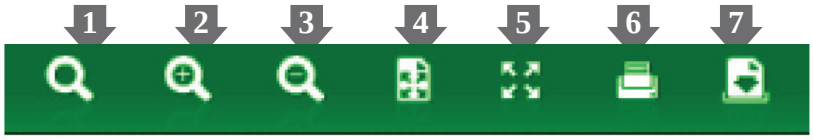
ASSOCIATED COMPLIANCE

FOR A COMMON PURPOSE

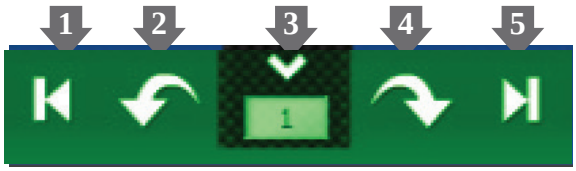
April 2017 Edition

Instructions

All the text in red are links. Click on that text to go to the relevant page.



Click on one of the above in the top menu (numbered arrow pointing to the icon):
1 = Zoom-in
2 = Zoom-out
3 = View actual size
4 = Fit to page
5 = View full screen
6 = Print
7 = Download newsletter



Click on one of the above in the bottom menu (numbered arrow pointing to the icon):
1 = Go back to cover page
2 = Go back a page
3 = Insert page number to go to the specific page
4 = Go forward a page
5 = Skip to the last page

Alternatively, click and drag on any corner of the pages with your mouse cursor to turn over the pages (just like you would do if you were reading a printed magazine).

Contents

- Click on text to navigate to the page -

FROM AC

We attended the FSB Conference in March and thought that the following points would be relevant to our readers. Understandably, the FSB has some issues which are delaying the release of comments and slowing down the approval through Parliament and its committees.

Market Conduct - Caroline da Silva

Caroline said that the first draft of the Conduct of Financial Institutions Bill will be released this year. It will include all 13 laws currently governed by the FSB and will be written on a functional basis - the FSCA will be organisationally structured the same way. “Function” pertains to Regulator activities such as Registration, Enforcement, Compliance, Supervision and the like.

Also, despite the Financial Sector Regulation Bill not being passed into law, the FSB may start to ask for complaints reports. This is in line with their obligation to manage the TCF outcomes.

Fit and Proper - Loraine van Deventer

The FSB said that it would release its response to comments on the Fit and Proper soon. We are assuming that the planned date has passed, as the plan was to release the final amended Fit and Proper Regulations at the end of April. We will keep you informed of developments.

Commenting on the Tier 1 and 2 product lists, it appears that they are not being viewed as exhaustive. We note though that this will allow the FSB to include whole industry segments simply by amending the list.

The presentation gave some explanation on ‘good standing’ which we are struggling with, despite the FSB’s insistence that it is common knowledge. The explanation was that “a person or company must become and remain compliant with applicable laws.”

Potentially, all product specific training can be rendered by "anyone." Class of business training must be through an accredited supplier. We imagine that this may be one of the issues holding up the release of the new Regulation.

CPD must be tracked by a professional body, but attendees do not need to be a member of the body. We doubt whether professional bodies are overly keen on the untold administrative work without commensurate subs and fees. Yet another cause for delay?

We were told that draft amendments to the FAIS General Code of Conduct would be released before the end of March. It was not clear what the reason for these amendments would be, but it was confirmed that any amendments to the General Code of Conduct will align with the (draft) PPR.

They also said that the Section 13(1)(c) exemption (pertaining to premium collection by Juristic Reps) was likely to be enacted by the end of March.

Supervision - Felicity Mabaso

The results of the 'themed visits' established the challenges faced by non-traditional insurance players (for example the motor industry, travel agents and freight forwarders) as they were in contravention of the FAIS Act and Regulations in various ways. The various results are being reviewed to see what solutions are possible. Further planned theme visits include: Category I FSPs with no Compliance Officer and Category I FSPs with Juristic Reps.

FICA: Consultation on the inclusion of Short-term insurers and brokers as Accountable Institutions under the Act is to be undertaken on 12 May 2017. We will attempt to find out how this consultation will take place and keep you informed.

