Australian Government
Department of Defence

Defence Security and Vetting Service
Intelligent security for an insecure world

Defence Security Manual

DSM Part	**2:2 Security Risk Management and Planning**				
Version	3	**Publication date**	July 2015	**Amendment list**	16
Optimised for	Screen; Print; Screen Reader				
Releasable to	Public				
Compliance Requirements	Defence personnel are, and external service providers subject to the terms and conditions of their contract may be, bound by security policy contained in the DSM and Information Security Manual (ISM). Failure to comply with the mandatory requirements of the DSM and ISM may result in action under the relevant contract provision or legislation including, but not limited to; the *Defence Force Discipline Act 1982*, the *Public Service Act 1999*, and the *Crimes Act 1914*. Mandatory requirements in the DSM and ISM are identified through the use of the terms **must** / **must not** and **should** / **should not.** Compliance with these requirements is mandatory unless the appropriate authority, if applicable, has considered the justification for non-compliance and accepted the associated risk through the granting of a dispensation. The terms ‘recommend’ and ‘may’ are used to denote a sensible security practice and non-compliance need not be approved or documented. **Note:** Non-compliance with a sensible security practice ought to be informed by sound risk management principles. The DSM compliance regime, including the authority to approve non-compliance with mandatory requirements, the use of dispensation indicators, and how to apply for a dispensation is detailed in DSM Part 2:1 *Dispensations*.				
Copyright	© Commonwealth of Australia 2010 This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Department of Defence. Requests and inquiries concerning reproduction and rights should be addressed to Defence Publishing Services, Department of Defence.				

Introduction

1. Security risk management and planning is the structured process used to determine the nature of threats, identify vulnerabilities, understand potential consequences of future events, and develop an approach to the conduct of security activities across Defence. Robust security risk management and planning enables informed, targeted and cost-effective allocation of resources and effort to the protection of Defence people, information assets and infrastructure in support of its capabilities and mission.

2. The purpose of Defence Security Manual (DSM) Part 2:2 is to detail policy for the application of the security risk management and planning process within Defence.

Policy

3. Defence will adopt a risk management approach to managing security. Security risks are to be identified and managed and risk treatments planned by commanders and managers in a manner consistent with AS/NZS ISO 31000:2009 *Risk Management: Principles and Guidelines* and the associated Handbook 167:2006 *Security Risk Management*

Principles

4. The principles underpinning security risk management are:

a. good security and good business complement each other;

b. security risk management is the business of everyone in Defence;

c. security risk management is part of day-to-day business; and

d. the process for managing security risks is logical and systematic, and should form part of the standard management process in each Group and Service.

Process

Australian/New Zealand Standard – Risk Management

5. AS/NZS ISO 31000:2009 and HB 167:2006 **must** [Auth:None] be used as the basis for security risk management in Defence in accordance with the requirements of the Protective Security Policy Framework (PSPF).

6. The risk management process is presented in varying degrees of complexity from the basic concept in AS/NZS ISO 31000:2009 to a more expansive concept tailored to security in HB 167:2006. An understanding of the basic concept in the parent standard can facilitate security risk management decisions where quick action is essential, such as for the application of short-term, physical, security-in-depth treatments in response to a rapidly emerging threat. However, a more rigorous application of the process as presented in HB 167:2006 is needed for longer term planning.

7. The risk management process involves the following steps, which are presented in detail in HB 167:2006:

a. communicate and consult;

b. establish the context (which includes the security threat);

c. identify risks;

d. analyse risks;

e. evaluate risks;

f. treat risks; and

g. monitor and review.

8. Additional guidance specific to Defence and relating to steps b, c, f and g above is detailed further in this DSM part.

Application of the Security Risk Management Process in Defence

9. The risk management process is applied to:

a. Defence as a whole;

b. Groups and Services;

c. Defence bases, establishments and industry facilities;

d. military or business units;

e. projects; and

f. events and activities

Establish the Context

10. The Defence Security and Vetting Service (DS&VS) supports commanders and managers at all levels in establishing the context for their own security risk management and planning by issuing the Defence Strategic Security Threat Assessment (DSSTA) and through the provision of advice. This ensures risks are identified and treated with common purpose and based on a common understanding of threats, threat modus operandi and of vulnerabilities.

11. The DS&VS develops the DSSTA as a high level threat assessment that draws on a range of sources, including, but not limited to:

a. Australian Security Intelligence Organisation (ASIO) for security threats;

b. Australian Crime Commission (ACC) and federal, state and territory police forces for criminal threats;

c. Australian Signals Directorate for ICT threats; and

d. Defence Intelligence Organisation for threats to military capability and operations.

