

# Vendor Risk Assessment

DOCUMENT VERSION: 09/22/04

Date Submitted: \_\_\_\_\_

Date Reviewed w/Edits: \_\_\_\_\_

Example Only  
Not Represented to be  
Approved by Regulators

## TABLE OF CONTENTS

OVERVIEW

VENDOR CHECKLIST

VENDOR PRE-ASSESSMENT QUESTIONNAIRE

CONTRACTS

VENDOR OVERSIGHT SURVEY

VENDOR RISK ASSESSMENT QUESTIONNAIRE

Important: View this document in "Print Layout" to see checkboxes. View layout can be changed under View menu.

# Overview

This document provides Questionnaires to assess the security controls in place at the outside vendor to safeguard MMFG data entrusted to the vendor.

The following information is covered in this document:

- [Vendor Pre-Assessment Questionnaire](#)
- [Vendor Risk Assessment Questionnaire](#)

Important: View this document in “Print Layout” to see checkboxes. View layout can be changed under View menu.

# Vendor Pre-Assessment Questionnaire

This section is for the reference of the Vendor Relation Manager\Project Manager facilitating this assessment. Please use this section to determine the impact of this engagement to the overall security of information.

Important: View this document in "Print Layout" to see checkboxes. View layout can be changed under View menu. Mark boxes by typing an "X" in the appropriate box.

	Name/Date completed
<p><b>1. Data Sensitivity:</b> What is the nature of data that vendor will have access to? (Mark all that apply)</p> <p>No Risk: No data exchanged, no security impact</p> <p><input type="checkbox"/> Low Risk: Only Demographic information and projected financial info</p> <p><input type="checkbox"/> Medium Risk: Only Names, Addresses and Phone Numbers</p> <p><input type="checkbox"/> High Risk: Non-public Private Information (NPI), for example SSN, medical, financial, proprietary and private information about real individuals</p>	
<p><b>2. Complete the <a href="#">Vendor Risk Assessment Questionnaire</a></b></p> <p>Complete survey, obtaining information from vendor as noted. Please return the completed questionnaire to Information Security consultant assigned to your project.</p> <p>Please make sure the email subject contains the line: Vendor Risk Assessment</p>	

# Vendor Risk Assessment Questionnaire

**Vendor Name:**

**Address:**

**Vendor Contact Name:**

**Vendor Contact's Phone Number:**

**Vendor Contact's Email Address:**

**Instructions:**

- Please complete the following questionnaire.
  - For requests for details/description, please describe in Comments (or “Additional Information and Comments” section at end of questionnaire) or attach documentation with the details.
  - Use N/A for Not Applicable where needed – enter under Comments).
  - Helpful hints:
    - View this document in “Print Layout” to see checkboxes. View layout can be changed under View menu.
    - Mark boxes by typing an “X” in the appropriate box.

Risk Assessment Categories	Yes	No	Comments
<b>Policies and Procedures</b>			
Has the security policy document(s) been published and enforced in your organization?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have policies and procedures covering the following:			
• HR Practices?	<input type="checkbox"/>	<input type="checkbox"/>	
• Authorized/acceptable use of Networked Services?	<input type="checkbox"/>	<input type="checkbox"/>	
• Use of Corporate Email, intranet and Internet?	<input type="checkbox"/>	<input type="checkbox"/>	
• Password Management?	<input type="checkbox"/>	<input type="checkbox"/>	
• Software/Hardware Acquisition?	<input type="checkbox"/>	<input type="checkbox"/>	
• Change Management?	<input type="checkbox"/>	<input type="checkbox"/>	
• Encryption Policy and Standards?	<input type="checkbox"/>	<input type="checkbox"/>	
• Security related incidence response/handling?	<input type="checkbox"/>	<input type="checkbox"/>	
• Data Handling Policy (to include data use, storage and destruction of sensitive data)?	<input type="checkbox"/>	<input type="checkbox"/>	
• Third Party Access & Remote Access?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you outsource any security management functionality?	<input type="checkbox"/>	<input type="checkbox"/>	
Are policies and procedures updated frequently?	<input type="checkbox"/>	<input type="checkbox"/>	
Is a senior corporate official directly responsible for the implementation of your organizational security policy?	<input type="checkbox"/>	<input type="checkbox"/>	
Are procedures employed to ensure compliance with privacy laws/regulation requirements related to maintaining security, confidentiality and protection of customer data?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have Information Security staff dedicated to the following:			
• Security Awareness?	<input type="checkbox"/>	<input type="checkbox"/>	
• Policy Enforcement?	<input type="checkbox"/>	<input type="checkbox"/>	
• Risk Evaluation?	<input type="checkbox"/>	<input type="checkbox"/>	
• Risk Mitigation?	<input type="checkbox"/>	<input type="checkbox"/>	

