Oklahoma State University IT Information Security Office	For Official Use Only Contents of Report C O N F I D E N T I A L

Risk Assessment Form

ISO-RAF-001

Shaded areas of form are for OFFICIAL USE ONLY

Risk assessment is the process of risk identification and risk evaluation. Risk assessments are designed to identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems [1].

Given the serious security risks to information technology (IT) assets, managing those risks effectively is an essential task for the University and its departments. The process is one that will benefit both the individual department and the University as a whole. Completing such a risk management process is extremely important in today's advanced technological world.

This form should be completed by those responsible for managing information in your department, often in cooperation with individuals in their area who are most familiar with the practices. Completed forms will be used to assess current information security, guide future information security efforts and to prioritize development of helpful standards, guidelines, and procedures.

1. United Kingdom. BS ISO/IEC 1799:2005. May-June 2005. Oct.-Nov. 2006.

Client Profile

Date:	
Prepared By:	

Primary Contact Information

Last Name:	First Name:
Title:	Department:
Phone: Fax:	Campus Address:
Email:	

System Administrator Contact Information

Last Name:	First Name:
Title:	Department:
Phone: Fax:	Email:

Send completed form to: IT Information Security Office
301 Whitehurst Building

Oklahoma State University

IT Information Security Office

For Official Use Only
Contents of Report
C O N F I D E N T I A L

Risk Assessment Form

ISO-RAF-001

Shaded areas of form are for OFFICIAL USE ONLY

Department Profile

Please provide a short description of your department:

Who are your clients?

Number of Employees:

Number of Workstations (desktops):

Number of Mobile Devices (laptops, handhelds, etc.):

Number of Servers:

Server Name	Server IP	Server OS	Asset Value
			☐ High ☐ Med ☐ Low
			☐ High ☐ Med ☐ Low
			☐ High ☐ Med ☐ Low
			☐ High ☐ Med ☐ Low
			☐ High ☐ Med ☐ Low

Have the systems ever undergone a risk assessment? ☐ YES ☐ NO

If yes, please specify the last date of assessment and who performed the assessment:

Are any diagrams available which illustrate aspects of the current environment? ☐ YES ☐ NO

(If yes, please provide the diagram(s).)

Data

Does your business role involve the transmission or storage of sensitive or confidential data? ☐ YES ☐ NO

If yes, please list any applicable legislative, regulatory, or contractual obligations regarding the transmission or storage of sensitive or confidential data for your department:

Oklahoma State University

IT Information Security Office

For Official Use Only
Contents of Report
CONFIDENTIAL

Risk Assessment Form

ISO-RAF-001

Shaded areas of form are for OFFICIAL USE ONLY

Data (Continued)

Is any sensitive or confidential data permanently stored on desktops or workstations?	☐ YES ☐ NO
Does your department role involve the transmission or storage of financial transactions?	☐ YES ☐ NO

If yes, please list any applicable legislative, regulatory, or contractual obligations regarding the transmission or storage of financial transactions for your department:

Describe any policies or procedure concerning the classification of data:

Policies and Procedures

Please provide copies of any/all departmental policies.

Describe any *procedures* in place which addresses security concerns (e.g. limiting public access, locking workstations, passwords, etc.):

Describe any *technical solutions* in place which addresses security concerns (e.g. door-keys, anti-virus, software firewalls, etc.):

Have policies been discussed with employees?	☐ YES ☐ NO
Are policies enforced?	☐ YES ☐ NO
Are new employees required to pass a background check before hire?	☐ YES ☐ NO
Does each user have a unique ID for computer system access?	☐ YES ☐ NO
Are employees given administrative or user level accounts on workstations:	☐ User ☐ Admin

Oklahoma State University

IT Information Security Office

For Official Use Only
Contents of Report
C O N F I D E N T I A L

Risk Assessment Form

ISO-RAF-001

Shaded areas of form are for OFFICIAL USE ONLY

Encryption

Describe any policies or procedures concerning the use of encryption:

Describe the implementation of any cryptographic controls:

Monitoring and Logging

Describe the implementation of any technical controls related to the monitoring of data security:

Describe the implementation of any technical controls related to audit logging:

Data Backup

Describe any implemented procedures or technical controls regarding business continuity (e.g. regular backups):

Are backups stored encrypted? ☐ **YES** ☐ **NO**

Thank you for completing this form.
Please return this form to the IT Information Security Office at 301 Whitehurst.