

## Compliance Committees

Naturally, you don't want your car's dashboard feeding you skewed data – particularly if it makes you break the road rules. In the same way, an Australian Financial Services (AFS) or Australian Credit (AC) licensee needs a reliable kind of “dashboard”. This can help it abide by its own road rules – that is, the disclosure and conduct obligations set out in the *Corporations Act 2001* for AFS licensees, and the *National Consumer Credit Protection Act 2009* for AC licensees. As a Responsible Manager or compliance manager, you need the right dashboard so that you can stay out of court and out of the hands of the regulator. That dashboard is typically referred to as a compliance committee.

## The Compliance Committee

You may have heard the phrase “a committee is a cul-de-sac down which good ideas are lured and then quietly strangled to death.”<sup>1</sup> That's not the kind of committee I'm writing about. A compliance committee should help you navigate your legal obligations by empowering your decision makers with the right information. That information needs to be tied closely to your key legal obligations as a regulated licensee. To provide an example, here are the top ten conduct obligations imposed on an Australian Financial Services licensee, extracted from section 912A of the *Corporations Act 2001*. There is a lot of overlap between these obligations and those imposed on an AC Licensee (albeit under different law).

## The 10 Commandments

Your primary obligations that are set out in section 912A of the *Corporations Act 2001* are kind of like commandments. Thou Shalt:

1. Do all things necessary to ensure that your financial services are provided efficiently, honestly and fairly. (The Courts have said that “a licensee performs [its] duties efficiently if [it] is adequate in performance, produces the desired effect, is capable, competent and adequate.”<sup>2</sup>)
2. Have adequate arrangements to manage conflicts of interest. (This doesn't just mean disclose them, but also control them or avoid them, as the situation requires.)
3. Comply with your AFSL conditions. (Did you know that there is an obligation in your AFSL to maintain a three-month cashflow projection *at all times*? There are lots of other juicy requirements in there that some licensees don't know about.)
4. Comply with the financial services laws. (This includes SIS legislation, most of the *Corporations Act 2001* and the *ASIC Act 2001*.)
5. Take reasonable steps to ensure that your representatives comply with the financial services laws. (This goes beyond the annual audit. You need monitoring and supervision systems that give you accurate, timely information. For example,

---

<sup>1</sup> Attributed by various websites to Barnett Cock.

<sup>2</sup> *Story v NCSC* (1988) ACLR 225 at 236.

you might review the advice provided by an adviser to a client that generated the top commission in your dealer group, on a monthly basis, to ensure that your representatives are not churning, and that they have a reasonable basis for advice which is generating high commissions.)

6. Have available adequate IT, HR and financial resources to provide your financial services and carry out supervisory arrangements. (Is your compliance team big enough? Are you meeting your minimum cash requirements? Have you tested your IT disaster recovery plan – ever?)
7. Maintain the competence to provide your financial services. (This means you need to have the right Responsible Managers and staff that know their stuff, have the right experience and keep their skills and training up to date.)
8. Ensure your representatives are adequately trained and competent to provide the financial services. (Sure – you have a training register and training plan. But have you ever benchmark tested or blind tested your advisers to see how effective your training is?)
9. Have adequate dispute resolution mechanisms when dealing with retail clients. (This means having internal resolution procedures and not just being a member of an EDR like the Financial Ombudsman Service).
10. Have adequate risk management systems. (A senior ASIC director once told me that the risk register was the first thing she asked to look at when visiting a licensee's premises, because the controls described in the register should act as a road map, describing various procedures and pointing the ASIC staffer to all the licensee's other processes.)

### **Good compliance culture = good compliance committee**

So, you have these obligations, and a stack of others too, including the obligation to report a breach of any of the “Ten Commandments” if it is significant. (You also need to be on top of other obligations relating to anti-money laundering, consumer credit, privacy, tax, trade practices and more). How does your business handle your obligations? This is determined by your corporate culture. Section 12.3 of the *Criminal Code Act 1995 (Cth)* says that if a company is criminally prosecuted, the evidence of a “guilty mind” can be established by looking at whether you had a corporate culture that “directed, encouraged, tolerated or led to non-compliance” with the law. That’s right – a company can’t go to jail itself, but it can be criminally prosecuted.

How does your business handle non-compliance? Justice Neville Owen conducted a Royal Commission into Australia’s biggest corporate collapse – that of insurance giant HIH. In his executive summary published in 2003, Justice Owen said: “...*the corporate officers, auditors and regulators of HIH failed to see, remedy or report what should have been obvious. And some of those who were in or close to the management of the group ignored or, worse, concealed the true state of the group’s steadily deteriorating financial position.*” He then asked a crucial question, one which is equally applicable to you, in your business: “*I found myself asking rhetorically: did anyone stand back and ask themselves the simple question—is this right?*” The founder of HIH Insurance, Ray Williams, went to jail for three years as a result of ASIC prosecution.

