HOLLEY NETHERCOTE
commercial & financial services lawyers

How to score an A+ at your next licensee compliance audit

When did you sit your last exam? Remember the mixed feelings of anticipation and dread? You probably recall the feeling more vividly than the subject matter. Memories like that are not stored in the same part of your brain as birthday parties and pony rides. Instead, they're jammed together with other repressed memories that you'd rather forget about.

Now, think back to when you last blitzed an exam. Recall that feeling of elation, relief and joy? That's the feeling you'll get if you work through this article and make required changes *before* your business is subject to an external Australian Financial Services (AFSL) compliance audit.

This article is a new edition of an article we wrote for Money Management in 2006. Since then, we've conducted an extensive Jim Collins-style research project on a sample of 47 licensee reviews conducted by our lawyers, looking for common themes and learning points. We've also been appointed external experts on some enforceable undertakings and imposed AFSL conditions.

Firstly, what is a compliance audit?

The person conducting the audit refers to it as a "review" because it sounds nicer. The subject of the review, however, refer to it as an "audit". Regardless, a compliance audit for our purposes occurs when external compliance consultants visit your business and assess it against the requirements of the financial services laws, your AFSL conditions, ASIC guidance and best practice. Then they provide you with a report. If the audit is the result of a special licence condition on your licence, or enforceable undertaking, the consultant will look at other matters, as dictated by ASIC, and will provide the reports to you and ASIC.

When you first applied for your licence, you probably told ASIC that you would have an annual compliance audit. There's no law that says you have to do it,[1] but your undertaking to ASIC during the application process arguably imposes an obligation on the licensee to have it done annually, at least for the first year or two. As time goes on, this may change.

How does it compare to a Registered Auditor's review?

Annual financial audits by ASIC-registered auditors are compulsory for all AFSL holders, unless they hold a limited AFSL and don't touch client money. Some licensees wholly rely on the financial audit and don't separately engage an external compliance auditor.

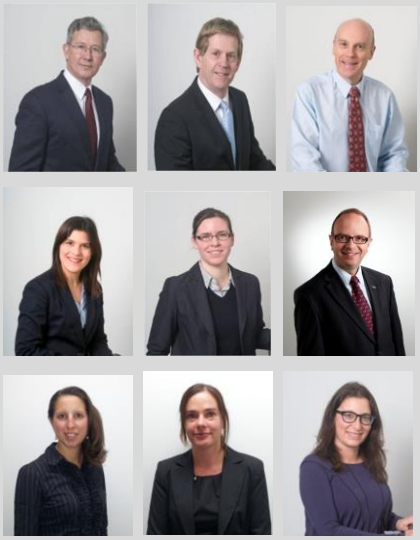
[1] That said, there *is* a law that requires licensees to monitor and supervise their representatives, and Responsible Entities of managed investment schemes do require an annual compliance plan audit.

This article was originally published in Money Management in 2005. It has been updated so it is relevant as at September 2013.

About the Author: Paul Derham

Paul's expertise is in commercial and financial service law. Since 2001, Paul has assisted participants in the financial services industry in complying with their legal and compliance obligations, both under the pre and post-Financial Services Reform regime. Paul regularly assists businesses in acquiring their Australian Financial Services licences, as well as providing ongoing compliance with their legal obligations. He is also involved in AFSL-related litigation and general commercial law-related matters.

Other members of our financial services team



Each year, you must lodge your profit and loss statement and balance sheet with ASIC, along with an Auditor's report. When conducting the audit and providing their report in FS71, the auditors need to:

- Include their opinion on the effectiveness of your internal controls used to comply with certain parts of the Act (dealing with client money and property, handling insurance payments, keeping records, lodging documents, appointing auditors and other conduct requirements).

- Report to ASIC within 7 days if they become aware of a contravention of a condition of your AFSL (or a number of other provisions). Your AFSL requires you to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that you comply with the provisions of the financial services laws. There is no significance test attached to this obligation – they need to report even the most technical breach.

- Report to ASIC within 28 days after becoming aware of circumstances such that they have reasonable grounds to suspect a contravention of the Corporations Act 2001 (the Act). A significance test applies. ASIC gives guidance to auditors about what it considers as "significant" in RG 34, and uses a civil penalty provision as an example (eg. if an auditor becomes aware of your failure to comply with FoFA's conflicted remuneration provisions, it would need to report this to ASIC).

- Make certain "reasonable assurance" statements (eg. "in our opinion, the internal control is effective…") and make certain "limited assurance" statements (eg. "nothing has come to our attention that causes us to believe that internal control is not effective").