As expected, it was confirmed that the Conduct of Business Reports (i.e. for FSPs) are planned to be implemented in 2018.

FAIS Compliance - Manasse Malimabe

This is a list of compliance issues the compliance department investigated:

- Conflict of Interest in the motor industry: this is ongoing and we can expect further cases or comments
- Fraudulent qualifications
- Unregistered Representatives

During the presentation, they said that "rent a KI" models are viewed in a very poor light and will be dealt with severely should they be in breach.

The following Enforcement issues were dealt with:

- Unregistered Representatives
- Sign on bonuses (we have already seen the results of this)
- Unregistered persons (i.e. incorrect license categories)
- Breaches of licensing conditions
- Failure to debar Representatives

The following Inspections are currently underway:

- Examination fraud
- Sign on bonuses
- Forex trading providers
- FSPs conducting pyramid schemes (i.e. making false representation that the product is a legitimate financial product)
- Key Individual lack of operational ability

We have discussed and written about most of these issues in previous Newsletters.

RDR - Leanne Jackson

Leanne said that changes to the Long- and Short-term Insurance Acts are planned to take effect in the second quarter of 2017. We're just a bit past half way through the first quarter, so let's wait and see.

Clarification was given regarding the difference in earnings on credit life policies which can be made up by a binder or outsource fee provided the work is actually being conducted, as this was the original intention of the commission structure.

One of the important changes as the RDR proposals are implemented is that premium collection will move into "services as intermediary" and will be chargeable for as part of outsource activities in comparison to its current place as part of binder activities.

Insurance Conduct of Business Returns

The FSB has issued a revised version of the bi-annual Conduct of Business Return ("CBR 1 2017_V2") for the period January 2016 to June 2016. This was done because of a few slight errors and inconsistencies that were identified in the previous version of the return published on 15 December 2016. The errors related to:

- The renaming of the portal on the FSB's website
- Some system adjustments that were needed
- Amendment of certain validation tabs
- Amendments of terms to correlate with the proposed PPR
- Amendments required to certain questions

The FSB has maintained its stance regarding the first submission to be a "best effort" attempt by insurers to complete the return as fully as possible based on their current data and systems capabilities. They say that the "best effort" basis will assist insurers to develop appropriate action plans, with clear transitional milestones, to ensure an adequate state of readiness for full and complete submission of returns by the end of 2018. The insurers' action plans must accompany the first return.

It will be interesting to see if progress against the action plan will be monitored by the FSB, although they say that this will occur.

To assist insurers, the FSB has extended the submission deadline date from 30 April to 30 June for the first return and 31 October for the second return of the year which will contain data for the period 31 July 2016 to 31 December 2016.

The following data will not be required for the first and second round of submissions due on 30 June and 31 October 2017 respectively:

- Long-term insurance group risk and fund member policies
- Long-term insurance linked policies
- Short-term insurance commercial lines policies

Recent FSB fines

On 24 March 2017, the New National Insurance Company was fined R100,000 for contravening Rule 7.4(a) of the Policyholder Protection Rules issued under the Short-term Insurance Act in that it failed, within a reasonable period, to accept a claim submitted by a policyholder.

As aggravating factors, the Registrar considered, amongst other factors, that New National failed to demonstrate sound insurance principles and practice in the interest of the policyholder and by taking a lengthy period to eventually settle the claim that resulted in the policyholder not being treated fairly.

In a more recent case, also relating to the PPR, Assupol Life Limited (Assupol) was fined R500,000 although there were additional issues of non-compliance taken into consideration by the FSB.

- During the period August 2014 to June 2016, Assupol remunerated its independent intermediaries by way of permitting them to share in underwriting profits in contravention of section 49 of the Long-term Insurance Act 52 of 1998 (the Act); and
- During the period 20 June 2012 to 13 July 2015, Assupol contravened Rule 16.1 of the Policyholder Protection Rules issued under the Act by rejecting claims without advising policyholders in its notice of rejection of their rights as stipulated in Rule 16.1. In particular, Assupol failed to inform its policyholders of:

  – Their right to lodge a complaint under the Financial Services Ombud Schemes Act
  – The time limitation for the institution of legal proceedings

The Registrar considered, amongst other factors, that Assupol failed to exercise proper oversight over its outsourced functions and that its failure to comply with the PPRs had the potential of causing prejudice to the policyholders whose claims were rejected.