12. The DSSTA is intended to be a practical guide, useful to all levels of command and management that will provide an understanding of the threats that pose a security risk to Defence. It includes an explanation of the modus operandi of each threat source. When conducting the security risk management process the DSSTA **must** be reviewed or threat advice **must be** obtained from DS&VS or a relevant Service Security Authority (SSA).

13. If there is insufficient information within the DSSTA for a local activity, such as a conference or other type of event, security threat advice, in the form of a tailored security threat assessment can be obtained from DS&VS or the relevant SSA.

14. Threat advice **must** only be sought from external sources to Defence by DS&VS or, in localised situations, the SSA.

15. To ensure the DSSTA is reactive to emerging or changing security threats, all Defence personnel **must** report to DS&VS any information they receive or become aware of threats to Defence concern. Commanders, managers and contract managers may seek assessment from DS&VS of that information and advice as to any change it causes to extant threat levels. On receipt of advice indicating a change to threat levels, commanders and managers **must** then reassess relevant risk.

Identify Risks

16. **Criticality assessment.** An important component of risk identification is, in the terms of HB 167:2006, a 'criticality assessment'. In the Defence context this involves the assessment of the compromise, loss of integrity or unavailability of information and security-protected assets and other critical contributors to capability such as people and infrastructure. This is essentially the identification of what needs protection, which is done by:

a. classifying official information;

b. assigning Business Impact Levels (BIL) to aggregated information and security-protected assets; and

Note: The processes of classification and assigning a BIL, identifies the value of information or security-protected assets to the national interest and Defence capability and informs the 'consequence' level in any risk assessment.

c. allocating a security priority to bases, establishments, facilities and military or business units.

Note: Bases, establishments, facilities and military or business units are provided a security priority by the First Assistant Secretary Security and Vetting Service (FAS S&VS) to assist Group Heads and Service Chiefs in the priority allocation of security resources across Defence. A security priority is shaped by the importance of information and assets protected by the facility, as determined by the classification/BIL process. A priority also influences the frequency of protective security surveys under the Defence Security Compliance Program.

Treat Risks - Security Planning

17. Application of the security risk management process results in a treatment plan. This is often referred to as a security plan and it captures identified risks, the analysis and evaluation of them and what treatments can be applied to mitigate the risks. Minimum compliance requirements within the DSM form the vast majority of risk treatments available to a commander or manager.

Note: In the case of aggregated information and security-protected assets, the assigned BIL will either dictate or provide guidance on the use of minimum security requirements. A classification will also dictate minimum security requirements for official information.

18. Where a risk is either not sufficiently treated by a minimum compliance requirement in the DSM or is not covered at all by a DSM requirement then the security plan **must** identify appropriate treatments. Where risk treatment cannot achieve compliance with DSM requirements then noncompliance **must** be managed and this is achieved through the dispensation process.

Review and Modify

19. Risk treatments should continually be reviewed, assessed, and modified in response to changes in the risk environment in which they work. Asset owners should explain acceptable levels of risk to assets based on the business impacts of a compromise of confidentiality, or loss or compromise of integrity, or availability. Such levels are to be examined during regular review and assessment processes.

20. The costs of compromise are to be quantified to the greatest extent possible as part of continuing risk management. Asset custodians are to select controls to effectively mitigate risk, and regularly measure and review their performance. Asset custodians should develop plans for remedial action to adjust risk mitigation deficiencies and carry out those plans following each review.

Security Risk Management and Planning on, and in, Bases, Establishments, Facilities and Military and Business Units

21. At a base level the responsibility for security risk management and planning falls on the Base Support Managers (BSM) and Senior ADF Officers (SADFO) in consultation with Heads of Resident Units (HRU) and if necessary subject matter experts. At a resident unit level the responsibility falls on each HRU.

22. The BSM, SADFO and HRU **must** align across a base the security risk management and planning process and are to ensure that security risk treatments are complementary, cost effective and able to contribute to overall security in depth for the base. Alignment allows HRU to abridge the process and their plan and focus specifically on threats and risks unique to their own organisation. As such it is recommended that unit security plans are annexed to and nested within the base security plan, which will avoid duplication of effort in the treatment of risk and is likely to introduce cost and resource efficiencies.

23. Base/unit security plans **must** [Auth:None] take into account the requirements of the *Work Health and Safety Act 2011* and associated regulations and codes of practice. Security plans are to identify and address any risks of harm to employees, contactors and the public arising from measures or activities designed to protect information and security-protected assets and take all reasonable practicable precautions to minimise those risks of harm.

