architecture Review Board was suspended from operation and no alternative review authority was operative. At some point the clone design was modified to include the use of a shared index. The Inquiry has not been able to ascertain how or where this decision was made but is clear that it was an intended change to the clone design.

69. The use of the shared index meant that when a search term was entered, the index contained not only content from the "live" Treasury website but also content from the "clone" website where the content setting met the "published" (i.e. completed) criteria on that site. The person searching was able to access document headline and snippet information (micro descriptors) for those documents. However, if the person searching then selected the document headline and attempted to click through to the full document, they would receive a "404 error" message from the clone website and the full document was

blocked from the viewer. A "404 error" message is standard web services messaging denoting that a web page or document can't be found.

70. The Inquiry has not received any documentary evidence that the 2018 design was either formally documented or subject to any review board process. Nor was the design referred to the Information Technology Security Manager for review.

71. As the working group was not part of the TWMP Project, it was not subject to Steering Group or any other overview. Consequently, the proposed design was adopted by the working group for implementation without any external scrutiny or assurance.

72. When the cloned Treasury website was subsequently created, approximately 2 weeks before Budget Day 2018, the clone was configured to use the shared index with the live website, thus breaking the "vault" as per the stipulated configuration. W&P team members responsible for producing Budget documents worked to develop those documents on the cloned website, and once finalised documents were set to "published" state on the cloned website. Because the cloned website and live website used a shared index, document headline and snippet information on the clone website where documents were set to "published" were able to be accessed by search users.

73. From interviews with relevant Treasury staff it is apparent that the ability to view Budget Sensitive document headline and snippet information in response to specifically worded search activity followed by an Error 404 script was known by individuals involved in determining to deploy the clone as the BDS solution for the Treasury website in 2018. There is no evidence to indicate the risk associated with visibility of document headlines and snippet information was formally escalated outside of this group. While it was contemplated not linking the index and cloning the index as well as the site, the testing method employed by CASS staff indicated it would take approximately three days to re-index the clone site prior to Budget Day which did not meet business requirements and consequently this option was disregarded. On the day of the incident the platform vendor was able to deploy an alternative method that re-indexed the clone site within one hour. The CASS IT team had not previously sought any advice from the vendor regarding methodology for re-index.

74. The clone solution to the BDS was applied to the 2018 Budget publication process. There is no information to suggest Budget Sensitive information was accessed prior to Budget Day 2018 although no monitoring of website search activity was undertaken so it is not possible for the Inquiry to confirm this was the case.

75. Budget documentation was successfully published on Budget Day 2018 and the Budget production was considered a success by the Treasury teams and stakeholders.

76. Documentation of the deployment of the 2018 clone solution was not completed (e.g. no technical run sheet for creation of the clone was completed) and post-implementation review of procedures were not undertaken.

The Lead up to Budget 2019

77. In the lead up to the 2019 Budget and based on the apparent success of the 2018 BDS solution, the CASS IT and W&P teams at Treasury elected to deploy the same clone solution to prepare and publish Budget documents on the Treasury website in 2019.

78. As no formal technical run sheet was developed in 2018 it is not possible for the Inquiry to determine whether or not the exact same process for creating the clone was followed, however those directly involved in its creation have indicated they believe that to be the case.

79. The clone website was created on 15 May 2019 by the CASS IT team and the W&P team proceeded to create Budget document content on the clone site. Once each Budget product was completed it was set to "published" on the clone site.

80. As in 2018, once set to "published" Budget documents headlines and snippets could be accessed upon specifically worded searches by the shared index and made available to users.

81. Search activity log analysis on the Treasury Website shows that between 6.48pm on 25th May and 12.49pm on 28th May 2019 three separate IP addresses were used to conduct 1923 searches using specific search terms to access headline and snippet information relating to Budget 2019 from the cloned website. It is apparent that information gathered through this activity was the basis for the documents containing Budget Sensitive information released on 28th May 2019.

28th May 2019

82. Upon learning late morning on the 28th May that Budget Sensitive information had been released, a member of the W&P team contacted the vendor at approximately 1pm reporting that the website was not behaving as expected. The vendor reviewed the web platform from their vantage point and confirmed the Drupal platform was operating correctly. They concluded that, if there was an issue, it must be in the CASS infrastructure environment to which the vendor had no access.

83. The vendor re-confirmed that controls to prevent "unpublished" content being accessed remained in place and that the issue was not at the Drupal application layer (i.e. that the Drupal layer was not allowing unpublished information to be accessed by the search function).

84. At this point the CASS IT, W&P team and the vendor discussed the index and search platform configuration (which had not previously been visible to the vendor). This highlighted that the clone had been set up using a shared index and it became apparent that that the embargoed Budget Sensitive content may have been accessed from the Treasury website.

85. From 1.15pm onwards the vendor and CASS IT team worked together to resolve the access issue and confirmed that the shared index was allowing document headline and snippet information to be accessed. Prior to the incident, the vendor had not had any visibility of

the CASS system infrastructure as their involvement had been limited to the Drupal platform and had not been aware of the clone design and use of the shared index.

