SEC TEMP 01.1	IS &IDAM Standards	Mandatory requirement	Criteria for compliance (Examples only)	Optional Additional Supporting Information / additional or equivalent controls	Current Compliance Status	Compliance Gap Criteria Not Met	Proposed Mitigation Plan (From *ICT Risk Assessment*) Mitigation Plan	Residual Compliance Status
GOV-1	SEC/STD/01 Information security management framework SEC/STD/05 Information security - User awareness training	Agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware of, and meet the requirements of the Agency's Information Security Policy.	Apply the Security awareness training guidelines have in place an ongoing security awareness program to inform and regularly remind individuals of security responsibilities, issues and concerns have briefed all Victorian Government employees and contracted service providers who hold a Negative Vetting Level 1 or higher level security clearance at least every five years as a condition of security clearance renewal. and have communicated and made available to all staff, including contractors, their agency's protective security policies.					
GOV-2	SEC/STD/01 Information security management framework	To fulfil their security obligations, agencies must appoint: a Senior Executive as the security executive, responsible for the agency protective security policy and oversight of protective security practices an agency security adviser (ASA) responsible for the day-to-day performance of protective security functions, and an information technology security adviser (ITSA) to advise senior management on the security of the agency's Information Communications Technology (ICT) systems.	the agency policy and procedures identify protective security roles and responsibilities the roles of security executive, ASA and ITSA have been assigned the functions of ASA and ITSA as described in *Australian Government protective security governance guidelines—Agency security advisers and IT security advisers functions and competencies* (as adapted - see *SEC STD 01 Information Security Management*) are clearly defined in their position descriptions and assessed against in their performance agreements					
GOV-3	SEC/STD/01 Information security management framework	Agencies must ensure that the ASA and ITSA have detailed knowledge of agency specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.	The ASA and ITSA are competent as detailed in the *Australian Government protective security governance guidelines—Agency security advisers and IT security advisers functions and competencies* (as adapted - see *SEC STD 01 Information Security Management)* the ASA and ITSA are responsible for the development, maintenance and review of agency protective security policy and procedures					
GOV-4	SEC/STD/01 Information security management framework	Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised every two years or sooner when changes in risks and the agency's operating environment dictate.	a security plan, covering all agency sites and operations, exists and covers the areas outlined in the *Australian Government better practice governance guidelines—Developing agency protective security policies, plans and procedures* consultation across major business areas within the agency and any business requirements are documented within the plan general security requirements are documented within the plan a documented risk assessment which informs the development of the plan agency head has signed-off on the plan the date of the plan's last review is not more than two years old the date for the plan's next review has been documented within the policy changes to business or new risks have been identified within the two year review period, and the plan has been updated to reflect those changes					
GOV-5	SEC/STD/01 Information security management framework	Agencies must develop their own set of protective security policies and procedures to meet their specific business needs.	protective security policies, plans and procedures exist, and covers the areas outlined in the *Australian Government protective security better practice guide—Developing agency protective security policies, plans and procedures* there has been consultation across major business areas within the policy business requirements have been documented within the policy a risk assessment has been documented and the results have informed the development of the policy legislative requirements relevant to the agency have been documented within the policy agency and whole of government policies relevant to the agency have been documented within the policy the policies and procedures are easily accessed by all employees agency head sign-off is given to the policies. plans and procedures the date of the policy's last review is not more than 2 years old the date for the policy's next review has been documented within the policy the policy has been updated to reflect any changes to business or identified new risks within the 2 year review period.					
