Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 3

RISK MANAGEMENT

Version 1.0

Objectives

301. As a security decision making tool, risk assessment methodology aims to provide a degree of assurance that the priority or appropriateness of security countermeasures used to counter specified threats is commensurate with the risks. The risk assessment methodology used in this manual has been adapted from the Protective Security Manual (PSM), and the Australian Standard AS/NZ 4360:1999 titled "Risk Management". The objective of this handbook is to present a risk assessment strategy that is consistent with the operation of information systems. Accordingly, it is not meant to replace the guidelines on managing security risk as published in the PSM, but rather it is an adjunct to the PSM, relating to the application of security risk management in an information system environment.

Security Risk Management Process

302. The risk assessment process involves: identifying key system assets, identifying and quantifying the threat likelihood (wherever possible) against each asset, determining the consequence/harm profile against each threat, and calculating the current risk for each asset. Determining an acceptable level of risk for each asset/threat pair, and the priority of the associated countermeasure (in broad terms) are the next steps in the process. This process is shown in **Figure 1.1** and is consistent with the security risk management process presented in the PSM and the Australian Standard. The outcomes of the risk assessment are used to provide ***guidance*** on the areas of highest risk.

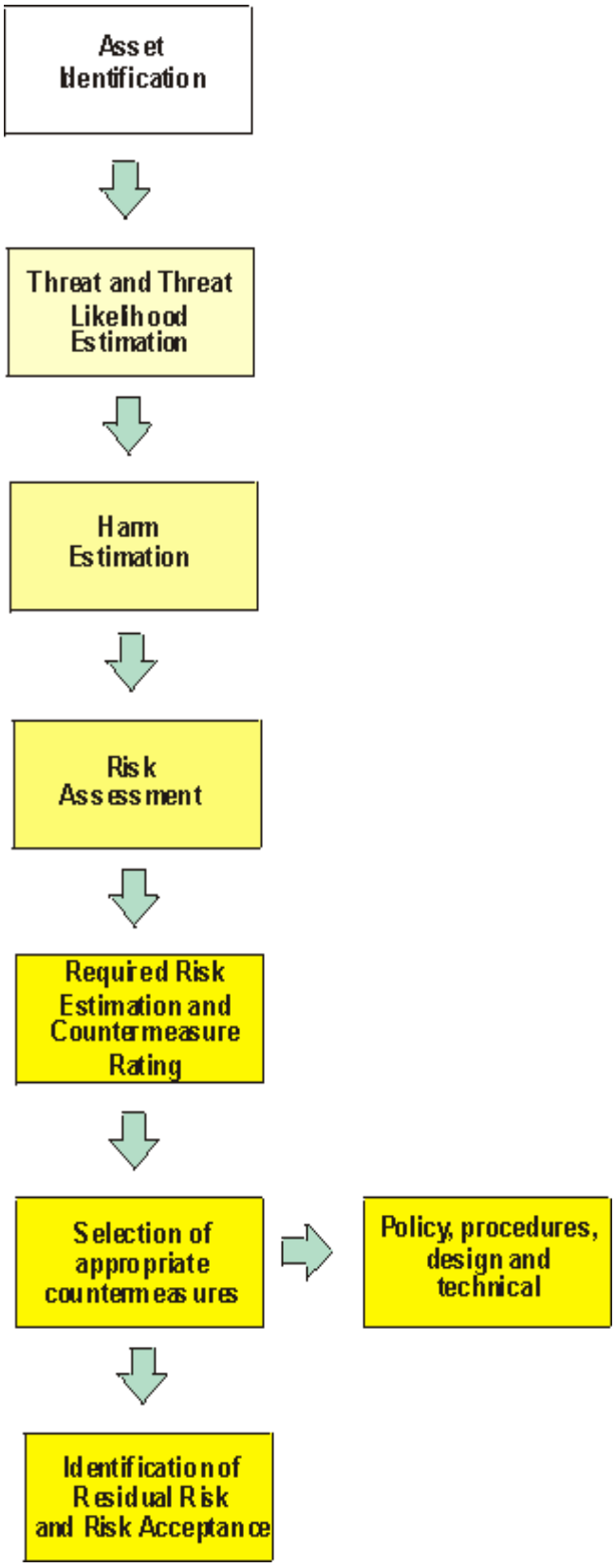

Figure 1.1: Security Risk Assessment Methodology

303. A risk assessment should be undertaken:

a. To determine effective security policy and controls.

