iQuda information risk management policy

Introduction

This policy has been created to help to manage information risk at iQuda.

Information risk is managed within work areas; all staff take responsibility for information risk. Management are to be tasked with:

- ensuring that the information assets within their departments are managed and confidential information is safeguarded:
- reporting on breaches of information security.

It is highly important to iQuda that we minimise information risks and safeguard the interests of our clients, staff and stakeholders. The introduction of the General Data Protection Regulations 2016 (the GDPR) further emphasises the importance of robust information security. iQuda is committed to the highest standards of compliance with the regulations.

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of iQuda continuously manages information risk. The business owners recognise that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all of iQuda's activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

The business owners acknowledge that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls.

Policy objectives

The Information Risk Policy has been created to:

- Protect iQuda, its staff, clients and stakeholders from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in approval, review and control processes;
- Encourage pro-active rather than re-active risk management;
- Provide assistance to and improve the quality of decision making throughout iQuda;
- Meet legal or statutory requirements; and
- Assist in safeguarding iQuda's information assets, and those of our clients

The iQuda Senior Information Risk Owner (SIRO) (Anthony Jones) is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for iQuda.

The SIRO is responsible for the ongoing development and day-to-day management of iQuda's Risk Management Programme for information, privacy and security.

Information risk assessments will be performed at least once each year on all information assets. The risk assessments will include:

- A risk register specifically for information risk
    - agreed mitigation plans
    - details of any assumptions
    - external dependencies for information management
    - specific actions required to control risk, with expected completion dates

The SIRO shall advise the business owners on information risk management strategies and provide periodic reports and briefings on Program progress.

Risk Assessment Methodology

Risks will be identified and calculated using an Impact vs Probability Matrix (please see the table below). The Impact vs Probability Matrix will help iQuda to measure the probability and potential impact of each risk we identify. The ultimate risk score we assign to a risk will decide the actions we take to treat the risk. Risks are measured using the following calculation: Risk = Impact x Probability

All risks are calculated using the QRA iQuda Risk Assessment document which contains the below table & the risk calculation methodology. The risk assessment methodology is used in the following way:

1. Risk is identified e.g. Server
2. The type of threat is identified e.g. Malware Attack
3. The probability (or likelihood) of the risk occurring is determined & a score is assigned to the risk based on how probable it is that the risk will occur. Scores are based on a scale from very low (0.1), low (0.3), moderate (0.5), high (0.7) or very high (0.9). I.e. if it is highly unlikely a risk will occur, it will be assigned a score of 0.1. If it is very likely that a risk will occur, it will be assigned a score of 0.9.
4. The impact, or potential impact that the risk will cause if it occurs is determined & a score is assigned to the risk. Scores are based on a scale from very low (0.05), low (0.1), moderate (0.2), high (0.4) or very high (0.8) i.e. if a risk occurring will have a very low impact its score will be (0.05). If the risk will have a very high impact its score will be 0.8.
5. The two scores are multiplied using the following calculation: Risk = Impact x Probability. The Impact vs Probability Matrix contains the calculation scores to make this process easier i.e. take the probability & impact score and find where they meet on the Matrix to determine the overall risk score.
6. The overall risk score will fit into one of the following categories, this is defined as the Risk Score.
    a. High Risk: Score > 0.14
    b. Medium Risk: 0.05 < Score < 0.14
    c. Low Risk: Score < 0.05
7. An appropriate course of action is assigned to the risk based on its Risk Score.
    a. Any low risk will be monitored or accepted. Our risk acceptance criteria is therefore below <0.05.
    b. Any medium risk must be treated.
    c. Any high risk must be treated as a priority.
8. All risks, regardless of their severity, must have a risk evaluation action code applied. These codes are:

   a. Accept Risks
   b. Apply Controls
   c. Avoid the Risks
   d. Transfer the Risks

9. All risks which are treated must have a target resolution date assigned, which will be monitored during management reviews.

Impact vs Probability Matrix					
Probability	**Threats**				
Very High / 0.9	0.05	0.09	0.18	0.36	0.72
High / 0.7	0.04	0.07	0.14	0.28	0.56
Moderate / 0.5	0.03	0.05	0.10	0.20	0.40
Low / 0.3	0.02	0.03	0.06	0.12	0.24
Very Low / 0.1	0.01	0.01	0.02	0.04	0.08
Impact	**Very Low / 0.05**	**Low / 0.1**	**Moderate / 0.2**	**High / 0.4**	**Very High / 0.8**

High risk	Score > 0.14
Moderate risk	0.05 < Score < 0.14
Low risk	Score < 0.05

Risk Management Documentation

Risks are managed in accordance with ISO 27001 standards. To this extent, we operate a risk management document through which regular risk assessments are conducted. Each reach that we identify has resolution or mitigation actions attached to it. This approach ensures that we continually reduce the amount of risk in our environment. Please refer to the QRA iQuda Risk Assessment Document. This can be found in the ISO 27001 folder on SharePoint.

Policy scope

This policy is applicable to all areas of iQuda and adherence must be included in all contracts for outsourced or shared services. There are no exclusions.

Communication

This policy is to be made available to all iQuda staff and observed by all members of staff.

There will be ongoing professional development and educational strategy to accompany the implementation of this policy.

Definitions

Key definitions are:

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of *impact* and *likelihood*.
- **Impact**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Probability**
  A qualitative description or synonym for likelihood or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
  - Accept Risks
  - Apply Controls
  - Avoid the Risks
  - Transfer the Risks
- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Appendix 1: Information assets include

- Personal and other information, including
    - Databases and data files
    - Back up and archive data
    - Audit data
    - Paper records (client records, supplier records and staff records)
    - Paper reports
- System / process documentation
    - System information and documentation
    - Operations and support procedures
    - Manuals
    - Contracts and agreements
    - Policies
- Software
    - Applications and systems software
    - Data utilities
    - Development and maintenance tools
- Hardware
    - PCs
    - Laptops
    - Tablets
    - Phones
    - Printers
    - External storage devices (USBs, External hard drives etc).

Priority must be given to information assets that comprise or contain personal information.