Summary of Department of Service Nova Scotia and Internal Services Implementation of Recommendations in IR19-01
(Department formerly known as Department of Internal Services)

Recommendation #1: Strengthen privacy leadership in government and due diligence in privacy impact assessments	
The Department of Internal Services' implementation activities include: • Issuing a directive from the Chief Information Officer requiring tech projects to assess and mitigate risks before going live; • Publishing a detailed guide to writing privacy impact assessments; • Training IAP Services staff in a Canadian Information Access and Privacy certification program; and, • Initiating a Privacy Forum across multiple government departments. To complete this recommendation the Department must: • Demonstrate that the privacy impact assessment process is producing more diligent assessments and that the Privacy Forum is effective in strengthening privacy leadership.	In progress
Recommendation #2: Contain the breaches	
The Department of Internal Services received confirmation from Halifax Regional Police that the records on the computer used in breach #1 will not be returned to the individual. The Department followed up on breaches #2-12 and obtained a signed statutory declaration from the responsible individual attesting that no copies of the records were made or shared and that the device used during the breach was destroyed. The Department completed two scans of the internet and found no evidence that the breached records were posted online and it plans to conduct another scan after one year.	Complete
Recommendation #3: Correct under notification of affected individuals	
The Department of Internal Services completed a risk assessment for additional affected individuals who were not originally notified. The risk assessment took into account that the person who acted in breaches #2-12 was identified and provided assurances along with the assurances provided by the Halifax Regional Police. The Department determined that the risk to other affected individuals was so low that it does not constitute a risk of harm or embarrassment and therefore decided not to notify any additional affected individuals.	Complete
Recommendation #4: Conduct internal post-incident review	
The Department of Internal Services' implementation activities include: • Messaging all members of the Department with a link to IR19-01, encouraging all to read it; • Sending a message from the Deputy Minister to all executive directors in the Department and to all staff involved in the implementation of IT projects to highlight their role in due diligence and carrying out the Department's action plan in response to the breaches. • Sending a message from the Deputy Minister to Deputy Ministers and other colleagues across government with a link to IR19-01, encouraging all to read it; • Giving a follow-up presentation to all information and computer technology services staff about the report and the Department's action plan; • Receiving a consultant's final report on post-incident review.	Complete
Recommendation #5: Review other technologies for security vulnerabilities	
The Department of Internal Services has identified a set of asset, technology, and information inventories that already exist which it will use to begin the assessment of security vulnerabilities and to create a plan.	In progress

To complete this recommendation the Department must: • Identify the assets and technologies that are most vulnerable and create a plan to mitigate those first with firm commitments and deadlines; and • Create a longer-term plan to complete the assessments and risk mitigation for all government assets and technologies.	
Recommendation #6: Clarify and strengthen the role of the Architecture Review Board	
The Department of Internal Services received a consultant’s report on the role of the Architecture Review Board. The chief information officer issued a directive to the Department requiring all projects and initiatives that introduce new architecture or change existing architecture, data or data flow for both on-premise and externally hosted solutions be reviewed and approved by the Architecture Review Board. To complete this recommendation the Department must: • Complete the review of the Architecture Review Board and implement terms of reference, guidelines, process requirements and standards to support a stronger role for the Architecture Review Board.	In progress