It is interesting to note that in both cases although the FSB has quoted the sections of regulation that had been contravened, they conclude with a breach of principles – a quick insight into what we can expect in terms of principles-based legislation perhaps?

Inseta's 'Unemployed Learnership' programme for 2017 to 2018

Inseta has decided to fund an 'unemployed learnership' programme for the year April 2017 to March 2018 and is calling on service providers to provide recruitment, HR and payroll support respectively, which services will be paid for by Inseta.

If you are interested in participating in this programme, please complete this form and send it off to Inseta as soon as possible.

FICA: To Report, or not to Report? … Is not the Question

We have recently conducted FICA (Financial Intelligence Centre Act 38 of 2001) training at some of our clients. Even though the understanding of the general principles was good, we realised that a genuine fear of reporting, especially suspicious and unusual transactions, exists. We therefore had to remind these institutions of their obligations in terms of the FIC Act.

On 5 April 2017, the FIC release Public Compliance Communication (PCC) 37, which focused on Reporting Institutions and their obligations. The timing could not have been better as this document included the importance of reporting certain transactions.

To recap, Cash Threshold Reporting refers to coin and paper money (local and foreign currency) in excess of R24,999,99 either paid to or by a client. These transactions should be reported to the FIC within two days.

The reporting of Suspicious and Unusual Transactions is the responsibility of all employees within the company, and reports must be submitted to the FIC within 15 days of becoming aware of the suspicious or unusual transaction.

These reports can only be submitted if the minimum client information was obtained while conducting a business transaction with a client.

Reporting cash threshold transactions, and suspicious and unusual transactions is therefore not a choice; it must be done in the correct manner within the specified timeframes. Please do not disregard this obligation.

To read the full document, click here.

How to Answer if the FIC Comes Knocking

FIC released PCC 38 on 31 March 2017 which provided clarity to Accountable Institutions, Reporting Institutions and any other person on information requested by the Centre, how to respond, by when and what needs to be included in the response. These requirements take effect on 2 May 2017.

Firstly, all institutions (as listed above) must identify a person within the organisation who will handle these types of requests from the FIC which will be received via the message board on the registration and reporting platform; or encrypted email messages. Other secure methods may also be used by the FIC. The recipient must respond by the same method through which the instruction or request was received. The FIC may also request a response via another method which they will inform the person or institution of. These responses must include all requested information in PDF, MS Word or MS Excel format and need to reflect the reference number provided by the Centre in their initial request. The person or institution will need to meet the deadline which will exclude Saturdays, Sundays and Public Holidays. An extension request can be submitted, but must include justification thereof.

Section 27 requests will relate to clients that might be suspected of involvement in money laundering and terrorist financing activities. Section 32 reports focus on reports made by the respective institution. Intervention by the Centre (Section 34) is specific to a suspicion that a transaction or proposed transaction involves the proceeds of unlawful activities or money laundering. The Centre may instruct the institution to refrain from proceeding with a transaction for a period not exceeding five days (excluding Saturdays, Sundays and Public Holidays). A Section 35 monitoring order only applies to Accountable Institutions. This means that the institution will receive a monitoring order which enables the Centre to obtain access to all the client's accounts and transactions related to these accounts.

To read the full document, click here.

FROM AC HAS

The third part of our HR practical implementation of the Fit and Proper amendments covers **competence requirements.**

AC HUMAN ASSETS SERVICES

The competence requirements state that an FSP, Key Individual and Representative must:

i. have adequate, appropriate and relevant skills, knowledge and expertise in respect of the financial services, financial products and functions that that person performs
ii. comply with the minimum requirements as set out
iii. maintain their competence

It is the FSP's responsibility to establish, maintain and apply adequate policies, internal systems, controls and monitoring mechanisms to ensure that its Key Individuals and Representatives comply with, are aware of, are trained, and are capable of rendering a financial service.

"Well – there's your problem. You can't upgrade the system without upgrading the staff."