The Guidance Statement GS003 sets out that financial auditors should look at a number of documents, and determine whether you as licensee are meeting your obligations. It goes on to discuss what we call the "10 commandments" found in section 912A of the Act. In our experience, auditors tend to focus on the financial obligations imposed on the licensee, and will spend some time checking over breach, risk and complaints registers. They'll also cast their eye over your compliance manual.

In contrast, the advantages of an external legal review are:

- There's no legal obligation on the reviewer to report any identified breaches to ASIC, unless the review is mandated by ASIC through imposed licence conditions or an enforceable undertaking. The reviewer can often help you resolve the issues after compiling the report.

- If the reviewer is a law firm, it's likely that client privilege will protect the report (except in the case of ASIC-mandated reviews).

- Good external legal reviewers don't look at your financial position, but will consider your overall compliance framework, and test whether it is actually working in practice. This involves going to the next "layer" of detail, when considering your documentation, and then systematically testing it by talking to relevant staff, including advisers. Importantly, it should include considering client-facing documents such as FSGs and SOA templates.

It's also worth noting that nearly every licensee dealer group that's entered into an enforceable undertaking with ASIC has been subject to an annual financial audit. We know of one large dealer group that, before being subject to an Enforceable Undertaking (EU), had *never* had an external compliance audit conducted, and relied wholly on registered auditor reviews. Of course, your overall compliance culture is your best line of defence against entering into an EU, and a strong record of external review is just one indicator of that.

So here are our conclusions. Take heed of what follows!

1. Consider your compliance culture

Did you know that "Culture" is defined in the Commonwealth Criminal Code? It's also referred to extensively by the Courts and ASIC. Culture is the link between procedural compliance and behavioural compliance. If behaviour is non-compliant, even the slickest compliance framework is going to fall over. It is easy to pick up quickly on an organisation's compliance culture. Poor compliance culture indicators that we commonly come across are:

- Inadequate compliance resources.
- Lack of ASIC-reported breaches on the breach register.
- Missing procedures, or procedures that haven't been updated in the last 12 months.
- Poor understanding of key obligations by client-facing staff.
- High compliance staff turnover.
- Compliance staff not being involved in the decision-making process from the start.

In contrast, healthy cultures demonstrate characteristics like:

- Genuine buy-in from senior management. This is easy to see – do they devote their *time* to compliance matters? We had one dealer group client whose CEO sat in on every Responsible Manager training session we ran for their team and AFS licensee network, annually for four years! He also chaired the compliance committee.
- An appropriately skilled and resourced compliance team.
- A compliance manager that gets invited to key decision-making meetings, before the decisions are being made.
- A compliance manager with direct access to the top levels of management.
- A compliance committee that reviews the 5 key registers (risks, conflicts, training, breaches, complaints) on an ongoing basis.
- Up-to-date procedures that reflect actual practice.

Changing your compliance culture requires buy-in, identification of barriers to improvement, the formulation of strategies to continually strive for improvement, and the allocation of sufficient resources.

Our licensee reviews consider around 19 different topics (Compliance Arrangements, Responsible Managers, Breach Reporting, etc). By far the most recommendations (173) were under the Compliance Arrangements heading. Common recommendations related to:

- Consolidating and updating existing compliance procedures.
- Ensuring adequate staff to get the job done.
- Separating roles to ensure proper reporting lines.
- Strengthening the compliance committee by changing its makeup, function or standing agenda items.

2. Keep up-to-date records if you advise retail clients

Do you know what your AFSL says about record keeping? It says you need to keep records of every version Financial Services Guide (FSG), every Statement of Advice (SoA), as well as certain information that supports your SoA, for at least 7 years. It's not enough that you have an agreement with your authorised representatives to access their documents. It's established best practice for licensees to keep their own (usually electronic) copies of such documents. You need to be able to show your auditor how you do that.

Over the years, some licensees have been unable to show how different versions and copies of documents are retained for the required period. This is changing and it is now more common that registers are fairly well maintained, based on the reviews that we've conducted.

3. Have a "living" risk management system.

Award winning author Arie de Geus wrote a book "The Living Company" which chronicled his findings after researching 27 companies that ranged in age from 100 to 700 years old. What do you think was one of his key observations amongst those companies? Meticulous, systemic risk management.

It comes as no surprise that the Act and your licence conditions both require you to have a risk management system, unless you're APRA regulated, in which case you'll have one under a different set of laws anyway. It should conform to the relevant standard (ISO 31000:2009 is the most recent, at the time of writing), and it needs to be updated on an ongoing basis. The managers and owners of your business are intuitively thinking about risk, so it shouldn't be difficult to capture those thoughts in a disciplined, methodical manner, as part of your ongoing compliance framework. Risk management analysis also benefits from involving "ground level" staff in the process – not just senior management.