b. When new systems or applications are introduced.

c. As part of change control procedures to determine if changes in configuration alter the agreed risk level, introduce new risk factors, and/or to reassess the risk associated with the change.

d. Periodically to ascertain if the risk environment has changed (ie emergence of new threats and vulnerabilities, changes in threat likelihood or changes in the asset value).

304. The level of detail and granularity of the risk assessment will need to be appropriate to the situation. Note that a risk assessment is not a one-off process that is completed and forgotten; it is an iterative process that should be reviewed regularly to take into account changes in the value of assets, the nature of threat, changes in function/service or design which may introduce new vulnerabilities, or changes in the applied countermeasures which may alter the risk level. A risk assessment should have a flow through effect into policy objectives and identification of countermeasures. It is a tool used to balance business objectives and security requirements in order to achieve cost effective security measures.

305. Risk assessment can be applied to a multitude of conceivable assets and processes within any operating environment. However, the aim of the assessment is to limit the scope to the granularity of those asset/threat pairs that are required for providing guidance to the next step, namely the policy development. An example of the level of granularity that would be required is given in the example risk assessment in **Annex A**. The level of granularity is left to those responsible for drafting a risk assessment, who should be mindful of the negative impact of a lengthy, confusing report.

Asset Identification

306. An "asset" can be a tangible item (such as hardware), a grade or level of service, staff, or information. It is important that the key assets for the information system be identified and the assessment encompasses all relevant risks and therefore countermeasures, so that the policy and design development can be undertaken in an informed manner. The assets could be briefly described as "what needs to be protected"; they then need to be attributed a value so that the consequences can be identified at a later stage in the process. It is also essential that the owners/persons responsible for the asset be identified.

307. As a guide to asset identification, the following "asset groups" may be considered:

Confidentiality of Information. This could include all major databases or information storage centres. Secure disposal and backup storage areas should also be included, since these assets could well be subject to an attack against confidentiality of information. Confidentiality of information during transmission may also be considered an asset. Examples of assets associated with confidentiality of information may include: protection of the personnel database, protection of internal emails , sensitive data contained on redundant information media, or sensitive data transmitted via the Internet and other public networks.

Availability of Resources and Services. This relates to those resources and/or services that require a degree of reliability, which has obvious implications on the infrastructure and system(s) configuration. Examples may include reliability of email and web services, reliable customer access to identified information resources, or internal staff access to services such as database access or wordprocessing.

Integrity of Information. Ensuring accuracy of information and the integrity of those processes required for creating or updating information is the third category of information assets that should be considered. The integrity of information may also be considered for transmission of information. Examples may include: integrity of email services, accuracy of customer information database, accuracy of published web information and integrity of information provided by external parties.

Equipment, including Software. This would include those assets related to the effective operation of the systems, including PCs, mainframes, PABX systems, photocopiers and printers. All the smaller office items can also be included in this category. This asset category could also cover software, including software licences.

Staff. This component may be included here, but more commonly forms part of a personnel or physical security risk assessment.

308. It is important that those staff member(s) undertaking the risk assessment determine a suitable level of granularity for the asset identification process. **Annex A** provides some examples of a possible level of asset identification granularity, based on the categories listed above. This could be used as a **guide** in developing a security risk assessment.

Threats and Threat Likelihood Estimation

309. Identifying the nature of individual threats, their source and probability of occurrence is the next step in the risk analysis process. There could be multiple threats associated with one asset, and this should be reflected in the risk assessment process. Threat estimation should include consideration of inherent vulnerabilities. It is counterproductive to detail all conceivable threats associated with an asset (eg there is a threat that the system could be destroyed by a falling building). Only those threats that could reasonably be expected to occur, or those threats, which if realised, will result in identifiable consequences should be considered.

