Review of the Risk Assessment Process for Payment Systems

Background
At a special meeting of the IPSO Board of Directors held on the 29/6/2012 to discuss the Ulster Bank technical incident, a decision was taken, arising from a request from the Central Bank of Ireland, to appoint an independent Risk Management Consultant to review the methodology employed at that time to conduct Risk Assessments in the Irish Retail Electronic Payments Clearing Company Ltd. (IRECC) and the Irish Paper Clearing Company Ltd. (IPCC).

A joint IPSO/Central Bank Steering Committee was appointed to agree Terms of Reference, identify a list of suitable consultants and manage the process. The Steering Committee comprised:

- David O’Riordan, Deputy Head of Payments and Securities Settlements Division, Central Bank of Ireland
- Enda Cullen, Head of Operations, BNP Paribas and member of IPSO Audit, Finance & Risk Committee
- Pat McLoughlin, CEO of IPSO
- Eilish McGuinness, Business Continuity Management, Central Bank of Ireland
- Paula Gray, Manager, Retail Payments, Corporate Services, IPSO
- Martin James, Manager, Wholesale Payment Systems, IPSO

The Scope of the consultancy was as follows:

- Review the methodology for conducting risk assessments of the end to end clearing processes, including how the process is conducted in each member bank.
- Benchmark both the Policy and the current practice against international best practice and standards where applicable.
- Produce a gap analysis and recommendations to ensure that IPSO’s future risk management process is sufficiently robust to maintain the efficiency, effectiveness and integrity of the retail payment systems.

Eight companies were invited to tender on the 27/7/2012 and following receipt of tenders, a shortlist was agreed by the Steering Committee and interviews held on the 27/8/2012. BH Consulting were awarded the tender and completed the exercise.

The following is a summary of their findings.

“BH Consulting conducted the assessment of the risk management and risk assessment processes employed by the Irish Payment Services Organisation Ltd. and its member companies to identify risks against the electronic and paper payments systems employed within the industry. By their nature the payment systems are considered critical systems which can have widespread consequences not just on any member organisation affected, but on the whole payments industry as a whole, and indeed on a wider societal scale. A prolonged issue with the payment systems could have a major impact on financial transactions and stability within the Irish market.

Also of concern to the Irish Payment Services Organisation Ltd. is the potential damage a prolonged issue could have on the reputation of the organisation and the industry; in
particular as it tries to introduce more progressive and modern ways of supporting electronic payments.

To conduct this review BH Consulting split the review into two phases:

- The first step was to review the processes, procedures and methodologies employed by the Irish Payment Services Organisation Ltd., the member companies and the role the Central Bank of Ireland plays in the process. This was facilitated by running a number of collaborative workshops with each of the above parties during the months of September and October 2012. Workshops were conducted with the following organisations:
  - The Irish Payment Services Organisation Limited
  - The Central Bank of Ireland
  - Bank of Ireland
  - Allied Irish Bank
  - Ulster Bank
  - Permanent TSB
  - BNP Paribas
  - National Irish Bank

  The methodology employed to conduct these workshops was based on a series of questions formulated from recognised industry standards such as:
    - ISO 31000:2009 Risk management -- Principles and guidelines
    - ISO 27005:2008 Information technology -- Security techniques -- Information security risk management
    - ISO 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity
    - The RISK IT Framework from ISACA

  The above standards are International IT, Information Security and Business Continuity Standards but not Payment Industry Standards per se.

  Each workshop was conducted face to face with each organisation ensuring the appropriate people with responsibility for the process within their organisation attended the meeting.

- The second part of the assessment was to review associated documentation, in particular the Irish Payment Services Organisation Ltd. risk assessment policy and the risk assessment questionnaires for the electronic payment systems and the paper payment systems.

  During the review it was noted that each organisation provided full and unequivocal cooperation with the review process with many seeing it as providing value to the industry. All organisations also found value in the risk management and risk assessment process as it focused resources to specifically risk assess their individual payment systems.

  The review found the current Irish Payment Service Organisation’s risk management process is a relatively robust process based on international best practices. The risk management process entails a risk assessment conducted every two years.

  This risk assessment contains a list of risks relating to payment clearing systems which are reviewed and agreed by the respective board members for the Irish Retail Electronic
Payments Clearing Company Ltd. (IRECC) and the Irish Paper Clearing Company Ltd. (IPCC) before being distributed to each member organisation. Each member organisation completes the risk assessment and returns it to IPSO for review at industry level. The IRECC/IPCC Board Director plus an authorised senior official from either of (a) Risk Management Policy, (b) Business Continuity Programme, (c) Internal Audit Practices, or (d) Operational Risk Review areas, signs off on their banks risk assessment result prior to submission. The industry level risks are presented to the respective board members for IRECC and IPCC. Feedback on any issues arising from the risk reviews, together with an overview of the industry risk appetite, are also presented to the board members who in turn are tasked with disseminating this information to the appropriate persons within their own member organisation. The boards took a decision at the end of 2011 to review the risk assessment against the clearing systems on an on-going basis at an industry level during the quarterly board meetings of the respective IRECC and IPCC companies.

BH Consulting made the following recommendations:

Risk Assessment
“Each members risk management process should be aligned with an industry recognised framework or standard. Independent verification that the member is adhering to the requirements of its selected framework/standard should be sought from a suitably qualified individual or firm, the member’s external auditors or be certified to the selected framework or standard by a qualified certification body.”

Timing of Exercise
“The current process for assessing the risks for the payments systems is every 2 years. Many members felt that this was too big a gap between assessments and that it should be conducted on a more regular basis. The 2 year gap results in a lack of familiarity with the process which then has to be relearned. In some cases this gap also results in staff no longer being involved in the process and new staff having to be trained and made familiar with the process. Making the process occur more regularly would help ensure the assessment is in line with the latest threats and risks.”

Consistency in approach
“Clearer guidelines with appropriate familiarisation workshops should be held to ensure all members understand the scope of the risk assessment, what the terminology means and what is expected from each member.”

Decision of IPSO Board of Directors
The IPSO Board of Directors, at its meeting on the 07/2/2013 accepted the recommendations and approved a formal implementation plan.

IPSO is now engaging a specialist firm to assist in delivering on the implementation of the recommendations including:
- To review and update the IPSO Risk Management Framework.
- To review and update a clearly defined risk assessment template for use by member banks.
- To facilitate risk assessment workshops with IPSO, member banks and the Central Bank of Ireland.
**Implementation**
The monitoring of the implementation will be undertaken by the Audit, Finance and Risk Committee of the IPSO Board and the Central Bank of Ireland will be part of the joint Steering Committee set up at the commencement of the project.

The new arrangements will see the following additional enhancements to the Risk Assessment methodology:

- The IPSO Risk Framework will be fully aligned to industry best practice.
- The risk assessment will be carried out annually (rather than bi-annually).
- There will be external validation of the Clearing Banks’ submissions to annual risk assessments.
- Risk assessments will focus on the payments system from a whole and not just against the individual elements that comprise the payments system.
- Representatives from member banks’ operating, I.T., and risk functions will present their assessments to a Payments Risk Governance Board comprising IPSO, the Payments and Securities Settlements Division and the Banking Supervision Division of the Central Bank of Ireland.

Pat McLoughlin  
Chief Executive  
IPSO