24. If a base incorporates satellite sites, the BSM and SADFO **must** apply the security risk management process and **must** produce a security plan for each site. Each site manager is then responsible to any relevant BSM, SADFO or HRU for implementation of the base security plan (and aspects of any relevant unit security plan) at that site.

25. Contract managers **must** ensure that Defence Industry Security Program (DISP) members conduct the security risk management and planning process and produce a security plan that treats risks for DISP accredited facilities and ICT systems. Where a DISP accredited facility or ICT system is resident on a base or co-located with other Defence or Defence industry facilities, matters of alignment are relevant.

26. Where a Defence establishment or facility is managed by an external service provider under a contractual relationship, the relevant contract manager **must** ensure the contracted entity conducts security risk management and planning, which **must** result in a security plan for the establishment or facility.

Co-location with other Australian Government Agencies

27. Co-location with other Australian Government agencies involves cooperation and shared acceptance of risk, often through a Memorandum of Understanding. Where Defence co-locates with other agencies the protective security measures applied **must** address the collective risks that result from the collocation and any specific risk that an individual agency might face.

> **Note:** One consequence of this shared responsibility is greater complexity in negotiating the implementation of security measures. It could also mean that security advisers from a number of different agencies need to work cooperatively in developing the agreed arrangements.

28. **Diplomatic missions.** Defence elements located within or attached to an Australian diplomatic mission overseas are covered by the mission's security risk management and planning process. This falls within the Department of Foreign Affairs and Trade's broader security responsibilities.

Co-location with Foreign Government Agencies and Elements Overseas

29. **ADF operations.** Requirements for co-location of ADF units with foreign military forces on operations will be covered by operational security planning, however for long-term shared tenancy arrangements, security risk management advice **should** be obtained from the DS&VS.

30. **Non-operational activities.** Security risk management advice for addressing risk associated with co-location with foreign government agencies and elements overseas **must** be obtained from DS&VS.

Construction and Refurbishment Planning

31. The security risk management process **must** be commenced and a security plan **must** be prepared for any site associated with the construction or refurbishment of Defence infrastructure, including if the site is a 'greenfield' site.

SAFEBASE Planning

32. A base security plan **must** include a base-specific response to each SAFEBASE alert level as an enclosure.

33. An establishment, facility or military or business unit security plan **must** include a response to each SAFEBASE alert level as an enclosure. For those tenanted on a base, the enclosure will include only those aspects unique to that tenant that are not otherwise covered in the base security plan's SAFEBASE enclosure. For further information on SAFEBASE see DSM Part 2:3 *SAFEBASE*.

Event Planning

34. The security risk management process **must** be applied and a security plan produced for Defence events such as conferences, open days and visits by dignitaries. Where events occur within locations covered by an existing security plan, planning may only need to involve those issues unique to the event such as an increased risk profile and access by the general public. Further guidance on event planning is covered in Annex A.

35. **Specialist advice**. During the planning phase of an event it is recommended that representatives from all organisations that may have a security-related role or could themselves impact on the security effort are to be contacted for specialist advice and to coordinate and communicate security requirements. These organisations may include, but are not be limited to:

a. military and civilian police;

b. fire and emergency services;

c. guard force, ushers, marshals;

d. ambulance and medical services; and

e. public relations.

Roles and Responsibilities

Secretary of Defence and Chief of the Defence Force

36. The Secretary and CDF are accountable to the Minister for all security risks incurred by Defence. Specifically, they are responsible for ensuring that:

a. Defence develops and implements an agency security plan appropriate to its functions and the security risks it faces; and

b. its plan, comprising a five yearly Defence Security Strategy and a supporting annual Defence Security Action Plan, is monitored and reviewed to minimise security risks.

37. The Australian Government requires the Secretary to consider, as part of Defence security risk criteria, its policies and legislation associated with official information, freedom of information, privacy, work health and safety, and fraud, and any Defence related legislation.

Deputy Secretary Intelligence and Security

38. As the Agency Security Executive, the Deputy Secretary Intelligence and Security is responsible for implementing the strategy and implementation plans and reporting to the Secretary on their progress.

First Assistant Secretary Security and Vetting Service

39. FAS S&VS is responsible for:

a. assessing Defence-wide security risks, including:

(1) developing and issuing the:

i. DSSTA,

ii. Defence Security Risk Assessment,

iii. Defence Security Strategy Implementation Plan, and

iv. Defence Security Implementation Plan; and

(2) monitoring and reporting on implementation of the Defence Security Strategy and the Defence Security Implementation Plan.

b. the provision of security risk management and planning advice to Groups, Services and defence industry, including to BSM and SADFO during the development of base-level security risk assessments and plans.

c. the provision of domestic, non-operational protective security threat likelihood assessments and advice in support of the risk management process.