Security risk management								
GOV-6	SEC/STD/01 Information security management framework	Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standards *AS/NZS ISO 31000:2009—Risk management—Principles and guidelines* and HB 167:2006 *Security risk management* .	the agency has developed its business impact levels, or adopted WoVG business impact levels (see *SEC GUIDE 01-3 Risk Management Criteria*) agency assets are identified and a business impact analysis was undertaken a threat and risk assessment was conducted and documented for all assets and the results inform the security plan the assessment's last review was not more than two years old the assessment was updated to reflect changes to business or identified new risks within the two year period					
Audit reviews and reporting								
GOV-7	SEC/STD/01 Information security management framework	For internal audit and reporting, agencies must: undertake an annual security assessment against the mandatory requirements detailed within this Framework. and report their compliance with the mandatory requirements as specified in the WoVG Information Security Management Framework Standard (2012) The report must use the template provided by DTF GSD Technology the report is to be submitted annually to DTF GSD technology and the Agency Executive and Risk and Audit Committee state any areas of non-compliance, including details on measures taken to lessen identified risks.	agency identified this reporting requirement and documented compliance and management compliance with the 33 mandatory standards has been mapped using these guidelines the agency head has endorsed the compliance review					
Security investigations								
GOV-8	SEC/STD/01 Information security management framework SEC/STD/06 Information security - Incident management	Agencies must ensure investigators are appropriately trained and have in place procedures for reporting and investigating security incidents and taking corrective action. *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations* (as adapted - see *SEC STD 01 Information Security Management*)	agency security incident management procedures have been documented and cover the review of and response to incidents as detailed in the *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations* (as adapted - see *SEC STD 01 Information Security Management*) records are maintained of security incident reports and corresponding investigations. Receipt of incident reports by relevant management channels disciplinary processes for deliberate violations or breaches of security policy have been approved by the agency head. Where these incident have occurred, agency records demonstrate that these processes have been applied agency records indicate that security incidents have been reported to appropriate authorities (e.g. DSD, police) where applicable					
Legislation								
GOV- 9	SEC/STD/01 Information security management framework	Agencies must give all employees, including contractors, guidance on applicable legislation requiring information protection including (but not limited to) the Information *Privacy Act (2001) and the Health Records Act (2000)* including how this legislation relates to their role.	staff are aware of and trained in the required legislative provisions with refresher courses available					
International security agreements								
GOV-10	SEC/STD/01 Information security management framework	Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Victoria is a party.	the agency has developed a guide to handling information from other governments (Commonwealth, State, Territory or foreign) when inviting dignitaries from other jurisdictions to agency events, the agency has considered any risks involved in such attendance staff being aware of and trained in the required provisions requirements being documented in the relevant policies and procedures					
Business continuity management								
GOV-11	SEC/STD/01 Information security management framework	Agencies must establish a business continuity management program to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment.	the agency has an approved business continuity plan (BCP) enabling the operational environment to be restored or recovered in the event of a major failure the ASA and ITSA are consulted in the development of the BCP business continuity risk and impact assessments processes have been approved. Agency records indicate that these assessments have been made, and inform the development of the agency's BCP existence of a risk register documenting how known risks will be managed (see GOV 6) the BCP has been regularly updated. Business continuity tests have been conducted on any weaknesses identified and have been addressed records show that all critical business processes and associated assets have been identified, prioritised and documented					
Contracting								
GOV-12	SEC/STD/01 Information security management framework	Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.	external security governance arrangements are in place in contracts as detailed in the *Australian Government protective security governance guidelines—Security of outsourced functions and services* (as adapted - see *SEC STD 01 Information Security Management*) external governance arrangements have been documented and approved by the agency head or authorised officer standard templates for contracts, service level agreements (SLAs) and operational level agreements (OLAs) including clauses dealing with protective security requirements routine checks of inclusion of protective security requirements in contracts. SLAs and OLAs being undertaken auditing of external party adherence to the agreements					
