|  |  |
| --- | --- |
| Question | **Answer** |
| Do we need to label both documents and emails by August 2020? | The protective marking reform grandfathering period is until Oct 2020. This timeframe aligns with the Commonwealth government's requirements outlined in the Protective Security Policy Framework (PSPF). |
| Do you have any accessibility friendly materials i.e. BILS reckoner and guides? | We are publishing a lot of content in HTML and word documents. If there is a document that you are having trouble accessing, please contact the Information Security Unit by emailing [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au) |
| Does an organisation have to address all 12 standards? | Yes |
| Has the information asset template altered? In particular, has there been changes to the recommended metadata that needs to be registered? | Yes, some of the content has changed based on feedback from partnering regulators and administrators. Please refer to the new [IAR template](https://ovic.vic.gov.au/resource/sample-information-asset-register-iar-template/) on the OVIC website. |
| I'm struggling to find the new resources online. Please help! | For resources relating to the Framework and Standards, please visit our resources page: <https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/> |
| Is there a plan for an eLearning on assessing information, using the BILs table, the application of Protective Markings and handling responsibilities? | Great question! This is something we are looking at in 2020. We are also launching Communities of Practice in 2020 which will provide opportunities to discuss eLearning requirements. |
| Is there still a requirement to have a data protection policy? | The security documentation an organisation develops may come in differing formats to suit their environment. This could take the form of a suite of documents, an information security policy, a framework, standards etc.  Organisations should refer to element E1.010 which states "The organisation documents a contextualised information security management framework (e.g. strategy, policies, procedures) covering all security areas." |
| Thank you for the document map-love the visual | Thank you for your feedback! |
| What happened to the High-Level PDSP and Self-Assessment? | The High-level PDSP and Self-Assessment have now been combined into the new PDSP form. |
| What has happened to the mobile app that we had to select Business Impact Levels (BILs)? | The mobile BIL app has not been updated yet to reflect the new BIL table and protective markings. We know this was a popular tool and are considering what other tools may serve the same purpose.  For those looking to perform a manual BIL assessment, please refer to the [Practitioner Guide: Assessing the Security Value of Public Sector Information.](https://ovic.vic.gov.au/resource/practitioner-guide-assessing-the-security-value-of-information-v2-0/) |
| What is difference between SRPA and self-assessment? | The SRPA is the security risk process organisations undertake to identify, assess and evaluate their information security risks.  The self-assessment is an assessment against the standards themselves and look at how the organisation is going with implementing the elements under each standard. The self-assessment is contained in the updated [PDSP form](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/pdsp-submission/) which can be downloaded from the OVIC website. |
| What is second column in the VPDSS Implementation Guide? | The second column of the [VPDSS Implementation Guide](https://ovic.vic.gov.au/data-protection/standards/) as shown in the presentation is a mapping to the previous iteration of the standards (V1.1). |
| What is the benefit of joining GovTEAMS? | Members of the [VISN](https://ovic.vic.gov.au/data-protection/for-agencies/victorian-information-security-network/) GovTeams community can access archived information security resources and VPS exclusive consultation material. In later release of the community additional features will be rolled out, allowing members to collaborate with one another. |
| Who can join GovTEAMS? | Anyone! |
| What's the rationale for the markings and the use of special characters? E.g. // | The administrative controls for the marking and labelling of public sector information aligns with the Commonwealth PSPF, enabling information sharing and informing the handling requirements for this material.  For more information on how to manage protective marked material in Vic Gov, refer to [Practitioner Guide: Protective markings](https://ovic.vic.gov.au/resource/practitioner-guide-protective-markings-v2-0/), and [the User Guide: Handling protectively marked information](https://ovic.vic.gov.au/resource/user-guide-handling-protectively-marked-information-v2-0/).  For more information on the Commonwealth PSPF labelling and handling requirements please refer to - <https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx> |
| When does the Incident Notification Scheme come into effect? | The Incident Notification Scheme has commenced.  Organisations should be notifying OVIC of information security incidents, following the process outlined here: <https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/> |
| When is the 2020 PDSP due? | 2020 PDSPs must be submitted no later than the 31st of August.  For information on PDSP submission, please visit: <https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/pdsp-submission/> |
| When will the Information Security Management Collection version be available please? | The former VPDSF Information Security Management Collection has been split up into three practitioner guides. These can be downloaded from our website.  Please visit the [VPDSF Resources](https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/) page of the OVIC website to download your copy. |
| Where can I find a list of the Elements? | A list of the Elements can be found in the VPDSS Implementation Guide, found here: <https://ovic.vic.gov.au/data-protection/standards/> |
| Where can I learn more about the new protective marking scheme? | For information on selecting an appropriate marking under the new scheme, please visit the [VPDSF Resources](https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/) page of the OVIC website. |
| Who was consulted in the redevelopment of the Standards? | An invitation to provide feedback on the redevelopment of the Standards was sent out to VISN members, VPS personnel, industry partners and members of the public. |
| Will OVIC issue a compliance report similar to the PSPF Compliance report that shows maturity and security status across the state? | With the release of the [new PDSP form](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/pdsp-submission/), OVIC will be able to analyse organisations responses in a more efficient and effective way.  This analysis will then be fed back to organisations to enhance their information security work programs. |