Please refer to the AC Special Newsletter for detailed information on the changes in competence requirements.

Let's take a look at the HR implications that come to mind for the proposed amendments in competence requirements:

Possible HR implications with regards to changes in competence requirements	
Recruitment processes	During your recruitment process, if you are appointing a Key Individual, you will have to ensure that the Key Individual must have obtained experience in the management and/or oversight of the rendering of a financial service in particular. Previously, only management skills were required irrespective of whether the business was related to rendering a financial service or not. Where automated advice is provided, your Key Individual needs to understand and have experience in **both** the insurance and technological systems being used. For both Key Individuals and Representatives, experience needs to be current, i.e. the experience in a specified category must be during the last five years, or else the experience will be deemed to have lapsed. Make sure that all your candidates have met the minimum requirements in terms of the qualifications. Request certified copies of Regulatory Examination and Academic certificates. Make sure that you are aware of who is exempt from having to obtain such qualifications.
Contract of Appointment	Make sure that your contract of employment includes the FAIS clauses that cover all elements of FAIS, including the competence and qualification requirements. This clause will also enable the employer to take action against fraudulent qualifications. Look at the sample Contract of Employment in the HR Manual on our website under: Basic Conditions of Employment/Sample Contract of Employment

Code of Conduct/ Disciplinary Code	We recommend that your Disciplinary Code/Policy explicitly includes the possibility of debarment should the required minimum qualifications and competence requirements not be met, as these are inherent job requirements.
Key Performance Areas	We recommend that Performance Contracts state that Key Individuals and Representatives maintain and comply with the required Class of Business and Product Specific training, Regulatory Examination and CPD requirements and that it is their responsibility to manage this.
Skills Development	It is advisable to: 1. do an audit on all your existing Representatives and Key Individuals in terms of their current qualification status and the transitional arrangements 2. determine whether some of your employees are now exempt from certain qualifications and how you are going to deal with any studies in progress 3. map a training plan for each Representative and Key Individual for: a. Class of Business training b. Product Specific training c. CPD training with the correct number of hours 4. keep accurate records of all training conducted, attended and attained. Look at the sample Training Register in the HR Manual on our website under: Training and Development/Sample Training Register 5. make sure that your employees belong to a Professional Body for the capturing of CPD points and if any costs are going to have to be incurred by the company 6. submit your Workplace Skills Plan and Annual Training Report before 30 April which will enable your company to receive a portion of your payable levies back annually.

If you have any other challenges that we have not included, please let me know so that we can assist and/or share the information.

Should you have any specific questions with regards to any other HR matters, please send these to bronwynn@associatedcompliance.co.za or has@associatedcompliance.co.za.

How to stay sane when using Track Changes in Word

Most people I speak to have said that they find Microsoft Word's Track Changes feature frustrating and difficult to work with. It's actually quite simple, but if you don't know how to use it, it will look like a whole lot of annoying, multi-coloured balloons, lines, and red marks that don't go away no matter which button you press.

AC-PROOFED

What are Track Changes?

Track Changes (also known as redlining) is a very useful tool when you want to keep track of who's done what to text within the document. Let's say that Craig puts together a document and emails it to his colleague, Bryan, for feedback. If Bryan edits the document with Track Changes on, when he sends it back to Craig, Craig will be able to see what changes Bryan has made.

I am going to do my best to explain how to use Track Changes to make life easier for you.

Where do you start?

First, you need to turn Track Changes on. The quickest way to do it (in all versions of Word) is to hold down the Ctrl+Shift+e keys. If you don't like the thought of having to remember keyboard shortcuts, you can click on the Review tab in the menu bar and then click on Track Changes. When the button is highlighted in grey, Word is tracking changes.

How to make Track Changes work for you!

There are several ways of displaying the changes that you have made. You have several options for what changes you want to see; these can be found in the menus in the Tracking group:

- **Simple Markup:** This shows the final version without inline mark-ups. You'll see a red line in the left margin to show where a change has been made.
- **All Markup:** This shows the final version with inline mark-ups.
- **No Markup:** This shows the final version and hides all mark-ups.
- **Original:** This shows the original version and hides all mark-ups.