86. Upon observing the configuration which drove both site searches to the shared index, the vendor recommended changing the configuration to remove the link to the shared index. The CASS IT team raised concerns regarding the time to rebuild the index. The vendor was able to show the IT team a standard command line which took just one hour to re-index the site (not three days as experienced by the CASS team in testing their own method).

87. Using the website search log, the vendor and CASS IT team were able to recreate the search activity and demonstrate how and what information had been accessed through search activity on the Treasury website.

88. By 5pm on the 28th May the live website was restored, and the clone website secured.

89. A timeline of events up to and including the 28th May 2019 is included in Appendix 2.

THE TREASURY'S SECURITY, RISK AND GOVERNANCE SETTINGS RELEVANT TO THE INCIDENT

90. As outlined above, at a technical level the incident occurred because the cloned and live websites were pointing at a shared index, thus breaking the "vault" and creating a known vulnerability whereby Budget Sensitive information was able to be accessed prior to its official release. The failure to subject the clone solution to any governance or risk assessment meant this was not formally assessed as a risk by the organisation.

91. In the view of the Inquirer, this flawed technical solution coupled with a lack of good practice was able to occur as a consequence of failures in the application and appropriateness of Treasury wider security, risk, control and governance settings. In the Inquirer's view, those issues created an environment in which similar incidents are possible until such time as the Treasury improves the application of its systems, processes and governance of similar activities. The adequacy of action taken by the Treasury post the incident was outside the scope of the Inquiry and has not been assessed.

Security Settings

92. The Treasury has a Chief Security Officer and a Chief Information Security Officer as required under the Protective Security Requirements. The CIO also holds the Chief Information Security Officer (CISO) role. At the time of the incident the Treasury Solicitor was the Chief Security Officer (CSO) responsible for Personnel and Physical Security.

Information Technology Security

93. Within the IT function, the CISO delegated much of the information technology security oversight and management to the Information Technology Security Manager.

94. The Information Technology Security Manager was involved in the Certification and Accreditation (C&A) of the Drupal hosting platform in 2016. When the Treasury Website was developed in 2018 industry standard penetration testing was undertaken and the website met security requirements.

95. The Inquiry is of the view that despite being resource constrained the Treasury's Information Technology Security function is well managed and that appropriate systems and frameworks were in place at the time of the incident. Had the clone design been escalated to the Information Technology Security Manager, it is the Inquiry's view that the risk associated with the accessibility of headlines and snippet information would have received greater organisational scrutiny and/or been deemed to be outside of Treasury's risk tolerance resulting in an alternative/modified solution being required.

96. The Inquiry considers the risk was not appropriately considered as a result of the failure to either seek a change advisory review or to escalate the clone design to the Information Technology Security Manager based on the fact that it represented a significant change either to existing processes and/or design and an increased risk profile.

Information Security

97. The Treasury is subject to the NZ Cabinet approved Protective Security Requirements (PSR) outlining the government's expectations for security governance and for personnel, information and physical security. An annual self-assessment measures compliance against 20 mandatory requirements and capability uplift against agency determined targets.

98. In 2019 the Treasury's PSR Self-Assessment assessed the agency as "meeting" the 20 mandatory requirements and "managed" or "enhanced" against the capability uplift measures. The Self-Assessment was supported by an independent moderator with the exception of a rating for Personnel Security where the moderator reduced the Treasury's self-assessed rating to "Basic +".

99. In the Inquiry's view a number of these ratings are inconsistent with the information made available to the Inquiry. Moderation was carried out as a desktop review which meant that the moderator may have had a limited view of the practical implementation of the PSR. The Inquiry had the opportunity to interview a broad range of people and view a wide range of documents which gave a greater level of visibility of practical implementation of the PSR leading to the Inquiry's view of inconsistencies with the ratings.

100. The Treasury's management of information security relative to the Budget spanned the division of roles between the Budget Oversight Group (BOG) and the CASS IT and W&P teams. A challenge for the Treasury in the preparation of the Budget Estimates is the number of people both internal and external to the agency who appropriately need access to Budget Sensitive information as part of the Budget Estimate preparation process.

101. Within Treasury, the extent to which Budget Sensitive information is routinely accessed is limited to the Budget Project team. As the Budget Estimates near finalisation the number of people involved and with access to Budget Sensitive information is reduced. The Budget Project team operated under the BOG and was responsible for the Budget Estimates Preparation working with Ministers and other agencies.

102. Staff working on the Budget Estimates Preparation and Budget Production teams received information on information security requirements as part of their induction, however at the time of the incident there did not appear to be any training, advice or policies which specifically articulate expectations regarding the handling of Budget Sensitive information or information accessed during the Budget process. The Inquiry considers the Treasury's approach does not fully meet the PSR and is inconsistent with the findings of both the 2019 self-assessment and June 2019 Independently Moderated report.

103. A particular aspect of the circumstances surrounding the incident relate to the Government's Digital Service Design Guidelines (updated in July 2018) for Managing Information Prior to Release in a Digital Environment. The decision to share an Index between the live Treasury website and the off-line clone did not fully meet the Government Digital Service Design Guidelines for managing information prior to release in a digital environment. Those guidelines require that information classified up to and including Sensitive content, must be held in "draft" status until ready for publishing. While the intent to use a "vaulted" clone was arguably more secure than was required under the Guidelines for Sensitive information, the decision to "publish" the information in the clone and then allow access to headline and snippet information via the shared index, did not fully meet the Design Guidelines.