Note: FAS S&VS is the Defence authority for domestic, non-operational protective security threat likelihood assessments.

d. liaising with relevant external agencies about assessment of threat, including, but not limited to ASIO, the ACC and federal, state and territory police forces.

Group Heads and Service Chiefs

40. Group Heads and Service Chiefs are responsible for:

a. effective security risk management and planning through the development of an appropriate security risk management and planning framework for their Group or Service;

b. focussing risk treatment on areas of significant security risk and for monitoring and reviewing risk treatments and ensuring that they are appropriate to the level of risk and are cost effective;

c. the effective management and oversight of dispensations in their Group or Service; and

d. producing a Group or Service wide security risk assessment and security plan that addresses strategic-level risks unique to the Group or Service (ie those not captured in the Defence Security Implementation Plan).

41. **Defence business process owners.** Where Group Heads and Service Chiefs are business process owners under the Defence Business Model, they are responsible for:

a. identifying shared security risks to the business process and ensuring that affected Group Heads and Service Chiefs are made aware of the affect of these risks on their business; and

b. risk mitigation and for accepting any residual security risks to the business process that fall outside of Groups or Services.

42. **System owners.** Group Heads and Service Chiefs who are system owners are responsible for:

a. acceptance and management of the security risks associated with the operation of an ICT system, and

b. producing a security risk assessment and security plan for any ICT system for which they are responsible.

Note: Where responsibility for an ICT system is shared, so is the associated risk. If a single risk owner cannot be identified, then the risk beyond that which the system owner can reasonably be expected to own is considered residual risk. If residual risk cannot be allocated to another responsible officer, then the CIO, in the case of non-operational systems, or CJOPS, who is responsible for all aspects of operational security, accept it on behalf of the Secretary and CDF.

43. **Asset owners.** Group Heads and Service Chiefs who are asset owners are responsible for ensuring that assets for which they are responsible are risk assessed to determine the business impact and assigned the appropriate Business Impact Level (BIL), see DSM Part 2:7 *Business Impact Levels* for further information.

Deputy Secretary Defence Support and Reform

44. In addition to his or her Group Head responsibilities, Deputy Secretary Defence Support and Reform (DEPSEC DSR) is responsible for security services as described under a Memorandum of Understanding with other Group Heads and Service Chiefs for the delivery of security as a base support management service. DEPSEC DSR is responsible for the development and implementation of security plans for each Defence base.

Group/Service Security Executives

45. Group/Service security executives are responsible to their Group Head or Service Chief for the security risk management and planning process within their respective Group or Service.

Group/Service Security Advisers

46. Group/Service security advisers assist their Group/Service security executive and senior managers in analysing the Group/Service security environment and identification and treatment of unacceptable risks. They can be responsible for the delivery of localised threat advice and assessments within their Group/Service, where arrangements have been made with the DS&VS for this function to be exercised. The Service security advisers are supported by the SSA in their responsibilities.

Service Security Authorities

47. SSA are responsible for the provision of security risk management and planning advice to single-Service units. They are responsible for the delivery of localised threat advice and assessments to single-Service units. The SSA work closely with DS&VS in this regard and are responsible for obtaining threat advice from external agencies, such as state and territory police forces, with respect to localised security issues affecting single-Service units.

Base Support Managers

48. Each BSM is responsible to DEPSEC DSR, through Head Defence Support Operations, for:

a. developing and maintaining the base security plan;

b. coordinating HRU co-located in an individual office building to produce a consolidated office building security plan;

Note: Although BSM are responsible for coordinating production of an office building security plan, each HRU is responsible for internal routine workplace security of their respective unit.

c. assessing, with the input of the Base Security and Emergency Management Committee as necessary, unit security plans and office building security plans developed by HRU to ensure appropriateness from a whole-of-base perspective; and

d. the effective delivery of whole-of-base security services in accordance with the base security plan; and

e. clearly articulating security risk management and planning arrangements associated with any site that is geographically isolated from its base or parent unit, eg, having specific security responsibilities for that isolated site manager.

Note: It is particularly important that command, control and management of security at an isolated site during heightened SAFEBASE alert levels are viable.

Senior ADF Officer

49. Each SADFO supports the BSM in the achievement of the security risk management and planning responsibilities noted above. Each SADFO has particular responsibilities associated with assumption of command at heightened SAFEBASE alert levels.

