

**Important notice:**

You are not authorised to use this procedure or any other material we provide until we have received payment from you. To do so would be a breach of copyright. Corporate Potential Pty Ltd, trading as Compact – Compliance & Corporate Training as at December 2007, owns copyright in the enclosed material. Once payment has been received, you cannot copy or distribute the documentation in any way other than for the use of your AFS licensee business. If you decide not to use the procedures, you must destroy them and any copies made within 48 hours of receiving this email.

Please be aware that the Pro Forma documentation we provide will not guarantee that the licensee will meet all of its obligations under the law. It needs to be tailored by the licensee to reflect its business practices and processes. There are also a myriad of other factors which may result in the license breaching its legal obligations.

**This procedure is normally 7 pages long. We've only provided 3.5 pages in this example.**

This procedure was last reviewed on:     /     /

## 1 Risk management

### 1.1 Responsibility

This procedure is reviewed every year by [name of internal person]. If there is a major compliance breach in this area, [name of external auditor] is engaged to review the procedure.

The risk management assessment is conducted by

- [insert name and position title of each person].
- 

It is undertaken every 12 months, or sooner if new risks are identified.

### 1.2 Overview

This procedure has been developed with reference to Australian Standard AS/NZS 4360:2004. Please refer to that document for more information on risk management systems.

This procedure is a dynamic (ie ever-changing) procedure that includes instructions as to how the responsible person(s) can conduct a risk management assessment of the business. Regulatory and operational risks should be considered.

### 1.3 Identifying new risks

In the Risk Register (see 11.6 below), there are some common risks which face many businesses, most of which are risks of *non-compliance* identified by ASIC. The list does not cover everything. The licensee has an ongoing obligation to update and add risks to the risk register.

## maintains the risk register, covering all the risks which face it.

To identify further risks, first, think of the organisation's goals and objectives. For example, one goal is to comply with obligations under its financial services licence. This is called "identifying the context". Second, think of threats to these goals. As inspiration, use:

- experience;
- records;
- systems analysis;
- industry consultation; and
- audit and other recommendations.

Each time you consider *what* can happen, also consider *how* it can happen. This is called “identifying the risk”.

## 1.4 Process

To assess and plan for these risks, follow the process below. Consider one risk at a time. **While you are doing steps 1 to 3, imagine you have *no* measures in place to control the risk.** As you complete each step, enter your results into the Risk Register, at 11.6 below.

### 1.4.1 Step 1: determine the likelihood of the risk occurring

Use this table and record your result (a letter from A to E) in the ‘Likelihood’ column in the Risk Register.

Level	Descriptor	Description
A	ALMOST CERTAIN	Is expected to occur in most circumstances
B	LIKELY	Will probably occur in most circumstances
C	POSSIBLE	Should occur at some time
D	UNLIKELY	Could occur at some time
E	RARE	May occur only in exceptional circumstances

(Remember, how likely is it that the risk will occur in the absence of any controls?)

### 1.4.2 Step 2: Determine the consequences of the risk occurring.

Use this table and record your result (a number from 1 to 5) in the ‘Consequences’ column of the Risk Register.

Level	Consequence Description	Detail description (Guide only – tailor to suit your business)
1	INSIGNIFICANT	No regulatory impact, no client or staff impact, no financial loss, no impact on targets
2	MINOR	No regulatory impact, low client impact, financial loss up to \$5k, no effect on operations, up to 1% impact on targets
3	MODERATE	Regulatory impact, medium client and staff impact, financial loss up to \$50k, some effect on operations, up to 5% impact on targets
4	MAJOR	High regulatory impact – enforcement action by regulator, medium client and staff impact, potential for legal action, financial loss up to \$100k, major effect on operations, up to 10% impact on targets

5	EXTREME	High regulatory impact – loss of licence, high client impact, financial loss in excess of \$1m, major effect on operations and on-going viability, greater than 10% impact on targets, adverse media attention, continuation of business jeopardised
---	---------	--

### 1.4.3 Step 3: Determine the rating for the ‘Inherent risk’.

Use the ratings you have found for likelihood and consequences to find an ‘Inherent risk rating’ on this table. This rating tells you how big the risk is regardless of any measures you have to control it.

		Consequences				
		Ratings	1	2	3	4
Likelihood	A	S	H	H	H	H
	B	S	S	H	H	H
	C	M	M	S	S	H
	D	L	L	M	S	S
	E	L	L	L	M	S

H = High      S = Significant    M = Medium      L = Low

Write the rating in the ‘Rating’ column in the Risk Register.

### 1.4.4 Step 4: Identify existing controls already in place

Now, identify the controls you have in place to reduce the likelihood and effects of the risk. For example: in relation to risk number 1 you might have a contingency plan for the sudden departure of a key person. Describe these controls in the ‘Existing controls’ column of the Risk Register. If there is not enough space, attach further pages.

### 1.4.5 Step 5: Rate your controls – how good are they?

Rate your controls using the following table. Write the rating (a number from 1 to 4) in the ‘Existing controls rating’ column of the Risk Register.

Level	Descriptor	Description
4	EXCELLENT	System is effective in reducing risk, responsibility clear, well documented, regularly reviewed
3	GOOD	Systems and documentation in place but room for improvement
2	FAIR	Some controls in place but incomplete
1	POOR/ UNSATISFACTORY	Ad hoc and poorly documented processes, or no controls at all

[procedure truncated]