104. Furthermore, due to the workload required to produce the Budget documents in the 6 weeks before the Budget, the Treasury has routinely utilised temporary staff to produce the Budget documents and did so for both the 2018 and 2019 Budgets.

105. The Inquiry considered whether the use of temporary staff of itself contributed to the incident and concluded there is no evidence that the practice of using temporary staff to publish Budget Sensitive information in any way contributed to the incident itself. However the Inquiry did not receive any information that documented the Treasury's active consideration of the risk of this practice; consideration of implications for all-of-government security; or considered the measures taken to mitigate any risks arising. As such the Inquiry considers the Treasury's approach does not fully meet the Government's PSR. Furthermore, it is inconsistent with the Treasury's self-assessment and the moderated report findings.

Risk Management

106. Information reviewed by the Inquiry indicates that the Risk Register operated by the BOG was limited to the risks associated with the preparation and finalisation of the Budget Estimates. Because the production and publication of Budget documents was not included in the BOG's scope there was no consideration of risks associated with production of the same by the BOG.

107. As the production of the Budget documents was viewed as a standard annual activity rather than a project, it did not operate a risk register. Both approaches failed to recognise that the publication of the 2018 Budget (and subsequent 2019 Budget) operated on a new website platform and as such represented a different risk profile to previous years.

108. The separation between the mandate of the BOG and the production of the Budget documents, and the lack of visibility of the end-to-end process contributed to the failure to identify and escalate the increased risk profile resulting from the proposed clone methodology. It also highlights how the separation between teams and the failure to take

an enterprise or end-to-end process approach contributed to increased risk profile for the organisation.

109. The Inquiry considers the Treasury's Risk Management Framework and systems were broadly fit for purpose and comprised of fairly standard risk tools, however the application of the same in relation to the circumstances surrounding the incident was ineffective and inadequate. This contributed to the lack of awareness and consideration of the risks inherent in the Budget process in 2018 and 2019.

Governance and Oversight Framework

Management Structure

110. The Treasury describes itself as operating a devolved management and enterprise leadership model. The Executive Leadership Team (ELT) is accountable for the strategic leadership of the Treasury with a focus on outward facing and crosscutting issues. It delegates to Kaiurungi responsibility for delivering on organisational strategy, enterprise leadership and for ensuring the programme of work across all directorates delivers on the Treasury's objectives and strategy. Kaiurungi is chaired by the Chief Operating Officer (COO) and is a Committee otherwise comprised of Tier 3 Directors.

111. Tier 4 managers are responsible for managing teams within Directorates. The Treasury considers this structure empowers its Tier 3 and 4 staff and authorises them to effectively manage the organisation.

112. In the Inquiry's view, the above structure contributed to the sub-optimal decision making and non-escalation that contributed to the incident. In particular, the Inquiry consider it contributed to:
    a. The inability of the TWP to engage the wider organisation resulting in the subsequent rescoping of the Treasury Website project to a mere "lift and shift" migration project;
    b. The non-escalation of organisational risk represented by the failure to consider securing additional budget for the replacement web hosting platform project and the resultant removal from scope of the BDS from the project;
    c. The lack of escalation pathway to provide visibility of the risk of Budget document headlines and snippet information relating to production of Budgets 2018 and 2019.

113. The Inquiry did not find evidence of effective oversight in relation to the teams involved in the incident and many of the people spoken to in relation to the incident raised concerns regarding the inability of managers to successfully escalate to senior managers matters such as the non-engagement by the wider organisation in the Treasury Website project or the de-scoping of the BDS from the same.

114. The Inquiry considers the organisational structure contributed to the incident particularly in relation to the operation of the Treasury/CASS IT team. As the senior manager of the Treasury and CASS IT function, the CIO was not a member of Kaiurungi at the time of the incident. The CIO reported to Kaiurungi on operational matters via monthly reporting on IT and Information Management however the Inquiry was told that corporate services was not a priority area of focus for Kaiurungi.

Lack of attention to core business operations

115. The Inquiry heard from a number of interviewees of the challenge within the organisation of gaining senior level engagement or commitment on matters associated with organisational functioning or performance, particularly where it related to corporate services. Furthermore the Inquiry observed an apparent organisational divide between "the business" and corporate services. In the Inquiry's view, a disregard for the role of corporate services coupled with a lack of prioritisation of delivering organisational objectives contributed to the incident in a number of ways as evidenced by:
    a. The inability of the Treasury Website Project to gain engagement from "the business" in the design, content and management of the new Treasury Website;
    b. The lack of consideration of the impact on the W&P team of the continual increase in demand for the production of Budget documents in the final 6 weeks of the Budget preparation and subsequent impact on organisational risk profile;
    c. The non-involvement of W&P in the BOG;
    d. The failure to develop end-to-end process or governance oversight of the Budget process;
    e. The failure to undertake effective close-out or other review procedures to inform organisational performance
    f. The non-inclusion of the CIO on Kaiurungi.

