PHC IG risk management Overview (Feb 2023)

This guidance provides information on the following*:

- ✓ Why conduct risk management activities?
- ✓ What is risk management?
- ✓ What is a risk register?
- ✓ How is the IG risk register managed?
- ✓ How are Department IG risks reported?
- ✓ Does the Department identify IG risks through other means?
- ✓ Does the Department maintain more than one RR?

*Refer to the Department IG 115 Risk Management Policy for more information.

1. **Why conduct risk management?** The University and Department can reduce the likelihood and severity of potential risks by identifying and taking steps to mitigate them.

2. **What is risk management?** The University and Department have established a risk management program (RM Program), which provides a framework to manage information governance (IG) risks and includes policies, processes and activities. The Department RM Policy program represents the core of the Department's Program along with the use of its tailored IG risk register and risk management reporting.

   For reference, refer to these definitions:

1. Risk	The effect of uncertainty on objectives. This may also be expressed as a deviation from expected outcomes that could be positive (opportunity) or negative (threat).
2. Risk management	Coordinated activities to direct and control an organisation with regard to risk.
3. Risk appetite	The amount of risk that the University/Department is willing to pursue or retain.
4. Risk management framework	A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the University. A risk management framework is expected to include policy, objectives, mandate and commitment to manage risk; together with plans, accountabilities, resources, processes and activities for risk management.

3. **What is a risk register?** The Department Program includes the creation, adoption and maintenance of an IG risk register (RR), which, identifies and classifies Department IG risks in a consistent and coherent manner and assigns risk ownership. IG risks include, but are not limited to, the adequacy of the following controls: equipment asset management; data protection across research operating environments; security review of products, services and applications; managing personnel (starters/leavers); etc.

   The RR contains:

   a) references to assigned owners;
   b) risk descriptions;
   c) gross risk scoring (pre-control);
   d) mitigation/action plans in place
   e) Net risk scoring (post-control); and
   f) Possible additional actions identified but not in place.

4. **How is the IG risk register managed?** The Department Head of Finance and Administration serves as the Senior Information Risk Officer (SIRO) and directs the management of the RR. In response to feedback from the Research and Department Strategy Committees (refer to **Table #1** below), the SIRO designee periodically reviews and updates the RR with the SIRO approving and removing entries as applicable.

5. **How are Department IG risks reported?** The SIRO, IT/IG Head and IG Manager designees review and provide periodic reporting updates on the Program to the Committees noted in Table #1 below. This reporting includes escalation of RR items identified as high risk and their proposed remediation strategy, including – where applicable, the determination to accept a risk as documented. They also propose and seek to obtain support for resources, which wholly or partially remediate the items identified in the RR, consistent with the Department's risk appetite determinations (e.g. proportionate to the expected benefits to be gained and the scale or likelihood of damage).

6. **Does the Department identify IG risks through other means?** Yes, as follows:

   a) During the completion of the University data protection by design (DPD) reviews, the Department routinely undertakes project specific data security and privacy risk assessments. For more information, refer to the IG 114 Data Protection by Design policy;
   b) Under certain circumstances, such as when a research team and its database resource migrate to the Department from another University (i.e. ORCHID), the Department is subject to a "bespoke" security review by the University Information Security (InfoSec) team;
   c) InfoSec conducts yearly baseline security assessments of the Department; and
   d) The Department conducts reviews of certain areas within the Department (i.e. Q Research) on an annual basis.

7. **Does the Department maintain more than one RR?** Yes, Department research teams may also develop and implement supplemental risk registers specific to their respective operating environments, such as the Department Clinical Trials Unit, the Q-Research team, etc.

Table #1