Fraud control								
GOV-13	SEC/STD/01 Information security management framework	Agencies must comply with the Financial Management Control Framework (FMCF):	fraud control policies and procedures relevant to the agency have been developed					
Personnel security								
PERSEC 1	SEC/STD/01 Information security management framework SEC/STD/02 Information security - data classification IDAM/STD/01 - Identity and access Mgt Staff authentication - evidence of identity IDAM/STD/03 - Identity and access Mgt Staff authentication -	Agencies must ensure that State Government employees, contractors and temporary staff who require ongoing access to Government information and resources: are eligible to have access have had their identity established are suitable to have access. and are willing to comply with the Government's policies, standards, protocols and guidelines that safeguard that agency's resources (people, information and assets) from harm. Access to higher levels of classified resources is dependent upon the granting of the requisite security clearance.	the agency develops personnel security polices, plans and procedures using the controls detailed in the Australian Government personnel security protocol and the Australian Government personnel security management guidelines—Agency personnel security guidelines (as adapted - see *SEC STD 01 Information Security Management*) job descriptions include protective security requirements agency personnel security policies having been approved by the agency head induction program documents include personnel security a security training plan has been approved by the agency head. Attendance records for the training have been kept. security awareness programs have been implemented using the *Australian Government protective security governance guidelines—Security awareness training* (as adapted - see *SEC STD 01 Information Security Management*)					
PERSEC 2	SEC/STD/01 Information security management framework	Agencies must, as part of their risk management approach to protective security, identify designated security assessed positions (DSAPs) within their agency that require access to CONFIDENTIAL, SECRET and TOP SECRET assets and information. Agencies must ensure that security vetting is only applied where it is necessary.	all positions requiring access to CONFIDENTIAL, SECRET and TOP SECRET assets and information have been documented in a DSAP register as detailed in the *Australian Government personnel security management guidelines—Agency personnel security guidelines* (as adapted - see *SEC STD 01 Information Security Management)* security clearances are only conducted for people occupying positions or performing functions assessed as needing a clearance as detailed in the *Australian Government personnel security management guidelines—Agency personnel security guidelines* (as adapted - see *SEC STD 01 Information Security Management)*					
PERSEC 3	SEC/STD/01 Information security management framework	Agencies must maintain a DSAP (DSAP positions or equivalent) register. The Vic Govt contact for DSAP is Jo Tan DPC.	all DSAPs are registered as detailed in the *Australian Government personnel security management guidelines—Agency personnel security guidelines* (as adapted - see *SEC STD 01 Information Security Management)*					

PERSEC 4	SEC/STD/01 Information security management framework	Security clearances must be sponsored by DPC. Security clearances are not available on demand or on a speculative basis. The Vic Govt contact for DSAP is Jo Tan DPC	a personnel security risk assessment has been documented and the results have informed requests for security clearances using the controls detailed in the *Australian Government personnel security protocol* and the *Australian Government personnel security management guidelines—Agency personnel security guidelines* (as adapted - see *SEC STD 01 Information Security Management*) requirements for security clearances are reviewed prior to revalidation of each clearance requirements for security clearances are assessed prior to advertising each position					
PERSEC 5	SEC/STD/01 Information security management framework	All Government agencies must follow the *Australian Government personnel security protocol* for personnel security,as contained in supplementary material within the PSPF. Only the DPC ASA can grant, continue, deny, revoke or vary a security clearance. The Vic Govt contact for DSAP is Jo Tan DPC	PSPF personnel security requirements have been documented within the aaency policy ongoing access to security classified information is subject to the granted of a suitable security clearance by the Vic Govt accreditation authority (contact for DSAP is Jo Tan DPC)					
PERSEC 6	SEC/STD/01 Information security management framework	Agencies must have in place personnel security aftercare arrangements, including the requirement for individuals holding security clearances to advise the Vic Govt contact for DSAP (Jo Tan DPC) of any significant change in personal circumstance that may impact on their continuing suitability to access security classified resources.	agency policy requiring security clearance holders to report significant changes in personal circumstances to the DPC ASA as detailed in the *Australian Government personnel security management guidelines—Reporting changes in personal circumstances guidelines* (as adapted - see *SEC STD 01 Information Security Management*) agency policy requires all employees to report suspicious contacts as detailed in the *Australian Government personnel security management guidelines* (as adapted - see *SEC STD 01 Information Security Management*) agencies advise DPC ASA of any information relevant to a clearance holder's ability to continue to hold a security clearance					