116. The vulnerability in this area was further exacerbated by a reported organisational belief that work on core business operations is less valued or important than policy work or other core economic or fiscal functions of the Treasury and therefore not prioritised.

Project Controls and Business Interface

Treasury's PMO

117. At the time of the incident the Treasury had limited project management capability, operating a small Information Technology Project Management Office (PMO) largely tasked with developing and providing technology project management structures as required. There was no Enterprise Project Management Office with broader organisational oversight and interface accountabilities in place.

118. As a consequence, the Treasury had observed a practice of contracting individual IT project managers in the years leading up to the incident and allowed project management disciplines to be largely driven by the experience, practices and frameworks used by those external project managers. This contributed to a lack of standardised project management documentation, systems or framework at the time of the incident.

119. The lack of an "enterprise" perspective contributed to the incident by virtue of the practice of information technology project delivery being allowed to operate in isolation of core Treasury business processes and without necessarily capturing any project related decisions with wider organisational or business impacts.

120. This explains in part how the Treasury Website project was able to seek and achieve Steering Group approval to exclude the BDS from scope less than 9 months before Budget 2018 and this not being picked up by the wider organisation. The Inquiry considers the intersect

between project-based activity and core business processes remains a key area of risk for the Treasury based on this aspect of its operating model.

Governance Groups

121. Interviewees reported struggling to gain regular, consistent engagement with the Steering Group of the Treasury Website Project (subsequently renamed the Treasury Website Migration Project). Documentary evidence supports the assertion that meetings were held infrequently, not well attended and ultimately reduced to the COO and Project Manager in composition.

122. The Inquiry considers that the Treasury Website Project Steering Group (subsequently renamed Treasury Website Migration Project Steering Group) did not provide effective governance oversight of the project and failed to alert the wider organisation to the significant risks associated with the project.

Lack of Post-Implementation/Close-out Review

123. Based on the information reviewed by the Inquiry, had the Treasury undertaken a robust post implementation review of the TWMP and a review of the BDS solution in 2018 it may have highlighted the risk created by the visibility of document headline and snippet information. This may have led the Treasury to consider how it could improve the BDS solution for 2019 and thus averted the incident.

124. The lack of post project review in relation to the TWMP and BDS solution for 2018 is consistent with findings from a number of independent reports commissioned by the Treasury and reviewed by the Inquiry in relation to the Budget Process and other risk matters. Furthermore the Inquiry observes that the Treasury has not implemented recommendations contained in a number of independent reviews commissioned by the Treasury. This is consistent with the Treasury's lack of prioritisation of working on core business operations and in implementing systems and governance to pursue the same.

Increasing Pressure on Treasury Staff working on the Budget

125. Following discussions with relevant Treasury staff, the Inquiry considers the Treasury's senior leadership did not adequately consider the impact on staff of ever increasing production expectations, milestone slippage outside of the Treasury's control or the impact on the risk profile for the Treasury itself of its unquestioning approach.

126. The Inquiry considers the lack of senior leadership consideration of the demands on the organisation contributed to an environment whereby:

    a. managers and teams felt they had no option but to deliver whatever was requested of them, irrespective of the impact on resourcing and potential organisational risk; and
    b. in which critical decisions were made for expediency's sake, in the absence of consideration of the wider organisation and security risk.

127. In recent years, in addition to the printed version, the Treasury's W&P team have been producing increasing levels of Budget information for 3 different digital solutions, in preparation for Budget Day:
    a. www.Budget.govt.nz
    b. www.Treasury.govt.nz
    c. The Media lock-up site

128. The range and complexity of digital tools and products required to be produced by the Treasury for the Budget has placed ever increasing pressure on the Budget Project and W&P teams in the critical weeks leading up to the Budget.

INQUIRY FINDINGS

129. Based on the information outlined above, the Inquiry finds the following:

130. Despite it being a core function of the Treasury to produce annual Budget documents on its website, the Treasury repeatedly excluded consideration of the Budget Day Scenario, initially from the Drupal Hosting Platform implementation, the Treasury Website Project and subsequently the Treasury Website Migration Project. This exclusion from scope contributed to the Treasury needing to implement a rushed, sub-optimal solution for production of the 2018 Budget which was then applied to Budget 2019.

    a. *The decision to exclude the BDS from the Drupal Platform procurement and subsequent Treasury Website Project scope was short-sighted and driven from a desire to contain budget and in the case of the Treasury Website Migration Project, manage delivery timeframes. Its non-inclusion failed to consider the genuine, known and foreseeable business needs of the organisation.*

    b. *The subsequent realisation that Budget 2018 was unable to be delivered using the approach previously applied resulted in a working group being hastily established and required to work under pressure to develop an alternative solution in an extremely short-time frame and without seeking appropriate scrutiny by risk and information security functions within the Treasury.*

131. The 2018 implementation of the clone, which included use of a shared index, allowed visibility of document headline and snippet information of Budget Sensitive information did not fully meet the Government Digital Service Design Guidelines for managing information prior to release in a digital environment.