You can personalise this feature and turn off balloons and other irritating features too. Personally, I've never met anyone who likes those overlapping balloons down the right-hand side of a document. It is so much easier on the eye to see what they call in-line changes (where the deleted text appears struck out, and added text appears in a new colour). Sadly, Microsoft thinks otherwise and by default, the latest versions of Word will use balloons. Don't let this put you off! All you need to do is to click on the small arrow next to Show Markup, then Balloons and make sure that the option to deselect the balloon mark-up option in favour of in-line mark-up.

While you're at it, you may want to disable track changing of formatting changes. Most of the time these changes (e.g. adding a line space or adjusting the indentation of a quotation, etc.) are inconsequential anyway, making the track change mark-up more of an irritant than anything else. Turn it off by unchecking Formatting in the Markup options menu.

Now, just because it's called Redlining, it doesn't mean that your changes have to be in red. There's nothing worse than getting a document back which looks like an army of red ants has marched all over your page. If you prefer to have your changes in blue, all you need to do is click on the little arrow on the bottom right of the Tracking menu, click on the Advanced Options button and choose a colour that works for you.

How to Accept and/or Reject changes

In the Review tab, you'll see the Accept and Reject buttons, each of which has an arrow at the bottom of the box. If you want to accept or reject one change, click within the change and then click either Accept or Reject. Then move on to the next change. If, however, you want to accept or reject everything in the document, you have the option of accepting or rejecting everything in one fell swoop. You can even accept or reject every single change made, and then stop tracking changes. Bonus!

If someone sends you a document and you want to see if there are any Tracked Changes, click on the Review tab and in the Changes section, click on Next. If the message says: "The document contains no comments or tracked changes" then there are no comments or tracked changes. Otherwise, your cursor will move to the first tracked change in the document.

Remember that if you turn off the display of tracked changes, it doesn't mean they're not there, but rather just hidden. If you want to remove them forever, you will need to either accept or reject the changes.

It's really as simple as that! If you have any questions, or you need me to help you with your document, I'm a phone call (083 657 3377) or email (kimh@associatedcompliance.co.za) away!

PROTECTION OF PERSONAL INFORMATION ACT (POPIA) – SECURITY SAFEGUARDS

Over the last seven months the POPIA articles have dealt with responsibility, processing, purpose, further processing, information quality and transparency or openness.

Now that you have established the reason and purpose for processing the personal information, in addition to establishing whether you are a "responsible party" or an "operator", the next question is how to manage privacy risks. In other words, how to ensure that the personal information in your possession is safe and secure. This is information security discipline, which is defined as "protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction." Remember that information may reside on information systems such as computer servers, networks, desktop and laptop computers, and cell phones, etc., and will most likely constitute intellectual property or confidential information.

It is a well-known fact that to protect information systems from increasing levels of cyber threats, organisations are compelled to institute security programmes. To do so, you will need to establish and understand what personal information, be it hard copy and electronic copy, your business has in its possession.

Section 19(1) of POPIA requires organisations to "secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent; loss of, damage to or unauthorised destruction of personal information."

Sections 20 and 21 deal with personal information that is being processed by operators or persons acting under authority and the required security measures as required by section 19.

What Condition 7 (Security Safeguards) tells you is what aspects of personal information must be secured, but not how you should go about implementing the required security safeguards.

The question to ask yourselves as a business is "what data or personal information" you have, because you cannot protect data that you don't know you have. The solution is to do a complete data inventory and data flow mapping exercise of personal information (risk identification of personal information), by establishing standards to classify the sensitivity of the personal information and as such determine the levels of protection that would be required. This would include an inventory of all types of personal information and the related processing activities, systems, and third parties that are involved in the handling and processing of such information. So, for example, what personal information the business uses, assessments and audits of databases and data flows/processing activities, with the outcome being a personal data inventory/dashboard and a data map of the data analysed enabling you to have a clear picture of the personal data you use across your business. It also needs to include the transfers of personal information data to and from third parties, and the collection and processing of data by third parties.

Once you've completed the risk identification of personal information, the next step is to assess the risks associated with specific information security-related risks, for example special personal information and children's personal information. The rationale here is that to choose effective and efficient information security measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats.

