Legislative Summary: Adoption of The Basel III Reforms

Shred-it Making sure it's secure.™

Capital Requirements Directive IV (EU Directive 2013/36)

Enacted: 15 October 2013; Into force: 1 January 2014

1 What the law covers:

The CRD IV is made up of two parts:

- **Capital Requirements Regulation** ("CRR") which is directly applicable to firms across the European Union ("EU")
- **Capital Requirements Directive** ("CRD") which must be implemented through national law

They cover:

- Implementation of Basel II and Basel III rules for the financial services industry within the European Union (The Basel Framework)
- Introduction of tighter regulatory controls to enhance the quality and quantity of capital
- Rules on the evaluation and measurement of risk
- Strengthening of minimum capital requirements for financial institutions to hold to meet their credit, operational and market risks
- Updated rules on corporate governance and standards for EU regulatory reporting (i.e. "COREP" and "FINREP")

The Prudential Regulation Authority ("PRA") and the Financial Conduct Authority ("FCA") are responsible for monitoring and enforcing compliance of the CRD in the UK.

2 Who must adhere to the regulations:

Credit institutions (banks and building societies) and certain investment firms.

3 What is The Basel Framework:

The Basel Framework (Basel Accord of 1988, Basel I and Basel II Reforms) is designed to:

- Be the international framework for banking and financial institutions
- Standardise the evaluation and measurement of risk
- Establish the minimum capital requirements to operate
- Ensure that future financial crises are prevented or minimised
- Give national regulators the choice on how best to apply it within their own countries

The Basel Accord was subsequently implemented in the EU via the Capital Requirements Directive ("CRD"). The CRD was revised upon introduction of Basel II and then the Basel III Reforms to become the current CRD IV.

4 How it relates to information management:

The Basel Framework is based on three 'pillars'. Pillar 3 aims to improve market discipline by requiring firms to publish certain details of their risks, capital and risk management.

Information management is, therefore, critical to ensure compliance. This includes adherence to the required document retention periods.

For example, Section 478 of the Basel II Accord states that "estimates of EAD (exposure at default) must be based on a time period that must ideally cover a complete economic cycle but must in any case be no shorter than a period of seven years."

The FCA created new rules and guidance for CRD compliance with the General Prudential Sourcebook ("GENPRU") and the Prudential Sourcebook for Banks, Building Societies and Investment Firms ("BIPRU"). BIPRU Chapter 11 sets out the provisions for Pillar 3 disclosure.

5 How to comply:

1. Determine the relevant compliance requirements (e.g. CRR, CRD, COREP and FINREP) and regulatory bodies (e.g. EBA*, ECB*, FCA and PRA)

2. Establish detailed record and information management policies and procedures

3. Create a formal disclosure policy, including:
   - Information to be disclosed and the exemptions
   - Frequency, media and location of disclosures

*European Banking Authority ("EBA") and European Central Bank ("ECB")

6 Offences/penalties for non-compliance:

CRD IV introduced a new administrative penalty system which will be enforced by the ECB, as of November 2014.

Penalties include:

- Withdrawal of banking license
- Binding orders to companies and/or individuals to stop and not repeat the violation
- Public declaration of violation
- Removal of an individual from a board, managerial position or function

Maximum fines:

- Individuals – Five million Euros
- Banks – 10% of consolidated turnover, based on year prior to violation

At the national level, the PRA and FCA can also impose disciplinary, civil and criminal penalties for non-compliance.

For more information:
PRA – bankofengland.co.uk
FCA – fca.org.uk

7 Secure document retention and disposal guidelines:

Recommended inclusions for a records management policy:

- ☐ A statement of purpose
- ☐ Categories of documents and how long they should be kept
- ☐ Definition of "document" and the format and length of time in which it is to be retained (electronic or hard copy)
- ☐ Guidance on creation of documents
- ☐ Members of staff designated to deal with the document management system
- ☐ Guidelines for ensuring all staff are trained on how to comply with the policies and procedures
- ☐ Methods of document destruction, including those carried out by third parties
- ☐ How to keep an accurate record of documents destroyed

8 How Shred-it can help:

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organisation's needs

Advice and Expertise

- Trained experts in information security
- Provide a Data Security Survey at your organisation
- Helpful resources available at shredit.co.uk/resource-centre

For peace of mind, contact Shred-it today

0800 028 1164 | shredit.co.uk

Making sure it's secure.™