132. The failure to subject the proposed Budget Day Scenario solution to review or achieve any formal sign-off of was inconsistent with the Treasury's own information technology security review policies, project management and information security management processes and with accepted good practice. Furthermore, there was no post implementation review of the same to consider how improvements could be made to future Budget production processes.

    a. *The 2018 clone implementation and associated risk of disclosure of document heading information and snippets of Budget Sensitive information was not referred to or considered by the Treasury Architecture Review Board, nor was it referred to the Information Technology Security Manager in either 2018 or 2019. The Inquiry's view is that the clone approach was of sufficient order of change and with sufficient organisational risk associated with its design that it represented a change that should have been referred to and reviewed by an appropriate Design Authority Board and by the Information Technology Security Manager.*

    b. *After the 2018 clone deployment by the Treasury there was no substantive technical quality assurance/close out review of the clone deployment. While the BDS solution was never technically established as a project, the failure to review such a substantive change to previously operating processes is at best inconsistent with good practice. It's unclear whether it was inconsistent with Treasury's own practices due to the absence of clear protocols or policy documentation and the uncertain status of the working group. Furthermore, there was no technical run sheet*

documented for the creation of the clone after the 2018 Budget. As such it isn't possible to determine with certainty whether exactly the same process was followed in 2018 and 2019.

c. *The non-performance of a Change Impact Assessment on core business processes of the Treasury Website Project and at the subsequent re-scope to the Treasury Website Migration project meant there was no consideration of the risk to core business processes which ultimately led to the BDS being able to be considered in isolation rather than under formal project management structures and also contributed to the lack of visibility of the impact of the removal from scope of the BDS.*

d. *A lack of formal information technology project management policies and processes allowed the BDS working group to be stood-up without any formal governance or oversight and consequently meant the associated risks didn't feature on relevant risk registers.*

e. *The Treasury's PMO was not effective in enforcing common project management frameworks and disciplines across the organisation. Neither did it have a mandate to take an enterprise wide view of priorities of projects and their impact/interface with the Treasury's wider organisational priorities.*

133. The Treasury did not have effective governance or senior oversight processes or systems in place to oversee the entire Budget process resulting in known risks not receiving appropriate consideration or escalation. This is consistent with the failure by senior leadership to pay attention to core operational performance as reported to the Inquiry.

a. *The lack of senior ownership and oversight of the Treasury Website Migration Project that allowed for the de-scoping of critical business functionality (i.e. the BDS) ultimately contributed to an inadequate solution being developed in the critical 6 week period before the May 2018 Budget and hence creating the risk that was subsequently exploited in the lead up to Budget 2019.*

b. *The use of the clone solution for the BDS was known within the CASS IT team (including the CIO), the TWMP PM, the website platform vendors and the Web and Publishing team members working on the Budget production. The decision to share the index resulting in the visibility of document headline and snippet information was not escalated or considered by the Information Technology Security Manager, CIO, wider Budget Oversight Group (BOG), Kaiurungi, or other committees within Treasury in either 2018 or 2019 as it fell between the considerations of any of the above groups. This is symptomatic of the absence of end-to-end process oversight of the Budget by Treasury which considered the production of Budget documents for publication to be separate from the preparation of Budget Estimates and in doing so failing to have any review body in place to oversee the former.*

c. *The absence of any formal Project and Change Management Governance structure into which the TWMP Steering Committee could report and the non-membership of the CIO on Kaiurungi meant it was challenging to escalate issues to a senior level. This is likely to have contributed to the initial decision to descope the BDS from the Treasury Website project based on a belief that cost parameters were the driving*

consideration in defining budget scope and also to the failure to escalate up the risk of document headlines and snippet visibility.

d. *The limited senior oversight of the Treasury Website Project and the inability of the project team to gain engagement and/or sponsorship from the wider organisation in the project contributed to the change of focus from the design of the website as a new technology business tool to a "lift and shift" of old content onto a new platform. This is symptomatic of the lack of appreciation of the shift in the role of technology in customer delivery by "the business"; lack of focus "on the business" that is widely reported and of the divide between "the business" and corporate services.*

e. *The non-implementation of recommendations from an Internal Audit Review of Treasury's Budget processes conducted in 2016 is consistent with the observed practice of non-implementation of changes recommended by independent reviewers. Had these changes been implemented, the Treasury would have moved to make a number of improvements to its processes that would have provided improved visibility and oversight over the entire Budget process.*

f. *The failure of the Treasury Website Project Steering Committee members to prioritise meetings led to inconsistent and variable attendance contributing to inadequate oversight or input into the Project.*

g. *The Inquiry found that many of the Treasury's policies and procedures were either:*

   i. *Not clearly documented*
   ii. *Not formally adopted by the organisation or subject to review or version control*
   iii. *In various states of draft*
   iv. *Missing*

   Consequently, it was difficult for the Inquiry to ascertain which if any, policies or procedures were operative at the time of the incident.