The risk assessment should include the following activities:

- Identification and classification of information assets;
- Identification of the threats to these information assets; and
- Identification of any vulnerabilities in the current information asset safeguards.

Your risk assessment should include assessments on the types of risk, for example:

- Intentional Conduct;
- Hackers;
- Organised Crime;
- Insider Attacks; and
- Attacks by service providers and other third parties, among others.

Once you've completed your risk assessments, the next step is to decide how to treat or manage the risk factors that have been assessed through:

- Avoidance: not performing the activity that generates the risk;
- Reduction: using controls to reduce or eliminate the risks by way of preventative, detective or corrective controls;
- Sharing or Transfer: sharing the risk via outsourcing or insurance; or
- Retention: where you decide to retain or self-insure the identified risk.

After assessing the assets, threats and vulnerability to threats of these personal information assets, you should now be able to start drafting and implementing information security programmes and privacy controls, such as data encryption, identity management and authorisation, computer security controls, network security controls, physical security, personnel security, application security and breach incident management.

The purpose of the controls would be to:

- Ensure the security and confidentiality of personal information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorised access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

Remember that where your organisation is regarded as being the "responsible party", it is necessary to ensure the security of personal information, since according to POPIA the responsible party is ultimately accountable for the personal information of the data subject, even if the privacy breach was caused by the third party, such as an operator. You would be recommended to discuss your security safeguards with your IT department or service provider/s.

The last section dealing with security safeguards is section 22. In short, the section requires you to draft and implement a "Breach Notification" policy supported by:

- a process for identifying the notification and related requirements of other applicable jurisdictions relating to the data subjects affected by the breach;
- a process for assessing the need for stakeholder's breach notification, if required by law, regulation, or policy; and
- a process for delivering the notice in a timely manner.

To summarise, physical security controls to include deterrent, detective, and preventive measures, are the means you put in place to mitigate physical security issues.

Deterrents aim to discourage those that might violate your security, detective measures alert you to or allow you to detect when you have a potential intrusion, and preventive controls actually prevent intrusions from taking place. In isolation, none of these controls is a complete solution, but together they can put you on a much stronger footing for physical security.

INTERESTING THINGS WE HAVE READ

Insurance Gateway

New binder regulations – is the writing on the wall? An article done by Associated Compliance, originally published in the Camargue Weathervane Newsletter.

Click here to read the article.

A number of relevant articles from Moonstone:

Legislative avalanche warning for FSPs

Click here to read the article.

Call for Caution on Regulatory Interventions

Click here to read the article.

Regulatory update on Short-term Insurance (see FA News article on the same subject below)

Click here to read the article.

FAIS Compliance - Compassion not an alternative to Compliance

Click here to read the article.

FA News

FSB addresses concerns surrounding Regulatory Reform

An article on a recent "round table" discussion with the FSB where aspects of the proposed new Insurance Bill were discussed. It's worthy of a read, even if you may not be in total agreement with the detail.

Click here to read the article.

COVER Magazine

To quote a recent edition of this magazine that dealt with their relationship with the IISA and more specifically how IISA events can now be accessed as recorded events and allow people unable to attend IISA events (usually held in Johannesburg) to access these and gain valuable IISA CPD hours (and soon FAIS CPD hours).

COVER and the **IISA** have a longstanding relationship and we have been looking for a way to bridge the distance gap for our readers/viewers and IISA members who are unable to attend the highly relevant IISA insurance forums.

"These forums can now be purchased to view online. The IISA will select which forums are appropriate for online viewing. Attendees/viewers who have logged in & purchased the course will gain the appropriate amount of IISA CPD hours after completing questionnaires at the end of each video".

Johannesburg Address:

Ground Floor

Lakeview House

Constantia Office Park

Corner 14th Avenue and Hendrik Potgieter Street

Weltevreden Park

Roodepoort

1709

Email:

info@associatedcompliance.co.za

Tel:

011 678 2533

Fax:

011 475 0096

This Newsletter was proofread by Kim Hatchuel of AC-Proofed.

Click here to download the AC-Proofed brochure

Layout and design by Dung Beetle Creative Studio - www.dungbeetlecs.co.za