• Regulatory Compliance?	<input type="checkbox"/>	<input type="checkbox"/>	
Are the consequences of non-compliance to the policies clearly documented?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Patch Management</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Do you apply security patches on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have an automated patch management solution deployed?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have vendor agreements in place for timely availability and application of software updates?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Physical Security</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
What kind of perimeter control(s) is applied to data center location?			
• Tokens/Cards?	<input type="checkbox"/>	<input type="checkbox"/>	
• Key Pad Controls?	<input type="checkbox"/>	<input type="checkbox"/>	
• Man Trap?	<input type="checkbox"/>	<input type="checkbox"/>	
• Biometric Controls?	<input type="checkbox"/>	<input type="checkbox"/>	
• Guards?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you monitor/log all access to data center?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have redundant public utilities connections?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you employ UPS (Uninterrupted Power Supply), Battery Banks, Generators etc?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you employ fire/flood detection and suppression systems?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you monitor and escort visitors through critical parts of your company?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you maintain visitor logs for more than 30 days?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Information Security Administration</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Can you provide a recent SAS70 report or other industry recognized audit report?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you limit administrator level access on network and systems infrastructure?	<input type="checkbox"/>	<input type="checkbox"/>	
Is your Information Security staff professionally certified (ISC <sup>2</sup> or SANS)?	<input type="checkbox"/>	<input type="checkbox"/>	
What is the average tenure of your Information Security staff?	<input type="checkbox"/> 1-3 years		
	<input type="checkbox"/> 3-5 years		
	<input type="checkbox"/> 5+ years		
Is access to security logs strictly controlled (Firewall logs, etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you employ version management, build & deploy process?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Network Infrastructure</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Do you maintain up-to-date network infrastructure and administration procedures?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have perimeter scanning/monitoring agreements with managed network services providers?	<input type="checkbox"/>	<input type="checkbox"/>	
Are all your routers configured with access control lists to allow only specific traffic to pass through?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you allow access to your routers via its console port only?	<input type="checkbox"/>	<input type="checkbox"/>	
Are all your networking devices at the latest patch level?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have a procedure to keep track of announcement of vulnerability patches for your networking devices?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you ensure default passwords are changed on networking devices?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you control the change frequency and distribution of admin access to network infrastructure?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you use 802.1x compliant security for your wireless network?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you employ the following intrusion prevention/detection system:			

• HIDS?	<input type="checkbox"/>	<input type="checkbox"/>	
• NIDS?	<input type="checkbox"/>	<input type="checkbox"/>	
• Honey Pots?	<input type="checkbox"/>	<input type="checkbox"/>	
• Rogue device and services detection?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Remote Access and VPN</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Are there any remote access/remote control methods available to access your network, as follows:			
• Call backs?	<input type="checkbox"/>	<input type="checkbox"/>	
• PKI?	<input type="checkbox"/>	<input type="checkbox"/>	
• RADIUS/TACACS?	<input type="checkbox"/>	<input type="checkbox"/>	
• User ID/Password?	<input type="checkbox"/>	<input type="checkbox"/>	
• Token bases access control?	<input type="checkbox"/>	<input type="checkbox"/>	
• Other? – If yes, what?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you allow supervisory/admin functions to be performed over unencrypted external links?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you collect/review audit log data on remote access?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Firewall and Intrusion Detection/Prevention</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Do you have a security team that keeps track of all known vulnerabilities?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have an Intrusion Detection System implemented?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have an Incident response team?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you employ Firewall server(s) to protect your network?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have any other applications (e.g. DNS) running on the same Firewall Server?	<input type="checkbox"/>	<input type="checkbox"/>	
Are your Firewall Server's Operating system & software at the latest patch level?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you allow non-standard (>1024) IP ports passing through your Firewall?	<input type="checkbox"/>	<input type="checkbox"/>	
Have you scanned and verified all the allowable services provided by your Firewall server?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you use firewall-reporting tools to analyze your Firewall log?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have your security policy on your firewall documented and verified?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you protect your internal IP address range(s) (E.g., use NAT/RFC 1918)?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Mal-ware Controls</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Do you scan all emails for viruses?	<input type="checkbox"/>	<input type="checkbox"/>	
Is there explicit policy requiring anti-virus software on networked computers?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you have centralized administration of virus control, such as distribution of signature updates, reporting, policy enforcement and vendor management?	<input type="checkbox"/>	<input type="checkbox"/>	
Are rules established for scanning outside software?	<input type="checkbox"/>	<input type="checkbox"/>	
Does the virus checking software run in the background with established frequency of scanning etc	<input type="checkbox"/>	<input type="checkbox"/>	
Are end-users prevented from disabling anti-virus software on personal computers?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you allow installation of personal and non-corporate approved software on network computers?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Disaster Recovery and Business Continuity</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Are the recovery procedures tested for efficacy?	<input type="checkbox"/>	<input type="checkbox"/>	
Are manual backup/restore procedures documented and practiced in	<input type="checkbox"/>	<input type="checkbox"/>	

case of automatic backup failure?			
Can you meet recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for all products and services contracted with MassMutual?	<input type="checkbox"/>	<input type="checkbox"/>	
Is there a Business Continuity Plan?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Monitoring</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Do you monitor the security/policy violations and application/networked services availability?	<input type="checkbox"/>	<input type="checkbox"/>	
Do you log successes and failures to access?	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Accounts Management &amp; Access Control</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
How will MMFG data be secured at your site?			
Will MMFG data be accessible from Internet?	<input type="checkbox"/>	<input type="checkbox"/>	
Who will have access to MMFG data?			
How do you prevent other clients accessing MMFG data?			
How and where are user IDs and Passwords stored? How secured?			
Will the access credentials be encrypted when passing through public network?			
Do you employ any mechanisms that facilitate secure data exchange?			
<b>E-Commerce (applicable if vendor conducts business on-line)</b>	<b>Yes</b>	<b>No</b>	<b>Comments</b>
Are the following maintained in e-commerce system:			
• Confidentiality?	<input type="checkbox"/>	<input type="checkbox"/>	
• Authorization?	<input type="checkbox"/>	<input type="checkbox"/>	
• Non-Repudiation?	<input type="checkbox"/>	<input type="checkbox"/>	
• Transaction Integrity?	<input type="checkbox"/>	<input type="checkbox"/>	
• Access codes encryption in storage and transmission?	<input type="checkbox"/>	<input type="checkbox"/>	

**Additional information and comments:**