



# Vendor Risk Management Assessment Services

## **Key Contact**

Jon Bosco, Managing Partner  
122 East 42nd Street  
Suite 608  
New York, NY 10168  
**Office:** 646-205-9961  
**Cell:** 917-939-2873  
**e-Mail:** [jbosco@edeltaconsulting.com](mailto:jbosco@edeltaconsulting.com)  
[www.edeltaconsulting.com](http://www.edeltaconsulting.com)

## **Key Contact**

Anthony D'Amato, Partner  
122 East 42nd Street  
Suite 608  
New York, NY 10168  
**Office:** 646-205-9962  
**Cell:** 516-903-2967  
**e-Mail:** [adamato@edeltaconsulting.com](mailto:adamato@edeltaconsulting.com)  
[www.edeltaconsulting.com](http://www.edeltaconsulting.com)



# VENDOR RISK MANAGEMENT ASSESSMENT SERVICES

EXPERT KNOWLEDGE OF THE INDUSTRY AND ITS CHALLENGES

## Overview

There continues to be increased risk associated with vendors and third-party providers in highly regulated industries such as financial services and healthcare, in media and retail, and any organization that is relying on third-party vendors to manage operations and processes.

These vendors include not just data management, IT and security providers, but also facilities environmental and power controls, along with any vendors that may have access to your network, data or facilities.

The list of standards and regulations with third-party risk implications include, but are not limited to the: Consumer Financial Protection Bureau (CFPB) regulations, ISO 27001/2, PCI Security Standards Council's data security standards, Office of the Comptroller of the Currency (OCC) Third-Party Risk Guidance, and NIST's Cybersecurity Framework.

Recent security breaches at several large companies has resulted in regulatory (e.g., Public Accounting Oversight Board - PCAOB) scrutiny of the way personal data is managed in an organizations IT environment.

## There are many questions to be answered as part of the vendor management process (examples):

- What are the service provider (vendor's) security precautions concerning transactions and confidential information?
- What are the vendor's standards, policies, and procedures relating to internal controls, record maintenance, background checks and physical security of its operation's?
- What kind of internal audit is performed at the vendor?
- Are there internal audit reports or internal control evaluations available for review by your organization?
- Does the vendor have contingency plans in place, and are those plans adequate?

## Additionally, we find that:

- Financial services organizations tend to have relatively mature vendor risk management programs compared to other companies.
- Organizations in the insurance industry are at a lower level of maturity in their vendor risk management program compared to the financial services industry.
- Different industries and organizations, having mature program governance capabilities, as well as established policies, standards and procedures for vendor risk management, are considered fundamental steps.

# Our Vendor Risk Management Maturity Assessment Methodology

Our approach assess a number of factors within an organization related to vendor risk. These include, but may not be limited to:

- Program Governance
- Policies, Standards, Procedures
- Contracts
- Vendor Risk Identification and Analysis
- Skills and Expertise
- Communication and Information Sharing
- Tools, Measurement and Analysis
- Monitoring and Review

For each of the factors within an organization, we apply a Vendor Risk Management Maturity (VRMM) rating, as follows:

1. Do not perform (not applicable)
2. Evaluating and assessing the need
3. Planning to implement
4. Process is in place
5. Process is in place and operating effectively
6. Continuous improvement implemented





# Vendor Risk Management Assessment Services

Expert Knowledge of the Industry and its Challenges

Based on the results of the VRMM Assessment, we will provide your organization with practical recommendations and solutions to move your Vendor Risk Management process forward to the next Maturity Level, using our extensive industry-wide financial, operational and information technology experience and knowledge.

To achieve this goal, eDelta combines extensive experience in multiple industries, with highly qualified audit and compliance professionals.