We made 86 related recommendations in the reports we analysed, and we observed that in many instances, systems were out of date, improperly completed, poorly integrated with Board or holding company risk frameworks, or simply misunderstood. In the most part, most risk management systems we reviewed did not comply with the ISO standard.

4. Show how your responsible managers are maintaining competence

You should have a written, forward looking training plan and an up-to-date training register that shows that your responsible managers receive ongoing training. The responsible managers should collectively oversee all the financial services and financial products named on your AFSL, and their training should reflect this. A responsible manager training plan should also show ongoing regulatory training. This might be seminars, courses and monthly regulatory updates. If you've got a Key Person condition on your licence, you should also consider training up a successor who can step in if the Key Person leaves the business.

Bigger licensees tended to have more recommendations on this topic than smaller licensees. Of the 112 recommendations made in the sample reviews, the main topics related to inadequate training or understanding of key regulatory matters, succession planning, and ensuring that there were adequate responsible managers. Another interesting challenge faced by lots of businesses was maintaining "competence" in financial products that the business was not currently offering.

5. Keep a tight leash on your outsourced providers

Show how you select and monitor your outsourced providers. They can cause you to breach your licence. For example, it's your fault if your auditors don't submit your financial reports to ASIC within 2, 3 or 4 months of the end of your financial year (this depends on what type of entity the licensee is). You should be monitoring them with KPIs, and have recourse if they cause you to breach your licence. Your outsourcing procedure should show who you outsource to, and how you monitor them.

Common issues we have identified in this area are a lack of legal review of key clauses in business-critical IT contracts, lack of ongoing monitoring, and lack of a formal review or appointment process.

6. Have a breach reporting procedure that works

If you've been operating your AFSL for some time, an empty breach register is a clear sign that something is wrong. The complexities of this regime dictate that your business will breach its licence at some time, if not often. A breach could be forgetting to provide an FSG. It could be failing to tell ASIC that you changed your registered address within 10 business days.

All staff should be trained on what constitutes a breach. If a breach is significant, then it should be reported to ASIC within 10 business days of it being identified.

Every process needs to comprehensively cover identification (do your staff know what a breach or incident is?), classification (is it a breach of the financial services laws?) and action (what are we going to do about it?). Over the years, we have found that licensees have become good at recording breaches. However, larger licensees often struggle with documenting all the breaches they pick up from adviser reviews, and appropriately remediating them.

7. Have a robust complaints handling process for retail clients

Complaints handling and breach reporting are reactive processes. For these processes to work effectively, it is important to know when to react. This means that staff need to be trained on what is a complaint (example: is it a complaint or a query?), and how to escalate complaints. Also, there needs to be a robust framework in place to identify breaches, escalate as appropriate and report within the required timeframe.

We found that a common problem is that client-facing staff do not understand what constitutes a "complaint", and the internal process is often not followed properly. We often recommend that policies be updated and refresher training be rolled out.

8. Sign off your promo material

Does your website and advertising include the warnings required by law? We have found this to be a common oversight by licensees. You should have a documented process for signing off promotional material. For example, anything containing general advice to retail clients should be signed off by an RG 146-compliant person.

In our experience, websites often include words like "independent", "impartial" and "unbiased" which are restricted for most licensees who receive commission payments. When was the last time you did a search? Try typing "independent site:[your web address]" into Google and see what happens.

9. Follow your recruitment process

In September 2011, ASIC released a report (Report 251) that summarised its findings from surveying the 20 largest licensees that provide financial product advice to retail clients. You may recall that ASIC asked the licensees a huge list of questions which caused a bit of a stir at the time in terms of the resources required to answer them. ASIC then released another report, Report 362, in July 2013, following responses from the second phase of questions targeted at the top 21-50 licensees. Both reports should be compulsory reading for anyone wanting to achieve an A+ in their next licensee review. Both reports also make comment about ASIC's concern that a poor appointment process may result in you taking on a "bad apple" adviser, which may in turn cause you a world of grief. ASIC has also released a guide called HB 322-2007 Reference Checking in the Financial Services Industry, in conjunction with Standards Australia. It includes loads of useful checklists and procedures that you can implement straight into your business.

We often tell licensees that it's not enough to rely on your external recruiter conducting the reference checks – you should have records on file that also show full RG 146 qualifications (including a skills module), as well as ongoing high-level monitoring of initial advice for an initial period. Other observations we made related to inconsistencies in employment contracts, and a lack of discipline in following the appointment protocol (this was often tied to rapid business growth or a lack of resources in HR).