Information security								
INFOSEC 1	SEC/STD/01 Information security management framework SEC/STD/05 Information security - User awareness training	Agency heads must provide clear direction on information security through the development and implementation of an agency information security policy and an agency information security plan as part of the overall agency security plan.	the agency has developed an information security plans policies and procedures meeting the controls detailed in the *Australian Government information security management protocol* (as adapted - see *SEC STD 01 Information Security Management*) and supporting guidelines, and *ISO/IEC 27002:2005—Information technology—Security techniques—Code of practice for information security management* the aaency information security policies and plans have been: - endorsed by the aaency head - reviewed and evaluated in line with changes to aaency business and information security risks - communicated on an on-going basis and is accessible to all agency employees, and where reasonable and practical, publicly available information security roles and resoonsibilities have been identified the policies and plans detail the tvoes of information that an emplovee: - can lawfully disclose in the performance of - must obtain authority to disclose the policies and plans are consistent with the requirements of the agency's protective security plan and information security risk assessment findings the policies and plans addresses the issue of data aatreation an aaency declassification proaram exists. and consequences for breaching the policies or circumventing any associated protective security measure have been explained					
INFOSEC 2	SEC/STD/01 Information security management framework SEC/STD/05 Information security - User awareness training	Each agency must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency's information environment.	the agency has developed an information security plans policies and procedures meeting the controls detailed in the *Australian Government information security management protocol* (as adapted - see *SEC STD 01 Information Security Management*) and supporting guidelines, and *ISO/IEC 27002:2005—Information technology—Security techniques—Code of practice for information security management* the policies and plans details the requirements for information security when entering into outsourcing contracts and arrangements with contractors and consultants as detailed in the *Australian Government protective security governance guidelines—Security of outsourced functions and services* (as adapted - see *SEC STD 01 Information Security Management*) entering into memorandums of understanding (MOU) with other agencies when regularly sharing information and where reasonable and practical, make the MOU publicly available the agency has ensured that prior to providing any other third parties access to Victorian Government information and ICT systems, security measures that match the security classification or dissemination limiting marker of the information or ICT system are in place, or are clearly defined, in aaaroariate Deeds of Aareements or Confidentiality Aareements. and the agency has ensured that appropriate permissions are received before providing third parties access to information not originating within the agency.					
INFOSEC 3	SEC/STD/01 Information security management framework SEC/STD/02 Information security - data classification	Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats) which match their value, importance and sensitivity.	all major information assets including hardware, software and services used in agency operations (including physical information assets used to process, store or transmit information) have been identified and their impact assessed using agency impact level guides based on WoVG guidelines - see *SEC GUIDE 01-3 Risk Management Criteria* All information assets have been assigned owners for the maintenance of security measures the classification of all agency information is in accordance with the *Australian Government information security management guidelines—Australian Government security classification system* (as adapted - see *SEC STD 01 Information Security Management*) a classification guide specific to the agency has been developed, maintained and is accessible to all agency employees using the *Australian Government protective security better practice guide—Developing an agency classification auide* the agency's classification guide does not limit the provisions of relevant legislative requirements or international obligations under which the agency operates the control of all sensitive and security classified information (including handling, storage, transmission, transportation and disposal) is in accordance with the *Australian Government information security management protocol* and the *Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information* (as adapted - see *SEC STD 01 Information Security Management*), and disposal of public records has been in accordance with legislative and regulatory requirements.					