134. Poor application of the Treasury's standard risk management tools contributed to the decision that visibility of document title and snippet information of upcoming Budget documents was acceptable**.**

a. *Within the CASS IT and W&P team working on the Budget publication it was a known issue that document title and snippet information relating to the forthcoming Budget would be visible to anyone searching for that exact information. This information was not entered onto the Budget Project (or any other) Risk Register neither was the link made to the risk of unintended disclosure of information identified on the Treasury's Master Risk Register, nor was it considered by any more senior management structure.*

b. *It is symptomatic of the Treasury's maturing risk culture that it was considered acceptable that snippet and headline information would be visible and that it wasn't necessary to escalate that decision within the organisation. While some staff have indicated they had a level of discomfort with the visibility of headlines and snippet information there was no formal escalation of the issue outside of the BDS working group.*

135. The devolved nature of management decision-making operating in the Treasury licensed the CASS teams to make decisions about the appropriateness of the BDS without seeking or being able to gain more senior level approvals.

    a. *The devolved, committee-like membership of Kaiurungi, non-inclusion of the CIO and lack of enterprise wide perspective contributed to there being no nominated line management responsibility or business owner for end-to-end delivery of the Budget.*

    b. *The inconsistent practice in the organisation regarding formal documentation particularly of decisions, the devolved nature of management decision-making and lack of enterprise wide perspective is likely to have contributed to the decision by the BDS working group not to seek formal approval or review of the clone design from either the Architecture Review Board, Change Review Board or the Information Technology Security Manager.*

136. The Inquiry considers the lack of senior leadership consideration of the demands on the organisation contributed to an environment whereby managers and teams felt they had no option but to deliver whatever was requested by the government of the day, irrespective of the impact on resourcing and potential organisational risk.

    a. *The failure of senior leaders to address the impact of schedule slippage and increasing Budget production requirements over a number of year has resulted in increased time pressure, increased complexity of production, extreme pressure on Treasury staff and heightened organisational risk in the lead up to the annual Budget.*

137. The Inquiry considers some of the above findings may be indicative of wider issues within the Treasury and we invite the current Secretary to the Treasury to consider these matters.

INITIATIVES UNDERWAY WITHIN TREASURY SINCE THE INCIDENT

138. A number of interviewees referred to initiatives being introduced into the Treasury that should strengthen the Treasury's operating environment. The Inquiry has sought input from senior Treasury Officials who have provided the following schedule of initiatives. The Inquiry acknowledges this progress but has not tested the status of implementation or effectiveness.

139. The initiatives completed and underway include:

Culture and operating model

140. Launching the Strengthening the Treasury programme, led by a newly-appointed Director, coordinating the work to:
    a. Strengthen the core systems and processes to support people to succeed;
    b. Create a culture where the Treasury is as focused and robust in how the organisation runs as in their policy advice;
    c. Maintain the benefits of the current operating model whilst strengthening governance and capability to manage risk.
141. Increasing leadership focus on planning and prioritisation and regular discussions with the Minister on priorities and trade-offs.
142. Undertaking an independent review of information management practices and behaviours.
143. Reviewing existing recommendations from previous internal and external reviews to ensure they are being implemented.

Strengthening and formalising the Budget process ownership, governance and process

144. Appointing an ELT member as the Senior Responsible Officer (SRO) for the Budget project.
145. Establishing a governance structure to oversee Budget 2020 comprising of:
    a. The Budget Governance Group including an external independent member, that meets monthly and is chaired by the SRO providing oversight of both the business and technical aspects of the Budget production and ownership of the Budget risk register;
    b. The Budget Co-ordination Group that meets fortnightly and reports to the Budget Governance Group.
146. Ensuring a member of the Budget Co-ordination Group is also on Kaiurungi which has responsibility for Budget 2020 resourcing.
147. Issuing guidance for handling Budget information for internal and external users.
148. Reviewing the security of Budget Day processes including ensuring that the search does not return embargoed information.
149. Undertaking a "lessons learned" review of the Half Yearly Economic and Fiscal Update/Budget Policy Statement process to inform Budget 2020 processes.
150. Establishing a project manager role for the Budget team covering end to end Budget preparation including corporate and publication processes.

Strengthening IT project management and governance

151. Establishing an IT Governance Committee as a sub-committee of ELT, including external independent members, to be responsible for strategic governance oversight of the management of IT assets and delivery of IT.
152. Reviewing IT policies, processes and governance structures.
153. Strengthening the Architecture Review Board with a formal terms of reference and more structured ways of working.
154. Establishing Terms of Reference for the Design Authority and the Change Review Board and refreshing the ongoing structure of the meetings.
155. Strengthening the mandate of the Project Management Office including a more formal decision making framework and clearer ownership of the risks and an enterprise view of business needs.
156. Formally appointing the CIO as a member of Kaiurungi.
157. Strengthening the IT leadership team with a Digital Channels Manager role with responsibility for publishing, as well as a new Principal Advisor IT role.