10. Your monitoring and supervision framework should be risk-based and fully resourced.

Are your reviewers ensuring that personal advice to retail clients meets the Best Interest obligations? No doubt you have just updated your monitoring and supervision framework to take into account FoFA in all its glory.

Monitoring and supervision is more than just an annual review. In our experience, it includes peer review, new adviser-file reviews, "anti-fraud audits", interactive training, "circular folders" that include the week's advice documents, and mentoring

systems. ASIC noted in Report 362 that the average number of advisers for each file reviewer was 53. In our view, that ratio can be higher and still successful if there are good compliance systems that are asking the *right questions* and addressing them.

11. Have an IT resources procedure

Your procedures should make sure the business maintains adequate IT resources. You also need a backup procedure and disaster recovery plan. In our experience, the biggest failure in this area is the lack of *testing* that takes place. Many licensees don't really truly test their IT backup plans. We've seen reports of IT systems tests that took *three attempts* before they successfully allowed the business to continue operating off-site. Have you made even one attempt? In an effort to be true to our word, we commissioned a test of our law firm backup processes. We discovered that they were completely inadequate, and put in place simple steps to address those shortfalls.

In addition to testing their own backup processes, dealer groups should be seeing evidence of tests being done by their software providers. This is particularly relevant to advisers given that most advice is stored in the cloud by third-party software vendors.

12. Keep your compensation arrangements updated

If you're required to have PI insurance, then make sure you get legal signoff if you renew your policy but change the terms. Alternatively, you can ask your broker to answer the following question, in writing: Can you please confirm that our PI policy complies with the requirements of RG 126 and, can you please explain any conditions or exceptions to your answer? The worst answer we've seen from a broker is "yes, the policy complies with RG 126, subject to the terms of the policy." That answer is useless.

13. Check your disclosure documents

This area is commonly less than perfect. We routinely find that FSGs do not comply with the various legal requirements. Also, SoA templates are often too long and complicated. Who conducted your last SoA review? Sometimes an SoA is prepared by someone who has so much time invested in it, they will be reluctant to hack it into one third the size, which is exactly what it may need. Try getting an external party to have a go at simplifying your advice document.

14. Update your research process

If you service retail clients, and research your products, then you need to have a procedure that sets out why you've chosen the products you have, and how advisers can deal with non-approved products. ASIC and the tribunals and Courts have made it clear that adopting someone else's rating system, per se, is not good enough. Make sure your procedure is followed, and that it explains what a representative must do if he or she wants to recommend a product not on the list. With the onset of FoFA, a big challenge for licensees with related party products on their list is showing that the related party product will result in the client being "better off" by switching to it. How does your business address this issue?

15. Use your conflicts of interest register

When the requirement to have a conflicts of interest procedure and register came into force in 2005, most people scratched something together and put it in their compliance manual. But, does it actually contain identified conflicts? Does it show that conflicts are being managed? If you're stumped for any conflicts, ASIC released a discussion paper in April 2006, which is packed full of examples. Also, the introduction of "conflicted remuneration" under FoFA should result in you updating your conflicts of interest procedures. It is no longer enough to manage some conflicts by "disclosing" them – they must simply be avoided. That said, disclosure is generally done quite well.

We made 74 recommendations in our sample reviews, and they related to updating conflicts registers, better managing related party products, capturing meaningful disclaimers from advisers who may have relationships

with external parties, and training staff on what actually constitutes a conflict. In our view, with the onset of FoFA, this is one of most topical issues facing the industry.

16. Be prepared for changes

A good compliance audit will invariably suggest changes. Amongst other things, a compliance audit stocktakes and reviews your compliance framework as a whole and assesses whether the framework is really addressing the key issues and risks. We find that new compliance managers who commission a review are open to the recommendations. Entrenched compliance managers will, understandably, tend to defend their programs.

According to ASIC's Enforceable Undertaking with City Index Australia Pty Ltd, entered into on 8 April 2013, City Index took 11 months to fully implement certain recommendations. We suggest that you devote as many resources as you need to have a speedy implementation in a shorter timeframe!

As you can see, preparing for a compliance audit is not a walk in the park. But, if you are constantly working on developing a positive culture of compliance, it won't be impossible. Think of compliance audits as a tool for positive change and a roadmap for navigating through the numerous regulatory obligations faced by licensees. You don't know what you don't know. Accordingly, any breaches, findings and recommendations in the report will ultimately make your business a better business, if you act on them in the right way, quickly.

Author: Paul Derham

The law is current as at September 2013.

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
Web www.hnlaw.com.au