INFOSEC 4	SEC/STD/01 Information security management framework SEC/STD/02 Information security - data classification SEC/STD/04 Information security - use of portable storage devices	Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security.	the agency has developed information security plans policies and procedures meeting the controls detailed in the *Australian Government information security management protocol* (as adapted - see *SEC STD 01 Information Security Management*) and supporting guidelines, and *ISO/IEC 27002:2005—Information technology—Security techniques—Code of practice for information security management* there are incident management procedures and mechanisms to review violations and to ensure appropriate responses in the event of security incidents, breaches or failures in place as detailed in the *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations* (as adapted - see *SEC STD 01 Information Security Management*) there are adequate controls to prevent, detect, remove and report attacks of malicious and mobile code on ICT systems and networks in place there are comprehensive systems maintenance processes and procedures including operator and audit/fault logs and information backup procedures in place operational change control procedures are in place to ensure that they appropriately approve and manage changes to information processing facilities or ICT systems implemented there is compliance with legal requirements when exchanging information in all forms. between aencies and/or third parties the application of the classification schemes and measures defined in the *Australian Government Information Security Protocol* (as adapted - see *SEC STD 01 Information Security Management*) and the ISM when exchanging information in all forms, between agencies and/or third parties, and the application of the requirements of the National e-Authentication Framework to online transactions and services.					
INFOSEC 5	SEC/STD/01 Information security management framework SEC/STD/02 Information security - data classification IDAM/STD/01 - Identity and access Mgt Staff authentication - evidence of identity IDAM/STD/02 - Identity and access Mgt Staff authentication - authentication mechanism strength IDAM/STD/03 - Identity and access Mgt Staff authentication - passwords IDAM/STD/04 - Identity and access Mgt Staff authentication - two factor credentials IDAM/STD/15 - User	Agencies must have in place control measures based on business owner requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Agency access control rules must be consistent with agency business requirements and information classification as well as legal obligations.	the agency has assessed access requirements against the National e-Authentication Framework the agency requires specific authorisation for people to access agency ICT systems the agency has assigned each user a unique personal identification code and secure means of authentication policies and procedures to manage operating systems security, including user registration, authentication management, access rights and privileges to ICT systems or application utilities have been defined, documented and implemented the agency applies the controls identified in the *Australian Government physical security management guidelines—Physical security of ICT equipment, systems and facilities* (as adapted - see *SEC STD 01 Information Security Management*) and the *Australian Government Information Security Manual* to restrict access to information systems where wireless communications are used, the agency appropriately configures the security features of the product to at least the equivalent level of security of wired communications the agency has implemented control measures to detect and regularly log, monitor and review ICT systems and network access and use, including all significant security relevant events the agency has conducted risk assessments and defined policies and processes for mobile technologies and tele-working facilities as detailed in the *Australian Government physical security management guidelines—Working away from the office* (as adapted - see *SEC STD 01 Information Security Management* . and the agency has assessed security risks and implemented appropriate controls associated with use of ICT facilities and devices (including non-governmental equipment) within the agency such as mobile telephony, personal storage devices and internet and email prior to connection					
INFOSEC 6	SEC/STD/01 Information security management framework SEC/STD/02 Information security - data classification	Agencies must have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks infrastructures and applications.	internal and/or external audit has been consulted when implementing new or significant chanaes to financial and critical business ICT svstems the agency has incorporated processes including data validity checks, audit trails and activity logging in applications to ensure the accuracy and integrity of data captured or held in applications the agency has applied the National e-Authentication Framework requirements to authentication techniques and policies the agency has carried out appropriate change control, acceptance and ICT system testing, planning and migration control measures when upgrading or installing software in the operational environment the agency has controlled access to ICT system files to ensure integrity of the business systems, applications and data, and the agency has identified and implemented access controls including access restrictions and segregation/isolation of ICT systems into all infrastructures, business and user developed applications.					
INFOSEC 7	SEC/STD/01 Information security management framework	Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the agency operates.	the agency has taken all reasonable steps to monitor, review and audit agency information security effectiveness, including assigning appropriate security roles and engaging internal and/or external auditors and specialist oraanisations where required. and the agency has regularly reviewed all agency information security policies, processes and requirements including contracts with third parties, for compliance and report to appropriate agency management.					