| Will the Standards / Framework be re-named to VPISF VPISS? | Not at this stage. We are bound by the terms used in the Privacy and Data Protection Act so the terms VPDSF and VPDSS will continue to be used. |
| Will you be providing guidance on the maturity levels in the self-assessment? | Yes! |
| Does a SRPA need to be redone in accordance with new standards, or can we use old (still valid) SRPA to develop self-assessment. | A Security Risk Profile Assessment (SRPA) is not an artefact or document. Rather, the term ‘SRPA’ refers to a process under which organisations continually assess their information security risks.  Organisations should revisit their risk assessments and see whether these are still current, updating them where required. These will inform the PDSP due in August 2020. |
| How does information notification scheme relate to DRFs cyber incident response service / will you be working with DTF in areas where they cross over? | In answering this question, we have assumed reference to DTF was a typo and it was instead intended to read DPC.  When developing the Incident Notification Scheme, OVIC worked with the DPC team who manage the Cyber Incident Response Service (CIRS), ensuring both groups referenced consistent incident notification thresholds and criteria.  Further information on the scheme can be found under the VPDSF Resources section of the OVIC website;   * [Overview of Incident Notification Scheme](https://ovic.vic.gov.au/resource/ovic-information-security-incident-notification-scheme-v1-0/) * [How to notify](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/) |
| Is it possible to release all documentation in a spreadsheet format? (My intuition is that many of us end up going through the same copy and reformat process) | In this recent release of material, the Information Security Unit has produced a [Document Map (November 2019)](https://ovic.vic.gov.au/wp-content/uploads/2019/11/VPDSF-Document-Map-November-2019.pdf) to help organisations readily identify what guidance material is available.  Where appropriate, some of this guidance material is available in excel form. |
| What happens to the current actions that arose from the v1.0 | Organisations should map their existing efforts, using the guidance tools provided under the VPDSF Resources section of the OVIC website:   * [VPDSS 2.0 to 1.0 Mapping](https://ovic.vic.gov.au/resource/mapping-vpdss-v1-0-to-v2-0/) |
| Question around Organisations previous PDSP action plans mapping to the new PDSP reporting requirements.  Concerns around action plans that arose from issues under the previous scheme not translating into the new scheme or a new action plan. | The Information Security Unit has produced a mapping document, outlining transition from the old [Standards (V1.0) to the new Standards (V2.0).](https://ovic.vic.gov.au/resource/mapping-vpdss-v1-0-to-v2-0/)  Previous action plans should map consistently to the new scheme.  If you have any queries, please speak with the Information Security Team. |
| Question around third party arrangements: Is guidance going to be issued for practitioners? | Yes - Guidance on this topic is coming |
| When will you update the Framework? | A refreshed Framework document will be released in February 2020. |
| Is there a way that we can get endorsement from OVIC regarding implementation of Protective Markings that deviate from the current guidance material? | The VPDSS protective marking requirements align with those set out in the Commonwealth Protective Security Policy Framework (PSPF).  Where organisations seek to deviate from the guidance issued by OVIC, we encourage them to consult with the Information Security Unit first. |
| Question around now PDSP which is now PDF based:  Is there going to be an API format associated with the PDF?  A csv. format or variant, for example, would be ideal for orgs so that they can extract data from their systems. | OVIC has not looked into API capability. The intent of the PDF form was to accurately report back to Government and organisations. |
| When is reporting required? | The PDSP and attestation is due by no later than 31 August 2020. For more information, please refer to the OVIC website:   * [PDSP Submission](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/pdsp-submission/) |
| So, the PDSP is due at the end of August 2020 and Protective Markings are due Oct 2020.  For small organisations are struggling with resources, can you get extensions of time? | Yes this is correct.  The PDSP submission timelines are set out in Part Four of the Privacy and Data Protection Act 2014. The Standards and subsequent reporting requirements are legislated and need to be completed in the timeframes advised.  The October 2020 timeline for the transition of the protective markings was informed by the Commonwealth PSPF requirements. Victorian Government is aligning with these, in order to promote secure information sharing across jurisdictions.  If there are specific concerns or issues within your organisation, please reach out to our Business Engagement Officers (BEOs). With the commencement of Communities of Practice, in February, there may be opportunity to leverage off the work of other organisations as well. |
| How will version 2 impact on implementation of standards. There are concerns around resourcing. | We understand that Version 2.0 of the Standards will involve some work, however the tools provided on the OVIC website should assist organisations in mapping their existing efforts.  For those undergoing 'significant change', please get in touch with OVIC early, to discuss your requirements. |
| How long should it take to get a response for a direction on 'significant change'? | Each notification of 'significant change' must be considered on a case by case basis. Some changes may be due to Machinery of Government's (MoGs), whereas others may be due to changes to the threat environment.  For this particular matter, the Information Security Unit has been working with MFB to find out more. Given the complexity of the issues involved in this particular MoG, the advice involved, and the subsequent actions do require some thought and effort to work through. Our Business Engagement Officers (BEOs) will continue with work with MFB. |

Further Information

**Contact Us**

**t:** 1300 00 6842   
**e:** enquiries@ovic.vic.gov.au  
**w:** ovic.vic.gov.au**Disclaimer**

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Freedom of Information Act 1982, or Privacy and Data Protection Act 2014 or any other legal requirement, to individual cases.