310. Information on the probability of external threats can be derived in quantitative form from police force reports, computer security surveys and bulletins, results of audit analysis or actuarial studies. The likelihood of internal threats may not be so readily ascertained. They can be estimated using previous experience, generic statistical information or a combination of the above. DSD may be consulted for advice on the threat or threat likelihood.

311. Some threats can be increased by inadequate security procedures, introducing a "feedback loop" into the risk assessment equation. For example, if no security countermeasures are provided for building access control, this

weakness may eventually be exploited, and the lack of security controls actually contributes to the increased threat likelihood.

312. The source of the threat may be used in determining its probability (eg the likelihood of an attack by a highly skilled and motivated hacker may be different from that of teenagers using tools downloaded from the Internet). The threat probability is a measure of the likelihood of the threat being realised and the source is a consideration of estimating motive and capabilities. Risk analysis methodologies include determining the threat by qualitative, semi-quantitative or fully quantitative methods. It is important that the most educated, informed estimate be used to provide realistic guidance for the risk assessment. This guide uses a semi-quantitative approach. The scale below in **Table 1** may be used as a basis for categorising the threat probability or likelihood:

Negligible	Unlikely to occur
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

Table 1: Threat Likelihood Rating

Note: These tables are examples only, granularity and probability levels should be adapted to suit the requirements of the organisation/situation.

313. In developing the risk assessment, it is good practice to document or reference the figures derived for the threat likelihood. Details of any research activity undertaken to better estimate the threat likelihood should be clearly referenced in the assessment. This will provide accountability and continuity when reviewing the assessment at a later stage. Previous history on the assessed threat, such as audit trail analysis reports, should also be clearly referenced.

Consequence Estimation

314. The consequence or harm caused to the system services or resources as a result of the loss or compromise of an asset will vary with the nature of the asset. It should be clearly noted that the harm *is not* related to the threat likelihood. For example, the threat likelihood of the loss of a proxy server due to an unstable operating system may be "high", but the harm may be "minor" if the proxy server supporting the service or resource is not viewed by the data owner or

management as critical. Alternatively, the likelihood of accidental misconfiguration of a firewall may be "very low", but its impact or harm could be "serious" to the security integrity of the system. Consequence and threat likelihood are two separate entities, where consequence reflects the value of the asset.

315. **Table 2** is a guide to the consequence definitions that could be used in developing a security risk assessment. The definitions used below may be changed, if necessary. It is important to remember that the critical component is the definition of the terms used to describe the consequences, not the terms themselves.

Insignificant	Will have almost no impact if threat is realised.
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or agencies. Will require some expenditure of resources to repair (eg "political embarrassment").
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. Will require expenditure of significant resources to repair.
Serious	May cause extended system outage, and/or loss of connected customers or business confidence. May result in compromise of large amounts of Government information or services.
Grave	May cause system to be permanently closed, and/or be subsumed by another (secure) environment. May result in complete compromise of Government agencies.

Table 2: Consequence Estimation Rating

316. Even though a threat likelihood may be assessed as "very low", if the harm the threat may cause is "serious" or "grave", then the overall risk can be significant. While the threats to an asset can be quantified or qualified by security specialists, the harm to an asset will always be determined by an executive, asset owner or asset manager. This is a critical factor in conducting a successful risk analysis: clear involvement of the executive or management of the relevant agency(ies).

Risk Assessment

317. Mathematically, risk can be expressed as

threat likelihood x consequence = risk

318. This equation lends itself to production of a statistical or quantitative analysis; it also indicates the two key factors that need to be considered for the analysis of risk. A general semi-quantitative analysis will greatly promote security policy and technical design criteria that focus limited resources on those (relatively) high security risks. The outcome of the risk assessment is an expression of whether the residual risk is acceptable. Security specialists and other managers can use this information to determine the general security countermeasures (if any) that may be required to reduce the risk to an acceptable level, and the order in which they should prioritise those countermeasures.