50. SADFO are also responsible, at all SAFEBASE levels, for commanding the response to a security incident that requires a capability beyond that routinely available on the base and involving ADF members. This includes planning the response to a security incident that poses a serious threat to the people or assets at the base, such as a terrorist or other violent attack.

Commanders and Managers

51. Commanders and managers are responsible for the ongoing application of the security risk management process and the development of a security plan that provides treatments that are both

appropriate to the level of security risk and are cost effective. Where a commander or manager is co-located with the next level in their command or line management chain, the security risk management planning for their unit may, if appropriate, be subsumed into the planning for the broader organisational unit at the next highest level, or in some cases, at the whole-of-base or establishment level.

52. Commanders and managers are responsible for ensuring that security incidents are reported in accordance with the DSM. The effective reporting of security incidents will aid the DS&VS in developing threat and risk advice.

53. **System owners.** The following system owners are identified for command and management responsibilities in relation to the operation of Defence ICT systems:

a. the CIO for networks and systems comprising the Defence Information Environment (DIE), connected to the DIE or for which no single risk owner has been identified;

b. CJOPS for networks and systems deployed in the operational environment; and

c. Group Heads and Service Chiefs for stand-alone networks and systems not connected to, or part of, the DIE.

54. **Asset custodians.** Commanders and managers who are asset custodians, are responsible for:

a. factoring the management of security-protected assets for which they are the custodian into their security risk management and planning;

b. using the BIL assigned by asset owners, to:

(1) determine or provide guidance on any minimum security requirements, and

(2) inform the consequence descriptor in determining a risk rating as part of a security risk assessment.

55. **HRU.** Commanders and managers, who are HRU on a base, support the BSM and SADFO in the achievement of the aforementioned security risk management and planning responsibilities of the BSM. This involves collaboration with the BSM and SADFO in the identification of risks that can be treated at the base level.

Contract Managers

56. Contract managers are responsible for ensuring the conduct of the security risk management and planning process relating to Defence information or assets handled by external service providers. In regard to DISP members this will involve any DISP accredited facilities and ICT systems. Where risk treatments require acceptance they are responsible for facilitating risk management decisions by the appropriate Defence owner of a given risk.

57. Where DISP accredited facilities and ICT systems are associated with multiple contracts, the contract managers are responsible for coordinating, apportioning and facilitating the sharing of risk appropriate to the business impact level and aggregation of Defence information and assets associated with each contract.

External Service Providers

58. External service providers are responsible for the implementation of security plans and for following security instructions associated with Defence information or assets that they handle.

59. DISP members are responsible for the conduct of the security risk management process relating to DISP accredited facilities and ICT systems; however, they cannot accept residual risk and are to refer all

decisions for acceptance of risk to the relevant contract manager for action. During the conduct of the process it is recommended that DISP members consult DS&VS for advice.

Security Officers

60. Security officers are responsible to their commander, manager or DISP member executive for the implementation of a security plan.

Key Definitions

61. **Risk management**. The culture, process and structures that are directed towards realising potential opportunities whilst managing adverse effects.

62. **Security threat**. A source of harm to Defence achieving its security objectives.

63. **Security risk**. An event that could result in Defence not achieving its security objectives; measured in terms of its probable likelihood and consequences.

64. **Security risk management**. The culture, processes and structures that are directed towards maximising benefits and minimising adverse consequences for security, consistent with achieving business objectives

65. **Business Impact**. An assessment of the contribution that information or an asset(s) makes to Defence capability and the ability of Defence to perform its mandated functions over a given period of time.

66. **Business Impact Level**. A standardised rating, that forms part of a security risk management process, that identifies the level of impact on the national interest, Defence capability and Defence ability to perform its mandated functions resulting from a compromise of confidentiality, loss of integrity or unavailability of individual or aggregated information and assets.

67. **Security planning**. The risk treatment phase of the security risk management process, which involves the production of a treatment plan, often referred to as a security plan.

68. **Security plan**. A plan that documents the security objectives of an organisation, the risks that could impact on those objectives, the courses of action to be employed, the resources for managing the risks, and the action required to implement the management strategies.

69. **System owner**. The person responsible for the operation of an ICT system.

70. **Asset owner**. The Group Head or Service Chief with responsibility and accountability for the asset for which responsibility has been assigned to them.

71. **Asset custodian**. The commander or manager responsible for the protection of asset(s) upon issue to them.

72. **Contract manager**. For the purposes of the DSM, an APS employee or ADF member who is responsible for the contractual relationship with an external service provider.

Further Definitions

73. Further definitions for common DSM terms can be found in the Glossary.

Annexes and Attachments	
Annex A	Event Security (current version published July 2015)