Risk Assessment Policy

Policy Owner	I.T. Manager – S. Britton
Policy Approver(s)	I.T. Management
Related Policies	
Related Procedures	
Storage Location	IT Share, http://in.banksdih.com
Effective Date	2014/09/30
Next Review Date	2016/09/30.

Purpose

Risk assessments are used to determine the likelihood and magnitude of harm that could come to an information system and ultimately Banks DIH Limited itself in the event of a security breach. By determining the amount of risk that exists, Banks DIH Limited will be in a better position to determine how much of that risk should be mitigated and what controls should be used to achieve that mitigation. Without risk assessments the potential exists that the organization can leverage inappropriate (either too strict or too lax) security controls to protect information systems.

Scope

This Risk Assessment Policy applies to all information systems and information system components of Banks DIH Limited. Specifically, it includes:

- Mainframes, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops and other devices that provide distributed computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.

Policy

1. Risk assessments will be performed on all information systems that house or access Banks DIH Limited controlled information. These assessments will address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

2. Risk assessments shall be performed upon initial acquisition of an information system (in the event that the information system is owned/operated by Banks DIH Limited or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of Banks DIH Limited). Further, the risk assessment shall be reviewed and, where required, updated after three years or whenever a significant change is made to the information system, whichever comes first.

Procedure 1

Determine the amount and nature of risk to which a system is exposed:

- Collect and document the information that defines the system.
- Identify and document all potential sources of threat to which the system could be exposed and, for those threats, identify and document all potential vulnerabilities:
    - *Use vulnerability sources such as the National Vulnerability Database.*
    - *Use outputs from System Security Tests.*
- Identify and document all implemented controls that are intended to have a mitigating effect on threats and vulnerabilities:
    - *Evaluate both Technical (access control systems, firewalls, etc.) and Non-Technical (policies and procedures) controls.*
    - *Evaluate both Detective (those that warn of violations) and Preventative (those that inhibit violations) controls.*
- Estimate the likelihood that a particular vulnerability will occur in the face of controls that may be in place to mitigate it:
    - *High likelihood indicates the threat-source is motivated and capable and controls are insufficient or ineffective.*
    - *Medium likelihood indicates the threat-source is motivated and capable but that controls may be sufficient and effective.*
    - *Low likelihood indicates the threats-source is motivated and capable but that controls are sufficient and effective* ***OR*** *the threat-source is unmotivated or incapable.*
- Estimate the impact that a particular vulnerability will have if exercised in the face of controls that may be in place to mitigate it:
    - *High impact indicates significant loss of assets or resources, significant damage to the organizational mission, or serious human injury or death.*
    - *Medium impact indicates moderate loss of assets or resources, moderate damage to the organizational mission, or human injury.*
    - *Low impact indicates minimal loss of assets or resources, or minimal damage to the organizational mission.*
- Cross reference the determined likelihood with the determined impact to determine the overall risk of each vulnerability. Decide if the risk level is to be accepted and, if not, to what degree it is to be mitigated:
    - *Very High risk constitutes high likelihood and high impact. Risks of this nature have the strongest need for corrective action and resolution should be considered an emergency action and undertaken immediately.*
    - *High risk constitutes high likelihood and medium impact or medium likelihood and high impact. Risks of this nature have a strong need for corrective action and a corrective response plan must be developed and put in place within 30 days.*
    - *Medium risk constitutes high likelihood and low impact, low likelihood and high impact or medium likelihood and medium impact. Risks of this nature have a moderate need for corrective action and a corrective response plan must be developed and put in place within 90 days.*

  - *Low risk constitutes medium likelihood and low impact or low likelihood and medium impact. Risks of this nature have a low need for corrective action and a corrective response plan must be developed and put in place within 180 days.*
  - *Very Low risk constitutes low likelihood and low impact. Risk of this nature can be considered negligible and no corrective response plan is required however the risk should be reassessed annually to determine if the risk level has been elevated.*
- Identify and evaluate additional controls that will reduce the identified risk to acceptable levels:
  - *Evaluate both Technical (access control systems, firewalls, etc.) and Non-Technical (policies and procedures) controls.*
  - *Evaluate both Detective (those that warn of violations) and Preventative (those that inhibit violations) controls.*
  - *Perform a cost-benefit analysis for each control to narrow the selection of controls to those that mitigate risk cost effectively.*

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- A minor breach will result in written reprimand.
- Multiple minor breaches or a major breach will result in suspension.
- Multiple major breaches will result in termination.

Revision History

Version	Change	Author	Date of Change