319. In the absence of a detailed statistical method, the risk assessment example provided in **Annex A** to this Handbook should be interpreted as guidance on those high security risks faced by the security management. In the future, as more detailed statistical data become available, the threat likelihood and therefore the risk assessment should reflect the actual risk more accurately. This could be achieved by conducting sensible auditing of the real-life threats and their likelihoods.

320. Using the definitions of *threat likelihood (***Table 1***)* and *consequence (***Table 2***)* defined earlier in this handbook, the data shown in **Table 3** could be used to produce the resultant risk.

			Consequence			
Threat	**Insignificant**	**Minor**	**Significant**	**Damaging**	**Serious**	**Grave**
Negligible	Nil	Nil	Nil	Nil	Nil	Nil
Very Low	Nil	Low	Low	Low	Medium	Medium
Low	Nil	Low	Medium	Medium	High	High
Medium	Nil	Low	Medium	High	High	Critical
High	Nil	Medium	High	High	Critical	Extreme
Very High	Nil	Medium	High	Critical	Extreme	Extreme
Extreme	Nil	Medium	High	Critical	Extreme	Extreme

Table 3: Resultant Risk

321. **Table 3** shows the risk mapping, using the threat likelihood and the consequence ratings. The outcome is the resultant risk, which provides a grading as to the expected risk *without* any applied countermeasures. The final step in the risk assessment process uses this information to provide guidance to the

policy and design development staff on which countermeasures should be prioritised. Note: the measures in Tables 1, 2 and 3 can be adapted to reflect the level of required granularity.

Required Risk and Countermeasure Rating

322. The required risk should be the desired "risk level", as set by the management authority of the system. One method that could be used to derive the required risk makes use of the following statement:

> ***"The Required Risk is the risk level that management are prepared to accept."***

This is best illustrated using the example Risk Assessment table in **AnnexA**.

> **Row 3** in the table details two threats to the same asset. The first threat (IP Denial of Service) states that the threat likelihood is "Extreme", which is defined in **Table 1** to mean that it may happen a number of times per day, and the harm is "Damaging" as per **Table2**.
> Using **Table 3**, the resultant risk is therefore "Critical". However, management requires that the threat likelihood be mitigated so that it should only occur once every two/three years or less (threat likelihood = very low).
> Again, using the mapping in **Table 3**, the "Required Risk" (**Column6**) then becomes "Low".

Another example.

> **Row 4** (Accuracy of Customer Information Database (CID) produces a resultant risk (**Column 5**) of High.
> Management has decided that this level of risk be mitigated to Nil (**Column 6**), and will therefore require countermeasures to be developed so that firewall access rules are *unlikely* to be inadvertently changed.

323. The next step in the assessment is the countermeasure priority rating. The countermeasure rating is the difference between the required risk and the resultant risk, and is used to provide guidance as to the importance that should be placed on broad security countermeasures. The following table is used to calculate the countermeasure rating (as shown in **Column 7** in the example):

Countermeasure Priority Rating:

Nil	0
Low	1
Medium	2
High	3
Critical	4
Extreme	5

324. **Column 7** in the example is simply the difference between the resultant risk and the required risk (**Columns 6 and 5** in the example) expressed as a number. This result is the Countermeasure Priority Rating, which is a critical outcome of the risk assessment process.

325. The priority of the countermeasures should be reflected in the security policy and planning documents. These may relate to:

a. addition of security measures;

b. reduction of security measures;

c. risk avoidance through change of service and system specifications;

d. acceptance of residual risk; and

e. minimisation of harm through response mechanisms.

326. The final step in the process is to broadly identify existing countermeasures. The results of the risk assessment should be used to test the appropriateness of these measures and identify requirements for new countermeasures. These requirements should be reflected in security policy and planning documents. A subsequent assessment of the residual risk following the application of identified countermeasures forms the basis of management decision making and endorsement.