## **Our Risk Management Assessment Services include, but are not limited to, the following areas:**

- Vendor Risk Management (VRM) Framework
- Affiliate Vendor Risk Management Policy
- Performance of Risk Assessment, Due Diligence, Contracting and Oversight
- Management and Monitoring of Vendor Risk
- VRM Governance and Policy
- Risk and Control Assessment for Vendor Risks (VR)
- Variations of Risks and Controls
- Risk Indicators (KRIs), Key Control Indicators and (KCI)s, etc.
- Vendor Supply Chain Risk and Controls
- Vendor Contracts and Service Level Agreement (SLAs)
- Communication of Vendor Risk
- IT Related Vendor Risks
- Data CIA (*Confidentiality, Integrity, Availability*)
- Control Testing Methodologies (examples):
  - Encryption
  - Access controls
  - Vendor CIA controls
  - Trans-border transmission of privacy-related information
  - Applicable Laws, Regulatory Requirements and Compliance Testing Methodologies
  - Gramm-Leach-Bliley Act (GLBA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Sarbanes Oxley (SOX)
  - Bank Service Company Act (BSCA)
  - Compliance with Dodd-Frank Consumer Finance Protection Bureau (CFPB and Other Legal and Regulatory Considerations)
  - Independent Service Provider Reports (SSAE16 and ISAE 3402, SOC 2, SOC 2 – Trust Services Principles)
  - Awareness and Training for Vendor
  - Interfacing Employees
  - Global/Cross-Border Outsourcing Policies
  - Business continuity and contingency plans for the business function in the event of problems affecting the third party's operations



## PROFESSIONALS EXPERIENCE (PARTNERS)

EXPERIENCE, KNOWLEDGE, SERVICE DELIVERY

### **Jon Bosco, Partner**

Jon helped establish eDelta Consulting, Inc. in 2000 with former Ernst and Young, LLP alumni in order to provide a wide-range of Internal Audit, Technology and Information Security services to Fortune 500, medium and small public and private companies.

For more than a decade, Jon has been evaluating information systems and associated business processes in major industries, including financial services, retail and entertainment. He has assisted the internal audit department of several Fortune 500 companies in developing and executing plans to mitigate technology and business risks. Jon has strong project management, organizational and technical skills.

Prior to eDelta, Jon was a Manager in Ernst & Young's New York ISAAS Group. As a manager at Ernst & Young, Jon managed various external financial audits across various industries. Jon is a frequent speaker on issues as diverse as Sarbanes Oxley, information security, disaster recovery, business continuity planning, corporate risk assessment, and Computer Assisted Audit Techniques (CAATs). He has an expert knowledge of technology challenges and their related regulatory and compliance impact on major corporations.

Jon is Certified Public Accountant and an active member of the Information Security Audit and Control Association (ISACA), and the Information Systems Security Association (ISSA).

Jon holds a Bachelor's degree in Computer Science and Masters in Accounting from the State University of New York at Albany.

### **Anthony D'Amato, Partner**

Anthony helped establish eDelta Consulting, Inc. in 2000 with former Ernst and Young, LLP alumni in order to provide a wide-range of Technology and Information Security services to Fortune 500, medium and small public and private companies.

Anthony has more than 25 years of experience in information technology consulting and information systems auditing. His industry background is across multiple industries. Anthony is an expert in IT operations and controls, and in developing operational policies and standards.

Prior to eDelta Consulting, Anthony was a Senior Manager in Ernst & Young's New York ISAAS Group, with extensive experience in managing and directing large engagements with multiple staff. He was involved in the development of planning, staffing, budgets, proposals and presentations to senior management.

Anthony's area of expertise include: Data Center Operations, Operating Systems experience and knowledge with mainframe, midrange and client server systems, developing policies and standards for all areas in Information Technology, including Data Security, Operations, System Development and Disaster Recovery.

Anthony is experienced in dealing with regulatory requirements for: FFIEC, New York State and FDICIA guidelines, including Sarbanes Oxley, HIPAA, and Gramm-Leach-Bliley. In addition, Anthony performed numerous SAS 70/SOC reviews for major financial service clients while at Ernst & Young.