This is an extreme example. A more common situation is where a group of decision-makers sit in a room – often as a compliance committee – and talk about a “breach” that’s been identified. For some reason, time after time, the committee determines that the breach identified is not significant within the meaning of section 912D of the *Corporations Act 2001*, and so does not need to be reported to ASIC. (As you know, a significant breach must be reported by AFS licensees to ASIC pursuant to section 912D of the *Corporations Act 2001*.) There are Enforceable Undertakings between ASIC and some of the Australian banks in which ASIC has specifically criticised this reluctance to report breaches.

So, your culture will determine how well you (1) understand, and (2) comply with your obligations, which includes the Ten Commandments.

Just as a car’s dashboard relays important data to the driver, the compliance committee should do a number of things:

1. **Show that the key obligations are being followed.** Key obligations (like the Ten Commandments) should be separate standing items on your compliance committee agenda. Table your Breach, Complaints, Conflicts of Interest, Risk and Training Registers at each meeting to prove that your systems are alive and well. For example, when you get to the heading “Risk Management”, ask questions like: Are there any new risks we need to review, analyse or control in light of our recent business decisions, or changes to our internal or external environment? Is our Risk Management procedure actually working? Let’s have a look at our Breach Register to see when it was last updated...”
2. **Report on breaches.** A failure to discuss and action breaches is a clear indicator of a poor corporate culture. If your compliance committee is not addressing breaches, then your licensee may be being fed incorrect information – you’re speeding without even knowing it. For example, show how external licensee audits, adviser audits and random internal audits are identifying breaches, and how the compliance team is remedying them. Hold the follow-up people accountable to deliver, via your compliance committee.
3. **Communicate compliance issues and business risks to the right people.** The “right people” include Responsible Managers who are directly responsible for significant day-to-day business decisions about the ongoing provision of financial services by the licensee (ASIC RG 105.5). I once conducted a licensee review for a large dealer group and spoke to the Responsible Manager. He wasn’t sure whether the licensee operated a compliance committee (or equivalent), and certainly didn’t receive any minutes. That needed to change.
4. **Include one or more external members** who understand the regulatory environment, and principles of good governance. This has a number of advantages. The external member:
  - a. can test reports and statements, and mine discussions for issues that may otherwise go uncovered;
  - b. may be able to share broad industry information about how other licensees are adapting to changes to the law;

- c. will not have the same commercial restraints in acknowledging that a mistake has been made, because they're not employed by the licensee; and
- d. are likely to be less susceptible to a company's internal culture which may be reluctant to discuss certain breaches.

Interestingly, many of these functions are required by law for Responsible Entities of managed funds who have retail investors. Independent compliance committee members, obligations to report breaches to the Board and to ASIC, and obligations to consider certain issues on an ongoing basis are all mandated by statute. This is because the idea of a compliance committee, when it works properly, is a benchmark of good governance.

A truthful, well structured compliance committee is your ultimate dashboard, because it helps manage two risks:

1. **Regulatory Risk:** I can think of two examples in the past 12 months when I have been involved in discussing and then implementing a new process, or addressing an existing risk in a compliance committee. On each occasion, by chance, ASIC has then conducted a surveillance of the licensee on the very issue discussed or risk identified. In those instances, ASIC did not take any further action, or require the licensee to take any further steps. It was clear to ASIC from the compliance committee meeting minutes and supporting documents that both licensees took their compliance obligations seriously and deal with them proactively.
2. **Operational Risk:** For licensees that deal with retail clients, it's often a client complaint that is the biggest risk to their business (as opposed to regulatory risk). A rigorous, ongoing assessment of monitoring and supervision processes at a compliance committee level is a strong control in minimising this kind of risk too.

I've spent most of my time since 2002 (when FSR was introduced) dealing with a broad range of Australian Financial Services licensees. Without fail, the healthiest corporate cultures have always sported a bright, shiny compliance committee. So, if you don't have a compliance committee, or if you don't think it's providing you with a clear dashboard of information, what are you going to do about it?

Author: [Paul Derham](#)

9 March 2011

The law is current as at March 2011.



**HOLLEY NETHERCOTE**  
commercial & financial services lawyers

Please note that this paper is a summary of the law only and is not a substitute for legal advice. *Holley Nethercote* is able to assist companies in meeting their obligations in this area by providing practical and prompt legal advice.

Training and creation of compliance programs are also available via an associated business, [Compact - Compliance & Training](#).

We invite you to contact *Holley Nethercote*:

Tel +613 9670 8200  
Fax +613 9670 5499

Email [law@hnlaw.com.au](mailto:law@hnlaw.com.au)  
Web [www.hnlaw.com.au](http://www.hnlaw.com.au)