justin greis

CASE STUDY: VENDOR RISK MANAGEMENT

HEALTHNEXT CARE SYSTEM

ASSIGNMENT OVERVIEW

Summary:	As a team, present the proposed solution to the case. The presentation should lay out clear recommendations for how management should address the problem.
Presentation Deliverable:	Case study presentation (in Microsoft PowerPoint format)**.**
Executive Briefing Deliverable:	Single page case study executive briefing (in Microsoft PowerPoint format).

BACKGROUND

A series of business incidents, due to internal and external factors, have revealed significant gaps in HealthNext Care System's Vendor Risk Management (VRM) practices. As a result, Samantha Currie, the VP of the Vendor Management group, has come under scrutiny from senior level executives including the CFO, Legal, Compliance, Enterprise Risk Management and Internal Audit. In a presentation to the senior executives and stakeholders, Currie was given approval to launch a VRM Improvement Program to address the noted gaps and strengthen their capabilities. You have been engaged by Currie to help improve the way HealthNext manages its vendor risks.

HEALTHNEXT CARE SYSTEM

Founded in 1946, HealthNext Care System prides itself on providing quality medical care to its patients. It quickly grew to a $16 billion national healthcare provider and currently operates as a hospital system as well as a research facility and education center for medical students.

HOSPITALS

HealthNext serves over 1.5 million patients on an annual basis and offers a comprehensive array of medical services. The doctors and practitioners are paid a lucrative salary that is consistently 20% above market and their salary does not vary based on the amount of service provided. As a result, practitioners prefer to spend more time attending to patient needs versus opposed to taking on more cases. This results in customized and specialized care for patients and is the primary reason why HealthNext is consistently rated as one of the best hospital systems in the United States by both patients and employees alike.

HealthNext has over 100,000 employees and includes physicians, scientists, doctors, residents, fellows, researchers, corporate staff and administrative staff. HealthNext is headquartered in Los Angeles, California. Shown below is a location chart for HealthNext.

Facility Location	Hospital	Research Facility	Education Center
Los Angeles, CA (HQ)	✓	✓	✓
Boise, ID	✓		✓
Honolulu, HI	✓		✓
Tucson, AZ	✓		✓
Dallas, TX	✓		✓
Minneapolis, MN	✓		✓
Chicago, IL	✓	✓	✓
Providence, RI	✓		
Miami, FL	✓	✓	✓
Birmingham, AL	✓		

RESEARCH FACILITIES

HealthNext employs a significant number of researchers in multiple locations to lead the cure and treatment of disease, improve clinical quality of care, and translate of findings from the laboratory to the clinical practice. They employ around 600 physicians and research scientists along with 3,000 allied health personnel and student practitioners. Their research initiatives have led to more than 5,000 research publications and medical review articles in peer-review journals. HealthNext scientists hold thousands of patents and jointly collaborate with large pharmaceutical companies on clinical trials and new drug testing. HealthNext has seen tremendous success from this model and relies on a growing portion of its revenue stream from collaboration and research conducted with other companies.

EDUCATION CENTERS

Education is one of the founding values for HealthNext. Educating medical students and providing them with on-the-job training is a big part of the investment HealthNext makes in medical education. It is also another source of revenue and a way for HealthNext to recruit young physicians and scientists pursuing a career in medicine. HealthNext also invests significantly in medical schools across the country and has formed partnership relationships with the University of Arizona and in the University of Colorado.

VRM RELATED DEPARTMENTS WITHIN HEALTHNEXT

Procurement, Legal and Vendor Management are the three departments within HealthNext which focus on Vendor Risk Management.

PROCUREMENT

The Procurement organization is responsible for sourcing, selecting and approving vendors. The group is led by Steve Colbert, Vice President of procurement operations at HealthNext. The Vendor Management responsibilities of the Procurement group are:

- Initiate vendor requisition

- Approve vendor requisition
- Initiate purchase order to vendor
- Maintain vendor master file
- Record vendor invoices
- File vendor change requests
- Lead request for proposals and request for information processes

Procurement also manages the vendor management system which is on an MS Excel spreadsheet. They have set up a vendor selection process.

LEGAL

The Legal Department is led by John Nash. Its vendor management responsibilities are to review and approve/reject any new or renewed contract to safeguard HealthNext against any litigation. This includes managing and executing the vendor master agreement to cover all legal obligations. Every contract entered through the procurement process needs to be reviewed and approved by Legal. Their tasks, while recognized as very important, are also considered burdensome by the business partners who want faster reviews and longer contracts to lock down discounted rates from their vendors.