Strengthening security maturity

158. Appointing a member of ELT as Chief Security Officer and reaffirmed the Chief Information Security Officer role.
159. Refreshing the Security Governance Committee chaired by the Chief Security Officer.
160. Updating the Security Policy including creating a summary for easy reference by staff.
161. Ongoing broad based security awareness campaign for all staff including holding workshops with staff to enhance awareness of security policies and requirements.
162. Implementing an annual attestation by all staff that they have read and understood the Security Policy, which has been completed by 100% of staff.
163. Recruiting an additional Senior Security Advisor to support the existing Information Technology Security Manager.
164. Commissioning a review of the security of our external websites including further independent penetration testing and review of security certificates.
165. Undertaking an independent security review of our critical IT systems to determine any gaps in security processes, documentation of policy and processes, and implementing any remediation or improvements required.
166. Re-certifying www.treasury.govt.nz through the certification and accreditation process.
167. Implementing new automated web and publications controls including a workflow tool that reduces the risk of accidental publication, builds in peer review and business approval, and provides the ability to quality assure documents prior to publication.
168. Putting in place new escalation tools for staff to raise concerns about security including the "See something, say something" awareness campaign.
169. Launching an online security training tool.
170. Reviewing security of personal data held by the Treasury to ensure compliance with Government Chief Privacy Officer advice on handling Personal Information.

Strengthening Treasury governance and risk management

171. Updating all corporate policies and establishing a system for keeping them up to date.
172. Refreshing our risk appetite framework and risk processes.
173. Launching a project to embed risk management in the way the Treasury operates.

174. Updating delegations policy and matrix.
175. Reviewing governance arrangements including the purpose and Terms of Reference for ELT and Kaiurungi and engaging an external governance expert to finalise the changes.
176. Reviewing our key advisory groups including the Risk and Assurance Committee and the Treasury Board Charters.
177. Refreshing the incident management plan for the organisation.
178. Implementing a new triage tool for incident management.
179. Updating our register of compliance with legislative and non-legislative requirements.

APPENDIX 1 – TERMS OF REFERENCE

Inquiry into the Treasury's Budget related Information Security Systems

Background

Two days before Budget Day 2019/20, documents were publicly released that contained Budget sensitive information. The information had been accessed from the Treasury's website.

Access to this information appears to have been possible because as part of its preparation for Budget Day, the Treasury developed a clone of its website. Budget sensitive information was added to the clone website as and when each Budget document was finalised. On Budget Day, the Treasury intended to swap the clone website to the live website so that the Budget information was available online. The clone website was not publicly accessible.

However, as part of the search function on the Treasury's website, content is indexed to make searches faster. Search results are presented with the text in the document that surrounds the search phrase. When the clone website was created all the settings for the live website were copied including where the index resides. This led to the index on the live website also containing entries for content that was published only on the clone website. As a result, specifically worded searches were able to surface small amounts of content from the 2019/20 Budget Estimates documents.

Objective of the Inquiry

The Budget process is a core function of the Treasury and is of fundamental significance to the operation of government. Given that the integrity of the Budget process is a matter of high public importance, it is necessary to conduct an inquiry.

The objective of the Inquiry is to address concerns raised by this incident about the security of the Treasury's Budget process, focusing on what happened, why it happened, the lessons learned, and the actions the Treasury needs to take to ensure that a similar incident will not happen again.

Scope of the inquiry

The inquirer is to investigate, make findings on, and report to the State Services Commissioner regarding:

- The circumstances surrounding this incident, including the security measures taken in response.
- The causes of the incident, including whether the Treasury adhered to its own internal policies relevant to the security of Budget sensitive information and to applicable government-wide policies and good practice guidance.
- The appropriateness and effectiveness of the information security systems that the Treasury had in place in relation to the final six-week production phase of the Budget Process. This will include an assessment of the relevant policies, processes, governance, capability and security culture and practice of the Treasury.
- Any linkages or implications for the Treasury's wider information security systems.

- Any other relevant matters necessary to provide a complete report on the above.

Out of scope

The inquiry may refer to, but will not make any findings in relation to, the following actions that were taken by the Secretary of the Treasury in responding to this incident and explaining its causes: the advice given to the Minister of Finance at the time; the Secretary's decision to refer the matter to the Police; and the public statements about the causes of the incident. The State Services Commissioner is assessing the appropriateness of those actions in a separate investigation.

In addition, the inquiry will not make findings on whether there should be further steps taken to initiate disciplinary, civil or criminal proceedings in relation to any individual.

Appointment

The State Services Commissioner appoints Ms Jenn Bestwick to undertake this inquiry.

Functions and Powers

Pursuant to section 23(1) of the State Sector Act 1988 and, for the purposes of the inquiry, the State Services Commissioner delegates his functions and powers under sections 7 to 9, and 10 of the State Sector Act to Ms Bestwick, with effect from 14 November 2019.

Application of provisions of the Inquiries Act 2013

The State Services Commissioner certifies it is reasonably necessary that the provisions of the Inquiries Act 2013, specified in section 9A(2) of the State Sector Act, apply in relation to the inquiry. This is because:

- Ms Bestwick should have powers to regulate the procedures of the Inquiry, including the gathering of additional evidence; and
- Given the nature of the Inquiry, and the need to balance the public interest in disclosure with the privacy interests of potential witnesses, the Inquirer should have the power to restrict access to the information he/she receives.

The previous inquiry

A previous inquiry in relation to this matter commenced on 11 June 2019 and was terminated on 13 November 2019, due to an undeclared conflict of interest within the inquiry team. Evidence gathered by the previous inquiry may be re-used by Ms Bestwick in undertaking this inquiry. Transcripts of interviews, however, may only be considered with the consent of each interviewee.