Physical security								
PHYSEC 1	SEC/STD/01 Information security management framework	Agency heads must provide clear direction on physical security through the development and implementation of an agency physical security policy and an agency physical security plan as part of the overall agency security plan.	physical security policies and plans are included in the agency security policies and plans all applicable controls as detailed in the *Australian Government physical security protocol* (as adapted - see *SEC STD 01 Information Security Management*) and supporting guidelines have been located in the physical security policy there has been consultation across major business areas in the development of the policy and plan business requirements have been documented within the policy a risk assessment has been documented and the results have informed the development of the policy and plan legislative requirements relevant to the agency have been documented within the policy agency and whole of government polices relevant to the agency have been documented within the policy the policy is easily accessible by all employees the agency head's signoff is located within the policy and plan the date of the policy's or plan's last review is not more than two years old					
PHYSEC 2	SEC/STD/01 Information security management framework SEC/STD/06 Information	Agencies must have in place policies and procedures to:	agency policies and procedures address the personal security of employees based on the agency risk assessment and in consultation with agency safety personnel as detailed in the *Australian Government physical security protocol* (as adapted - see *SEC STD 01 Information Security Management*) and supporting guidelines					

	security - Incident management	· identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases. · report incidents to management, human resources, security and law enforcement authorities. as appropriate · provide information, training and counselling to employees, · maintain thorough records and statements on reported	· agency incident management procedures have been documented and cover the review of and response to incidents as detailed in the *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations* (as adapted - see *SEC STD 01 Information Security Management*) · have an ongoing security awareness program to inform and regularly remind individuals of issues and concerns as detailed in the *Australian Government protective security governance guidelines—Security awareness training* (as adapted - see *SEC STD 01 Information Security Management*)					
PHYSEC 3	SEC/STD/01 Information security management framework	Agencies must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.	· there has been consultation across major business areas regarding protective security prior to any new works in, or selection of new, agency premises · protective security requirements have been documented · a risk assessment has been documented and the results identified protective security requirements · the agency has prepared site plans using the controls in the *Australian Government physical security management protocol* and the *Australian Government physical security management guidelines—Security zones and risk mitigation control measures* (as adapted - see *SEC STD 01 Information Security Management*)					
PHYSEC 4	SEC/STD/01 Information security management framework	Agencies must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.	· employer occupational health and safety legislative requirements relevant to the agency have been documented within the policy · physical security policy and procedures have been developed in consultation with agency safety personnel					
PHYSEC 5	SEC/STD/01 Information security management framework	Agencies must show a duty of care for the physical safety of those members of the public interacting directly with the Victorian Government. Where an agency's function involves providing services, the agency must ensure that clients can transact with the Victorian Government with confidence about their physical wellbeing.	· there has been consultation across major business areas regarding client safety · agency policies and procedures addressing the safety of clients has been developed using the agency risk assessment and in consultation with agency safety personnel · agency incident management procedures have been documented and cover the review of and response to incidents involving clients as detailed in the *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations* (as adapted - see *SEC STD 01 Information Security Management*) · the agency has an ongoing security awareness program to inform and regularly remind employees of client safety as detailed in the *Australian Government protective security governance guidelines—Security awareness training* (as adapted - see *SEC STD 01 Information Security Management*)					
PHYSEC 6	SEC/STD/01 Information security management framework	Agencies must implement a level of physical security measures that minimises or removes the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.	· ICT equipment, systems and facilities are secured using the controls detailed in *Australian Government physical security management guidelines—Physical security of ICT equipment, systems and facilities* (as adapted - see *SEC STD 01 Information Security Management)*					
PHYSEC 7	SEC/STD/01 Information security management framework	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian and Victorian Government may direct agencies to implement heightened security levels.	· the agency physical security policies and plans based on the agency risk assessment which address heightened threat levels · there has been consultation across major business areas within the policy and plan · business requirements have been documented within the policy · the agency puts in place any pre-emptive physical security measures required for a heightened threat environment that cannot be easily deployed					