VENDOR MANAGEMENT

The Vendor Management group, led by Sam Currie, is responsible for managing the daily operations of the vendors with respect to HealthNext. For services vendors, this includes managing projects, verifying and upholding quality of service and facilitating communication among relevant stakeholders. For product vendors, the group works to ensure that the product is running smoothly and that the vendor is compliant with all legal and regulatory requirements as defined by HealthNext.

In the past, the lack of documented roles and responsibilities and training procedures for employees has led to miscommunication between the procurement and vendor management groups. As a result, the vendor selection process is often conducted in silos. This results in inconsistency in the vendor selection and vendor due diligence processes. The risk and compliance management group is also decentralized and disconnected from the three groups described above. So, it is a tedious job for the group to manage and share vendor information with different business units. Compliance tracking and reporting for vendors is manual and generally conducted through email.

KEY STAKEHOLDERS

STEVE COLBERT, VP PROCUREMENT

Steve Colbert has worked for HealthNext for the past 23 years. He has risen through the ranks in the organization to become a Vice President of the procurement group. He has extensive experience in managing and leading the vendor selection process (product vendors and service vendors). Colbert majored in marketing from Michigan State University and received an executive MBA from the Stanford University. He takes pride in leading a group of people who focus on performing appropriate due diligence on the company's vendors but understands that there are some barriers that need to be overcome in order to make his group relevant to their business stakeholders. He is currently planning a company-wide campaign to increase awareness of this particular service (vendor due diligence) provided by his group.

JOHN NASH, VP VENDOR LEGAL RELATIONS, LEGAL

John Nash has been practicing law throughout his life focusing specifically on corporate law and contracts. He had his own partnership based out of Boston with several large corporations as clients before he was offered the job in the legal department. Nash is well respected in the organization and it is well known he will be the next General Counsel of HealthNext within two years upon retirement of his boss. Nash is very thorough in his evaluation and drafting of vendor contracts. Nash calls himself an "old school lawyer" and likes to do business "by the book". Nash has run into many difficult circumstances where employees draft and execute loopholes in vendor contracts. Nash has made it his personal mission to standardize the terms and conditions of every contract and is in the middle of a comprehensive contract review to incorporate new terms and conditions, especially those that cover expectations around vendor privacy and information security.

SAMANTHA CURRIE, VP VENDOR MANAGEMENT

Samantha Currie ("Sam"), like Colbert has also risen through the ranks in the organization. She joined HealthNext after graduating with a degree from University of Minnesota with a major in supply chain and operations. She has risen significantly faster through the organization than most of her colleagues. She is considered to be a "maverick" when it comes to dealing with vendors. She takes an "us versus them" attitude and often places difficult demands on the vendors that adds overhead prolongs vendor negotiations. This characteristic trickles down through her team and is seen as a barrier to getting work done at HealthNext. Employees often do their best to go around Currie and manage the vendor relationships themselves.

CURRENT VENDORS

VENDOR 1: INFINITY CLOUD STORAGE

Infinity is a cloud services provider who sells cloud Infrastructure as a Service (IaaS) services. Organizations are provided with servers and data centers to host their data on the cloud. Infinity is reputed for a service called the "Cache Cloud." Through this service, Infinity installs local servers in their client's data center which synchronizes with the Infinity server in the cloud. This hybrid cloud model makes frequently used documents, easier and faster to access. It also provides redundancy and fail-over in the event that the customer's data center goes down. In the rare event Infinity goes down, the client will fall back to its own data center. Infinity has a niche in providing their services to small to medium sized businesses but has plans to grow to large, enterprise customers. HealthNext is by far their largest client. Infinity won this deal mainly through established relationships with senior executives in HealthNext.

VENDOR 2: EPIHEALTH PATIENT MANAGEMENT SYSTEM

EpiHealth provides a patient management system and electronic medical records to HealthNext. This software helps HealthNext doctors manage their patients' health information. This system stores a significant amount of Personally Identifiable Information (PII) and Protected Health Information (PHI). EpiHealth is a Dallas based company and has support offices in 20 different states with a global client base. Apart from the legacy Patient Management System, they provide clients with Hospital Scheduling Systems, Ambulatory Management Systems and Dental Record Solutions. EpiHealth is a recognized leader in their industry and is seen as the "gold standard" in electronic medical records software.

VENDOR 3: WELLNESS CLAIMS PROCESSING SYSTEM

Wellness Claims Processing provides HealthNext with a Claims Processing system to enable health insurance reimbursement for the care they provide. This system handles a significant amount of financial information specific to patients and in many case relatives of patients. Along with financial information this systems also stores information that can be classified as Personally Identifiable Information (PII) such as patient names, social security numbers and addresses.