Reporting

The Inquirer is to report her findings to the State Services Commissioner in writing on or before 28 February 2020.

If Ms Bestwick identifies issues which may impact the delivery of her report by 28 February 2020, she will notify the State Services Commissioner as soon as possible with a view to resolving an appropriate solution, which may include an extension of time.

Peter Hughes
State Services Commissioner

13 November 2019

APPENDIX 2 – TIMELINE OF EVENTS LEADING TO THE INCIDENT

1	June 2014	Central Agencies Shared Services (CASS) issue a Request for Proposal (RFP) for Content Management System (CMS), platform and services for multiple websites and including the Budget Day Scenario (BDS).
2	July 2014	RFP closes with no preferred supplier identified.
3	September 2014	Scope of the RFP is reduced and approved.
4	November 2014	Second RFP is issued with a modified scope.
5	February 2015	Preferred supplier is identified and negotiations entered into for the Content Management System (CMS), visual design, build and support sections of the RFP. The infrastructure is to be managed in-house by CASS.
6	May 2015	A statement of work (SOW) is issued to undertake workshops to clarify the scope of the project.
7	May 2015	Workshops identified the project outlined in the RFP was not feasible.
8	May 2015	A 12 month implementation roadmap for the migration of websites for other agencies onto the Drupal platform is developed.
9	September 2015	The Treasury enters into a service agreement with the Vendor for Content Management System Support Services using the new Drupal platform with BDS) excluded.
10	2015/2016	Smaller websites are migrated onto the Drupal platform.
11	November 2016	Independent internal audit report on the information security follow-up review: governance frameworks and processes
12	January 2017	Base platform for the new Treasury website is built.
13	April/May 2017	Treasury uses clone methodology to produce 2017 Budget information on www.Budget.govt.nz
14	June 2017	BDS scoping and automation are removed from the vendor's deliverables for the project.
15	July 2017	The Treasury receives a timeline warning from the Vendor that they won't be able to deliver the new Treasury website if they encounter any further delays from Treasury.
16	July 2017	New Project Manager (PM) for the wider Drupal Platform and website build projects starts.
17	July 2017	A Business Case for the Treasury Website Migration (TWM) Project is produced that does not include Budget Day Scenario (BDS) requirements.
18	July 2017	Steering Group for the TWM project is stood up.
19	July 2017 – Feb 2018	Seven SOWs are issued to the vendor for base build, migration, implementation and content support over this time period.
20	August 2017	Migration of content onto the new Treasury website begins.

21	20 December 2017	Independent internal audit report on the Treasury Budget process review
22	29 January 2018	Independent report on the review of the Corporate Shared Services (CSS) Project Management Office (PMO)
23	February 2018	The Steering Group is made aware that there is no provision for delivering Budget 2018 on the new Treasury website
24	March 2018	The Treasury emails the vendor with a list of requirements for delivery of Budget 2018. The vendor notes that the tasks for BDS had been scheduled in the high-level production plan for 2016/17 to start in June 2017 and would take 6-9 months to fully complete.
25	14/15 March 2018	Two workshops with Treasury/CASS representation to discuss BDS options that would allow for the bulk upload of content; the clone method was agreed.
26	March 2018	The decision to clone the website is made; There is a clear demarcation between Treasury's infrastructure and the supplier's environment and role, the clone would be built and managed entirely within the CASS environment
27	March 2018	The new Treasury website goes live
28	April 2018	Independent internal audit report on Technology Risk Management
29	09 April 2018	SOW is issued to vendor for the approach and services to implement Budget Day Scenario 2018
30	April 2018	The Treasury Website Migration project closes
31	May 2018	Dry run of the clone and go-live process is conducted
32	10 May 2018	The Chief Architect undertakes a technical review of the digital publishing solutions for Budget 2018 and reports back to the CIO that things were in good shape, tracking to schedule and largely following the same track as previous years. The report (email) was later copied to the ITSM
33	May 2018	Budget 2018 is successfully delivered on the new Treasury website using the clone method.
34	April/May 2019	Budget 2019 production is underway using the clone method of 2018
35	25 - 28 May 2019	Logs of the Treasury website show 1923 searches performed in this period
36	1:05pm 28 May 2019	The Treasury call the vendor about the incident and their concerns about the unusual behaviour of the search function on the live website.
37	1:10pm 28 May 2019	The vendor responds to the call from Treasury as a P1 incident. Before going to Treasury the vendor performs some due diligence and witnessed controls in place for the environment the vendor supports i.e. the internal environment the vendor has access to.
38	1:15pm 28 May 2019	Two representatives from the vendor arrive at Treasury; one of them sits with a CASS IT staff member and identifies the clone site is not vaulted because of the shared index configuration.

39	1:50pm 28 May 2019	The CASS IT staff member with support from the vendor remediates the settings for the clone and re-indexes the site using an alternative method prescribed by the vendor.
40	2:30pm 28 May 2019	The clone site is secured by CASS IT staff with the assistance of the vendor. The vendor stays on site until 5:00pm.