Anthony has Graduate Certificate in Networks & Telecommunications from Pace University, holds BS in Mathematics from the State University of New York, and an AAS in Electrical Engineering Technology.



# EDELTA'S VENDOR MANAGEMENT SOFTWARE

## VENDABILITY - STRUCTURED RISK ASSESSMENT PLATFORM

The screenshot shows the top portion of the Vendability website. At the top left is the Vendability logo. To its right is a navigation menu with links for BENEFITS, FEATURES, PRICING, MEMBERS, CONTACT, LOGIN, and SIGN UP. Below the navigation is a hero section with a background image of hot air balloons. On the left side of the hero section, there is a text block describing the platform and a 'GET STARTED NOW' button. Below the hero section is a 'Benefits' section with a background image of a hand giving a thumbs up. This section contains a paragraph of text and another 'GET STARTED NOW' button.

**Vendability** is a cloud-based platform that allows Companies and Vendors to efficiently and effectively exchange critical risk and control information, real time and/or on a scheduled basis, integral to their business relationship and services provided.

[GET STARTED NOW](#)

### Benefits

**Vendability** is designed to provide a structured risk assessment platform for Customers and Vendors using industry standard approaches. The community of members, whether customers or vendors, can learn, use and re-use industry accepted assessment questionnaires and responses, thus, facilitating in the accomplishment and approval of assessments and risk ratings.

[GET STARTED NOW](#)



# EDELTA'S VENDOR MANAGEMENT SOFTWARE


VENDABILITY - PROVIDING INDUSTRY TEMPLATES FOR VENDORS & CLIENTS

The screenshot shows the Vendability software interface. At the top left is the Vendability logo and the company name 'eDelta Consulting, Inc.'. A navigation sidebar on the left contains 'Dashboard', 'Risk Assessment', and 'Reports'. The main content area is titled 'Industry Templates' and features a section for 'AITEC Standards' with a 'Copy' button. This section is divided into 'Control Categories' and 'Risk Categories'. The 'Control Categories' list includes items like 'DDQ-01-Information Security Policy' through 'DDQ-D12 System and Services Acquisition'. The 'Risk Categories' list includes 'Availability', 'Confidentiality', 'Integrity', and 'Regulatory'. To the right, there are two additional sections: 'Industry Templates' with a list of templates like 'AITEC Standards' and 'HIPAA/WHITECH', and 'Upcoming Webinars' with titles like 'Introduction to Risk Management' and 'Risk Management'. Below these is a 'Links' section with titles like 'Addressing Procyclicalty' and 'Bankers Banquet'. At the bottom, there is a 'Control Questions' section and a table header for 'Expand/Collapse Control Category'.



# EDELTA'S VENDOR MANAGEMENT SOFTWARE

## VENDABILITY - SAMPLE VENDOR CONTROL QUESTIONNAIRE

 Company: eDelta Consulting, Inc.

Dashboard  
Risk Assessment  
Reports

Maintain Control Questions

Customer Template : EdeltaTemplate - Edelta Consulting Template

Select Control Category:

#	Control Question	Response	Risk Categories
1	Are there policies in place as to when to alert clients of a security incident?	<input type="radio"/> Yes <input type="radio"/> No	Availability
2	Briefly describe the process used to determine when a client should be notified?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A	Confidentiality
3	Does your company have formally documented information security policies and procedures that are approved by senior management (CXO Level or equivalent) communicated to staff reviewed at least annually and published appropriately as to be available for reference and application?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A	Integrity
4	Is the IT security policy reviewed on a periodic basis to determine if the controls are operating as intended?	<input type="radio"/> Yes <input type="radio"/> No	Regulatory
5	Does senior management approve changes to the Information Security Policy?	<input type="radio"/> Yes <input type="radio"/> No	Confidentiality
6	Are changes and improvements to the IT Security Policy applied as needed and documented within a change log?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A	Confidentiality
7	Does your company have a designated person responsible for oversight of the information security program?	<input type="radio"/> Yes <input type="radio"/> No	Confidentiality