BUSINESS PROBLEM

A series of incidents served as a wake-up call for HealthNext's leadership to look at their vendor management capabilities more closely. It was soon realized that the lack of a formal Vendor Risk Management (VRM) program was leading to alarming gaps in controls necessary for ensuring business continuity, risk mitigation and cybersecurity. These incidents highlighted the need for developing a VRM program to standardize the vendor selection processes and facilitate tighter governance around vendor oversight and compliance.

LACK OF PLANNING STALLS RECOVERY FROM NATURAL DISASTER

Last year, HealthNext's day to day operations were crippled due to the devastating effect of hurricane the northeast area of the country. Infinity Cloud Company, who had outsourced their data centers to a company based in New Jersey, switched over to the back-up generator power because electricity was down in the Northeast corridor of the United States. However, restoration of power took longer than expected and generators soon ran out of fuel. To make matters worse, HealthNext's data center was also hit with a power outage, and within 24 hours had to resort to manual, paper-based methods to continue serving their patients and customers. All systems were down for two days, including Infinity and EpiHealth. It was later discovered through an audit that Infinity did not have a documented disaster recovery plan. Typically, multiple site disaster recovery designs provide a higher level of zero data loss over long distances. However, Infinity's back-up data center was located within the same region that was impacted by the hurricane so the failover was effectively worthless.

HACKING INCIDENT CAUSES LOSS OF CUSTOMER DATA PRIVACY

Earlier this year in April, EpiHealth's network server was compromised by hackers who illegally accessed 156,000 patient electronic health record data. The data included patient names, social security numbers, date of birth, home addressees, account numbers, and healthcare services and related protected health information (PHI). HealthNext did not discover the breach for five months and was immediately slapped with a fine of $2.5 Million by the state attorney general in accordance with Health Insurance Portability and Accountability (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. HealthNext only found out about the breach from a patient that happened to be Googling her name and found a text file with thousands of patients' information posted on a suspicious looking website. HealthNext also had to issue a notice to all affected customers leading to reputational damage and costly remediation efforts.

Upon investigation, it was determined that HealthNext did not carry out a risk assessment during outsourcing to EpiHealth. HealthNext was moving from its internally hosted instance of EpiHealth to EpiHealth's EpiCloud product which was designed as a subscription-based software-as-a-service medical records software platform. HealthNext was conducting a pilot with 200,000 patients as part of the trial move

to EpiCloud. Unfortunately, HealthNext did not perform any due diligence on this new product and relied solely on EpiCloud's security policies, without verifying their level of compliance or level of effectiveness. It was also discovered that there was a lack of clarity on roles and responsibilities, especially when it came to incident management and recovery. Per their contract, EpiHealth/EpiCloud assumed no responsibility of any financial impact due to unauthorized access of data due to unauthorized access or security attacks, thus was not subject to the fine. This contract was not reviewed by Legal.

SOFTWARE GLITCH IMPACTS QUALITY OF SERVICE DELIVERY

In August, HealthNext's claims processing system was down for six consecutive days. The system, managed by Wellness Claims Processing System, delivered a software service pack update that caused a series of slowdowns and eventual outages. The system slowed when claims examiners tried to perform simple transactions with claims files, such as search, update, save or retrieve. The problem was aggravated due to the fact that Wellness Claims did not maintain a regular release calendar and maintenance schedule. The system was eventually restored and the patches rolled back based on incremental storage backups.

CALL FOR ACTION

These incidents were a wake-up call for the executives that their vendors weren't as stable as they thought. The Vendor Management group has not been able to effectively manage the sheer spread of vendors along different lines of the business. The incidents also exposed HealthNext's heavy dependency on their vendors and failures on their part presented a risk to the company's operations.

As the VP of Vendor Management, Currie understands that she needs to create awareness within the organization about the threats posed to business continuity due to the lack of Vendor Risk Management (VRM). Her goal is to set up a formal VRM program to standardize the due diligence process carried out by the Procurement group. She aims to have a standardized process with defined parameters for vendor selection based on the nature of service or product provided, type of data handled and criticality to business operations. This will help remediate the issues introduced due to ineffective vendor risk management. To set up the program and facilitate dialogue among the stakeholders, she organized a meeting with the CIO of HealthNext along with department heads from Procurement, Legal and other business units to discuss her vision. The CIO recognized the need to improve Vendor Risk Management (VRM) discussed the importance of integrating it into the overall Enterprise Risk Management framework. She also gained support and willingness of participation from other stakeholders.

While getting endorsed was a step in the right direction, Currie is concerned about the cultural and political barriers that may inhibit the success of the project. The IT leaders in the business unit are very autonomous and gaining their support is going to be a challenge. The process set up by Procurement has not been effective and there is a need to have a standardized vendor selection and renewal process.

She is also concerned about the vendors' lack of responsiveness and ownership to critical risks and wants to build a culture of accountability. She feels that HealthNext needs to re-assess the vendors and identify risks, issues and develop corresponding mitigation steps.

To get organized, Currie has hired a team of consultants to help her put plan an approach and execute some of the remediation activities. The team met with Currie to understand the scope and the endorsed vision and is planning to conduct a kick-off meeting.

TOOLS AND FRAMEWORKS

- **Exhibits One and Two** - During a previous engagement for a major Agricultural and Biotechnology Company, your team developed these frameworks to build out the VRM program. Exhibit One describes the organizational structure used to set up the program and provide oversight. Exhibit Two maps the Vendor Lifecycle Management (VLM) process to key activities and stakeholders. Since then, this framework has been successfully leveraged multiple times to enhance VRM program governance and improve operational efficiencies. Modify these frameworks based on the facts of the case and use them as a platform to launch the VRM program at HealthNext.
- **Exhibit Three** - Critical to any Security Risk Assessment (SRA) program is the ability to manage the life cycle of risk assessment processes. In collaboration with the Procurement team, Sam has outlined a Vendor Security Risk Assessments (VSRA) process for HealthNext's vendors which aligns with its objectives. This process includes continuous prioritization, assessment execution, follow up and reporting. Her plan is to use this framework to conduct a proof of concept on a handpicked group of vendors and present the results of the assessment to the CIO to build support for the VRM group. Sam realizes that strong project governance predicates the delivery of this project. Consistent and frequent monitoring and communication of engagement activities with leadership will be critical to keeping work focused and relevant. It will also help to reduce lag time between requesting and receipt of information.
- **Exhibits Four and Five** - HealthNext has business relationships with hundreds of vendors. To conduct a risk assessment for every vendor in the landscape will be time consuming and expensive. Segmentation based on nature of services provided and type of data handled makes the vendor universe manageable. Risk tiers define how an individual supplier's risk profile is managed during its lifecycle. Use Exhibits Four and Five to segment HealthNext's vendors to ensure that the required assessment effort aligns with the potential risk exposure. While developing parameters for each tier, take into account how it will be put into operation.
- **Exhibit Six** - Most often, Accounts Payable (A/P) is the authoritative source for building the vendor inventory. Sam asked her team to perform an analysis of A/P spend (invoices) and the contracts repository to determine an exhaustive list of vendors. She also interviewed business stakeholders to gain an understanding of current vendor relationships. Exhibit Six is the group of suppliers handpicked by Sam and represents a comprehensive cross section of HealthNext's vendor universe.
- **Exhibit Seven** - After several meetings with other business stakeholders such as audit managers, vendor relationship managers and Information Security, Sam has developed a list of key risk areas. In order to capture the true risk profile for HealthNext's suppliers, it is important to align the risk assessment questionnaires with these risk areas.
- **Exhibit Eight** - After conducting an assessment, the results are analyzed and the vendors are asked to take remedial measures to mitigate the identified risks. Exhibit Eight provides a matrix which maps remedial action to the level of risk exposure. Use this exhibit to come up with a remedial action plan for the three vendors described in the case.

YOUR TASK FOR THIS CASE – PRESENTING TEAMS

You are the consultant team hired by Currie to execute the VRM Improvement Project. In preparation for the kick-off meeting, prepare your proposed solution to address the business problems described below.

- Sam needs your help on two primary action items:
  - To establish a Vendor Risk Management (VRM) program. Its main components will be:
    - A Vendor Lifecycle Management (VLM) process
    - A framework to perform Vendor Security Risk Assessments (VSRA)
  - To integrate the VRM program with Enterprise Security Risk Management (ESRM)

- The following questions need to be addressed while setting up the VRM program
  - What should be the composition of the steering committee responsible for setting up the program and which departments need to be involved in the decision-making process?
  - Once the program is established, what kind of user training should be provided to deploy the program within HealthNext?
  - What parameters should be established to segment (existing and newly added) vendors based on criticality of function and impact to the business?
  - Based on this segmentation, how will the risk assessment process change for vendors classified into different tiers?
  - How will vendors be evaluated for risk in a RFP, in a contract renewal, periodically and on request of a business stakeholder?
- Your solution should, at a minimum, include the following-
  - A plan of action for implementing an enterprise level strategy for VRM (use Exhibit One).
  - An outline for communication and formal training for the VRM program.
  - Procedures to enhance end to end vendor lifecycle management (use Exhibit Two to prepare a swim-lane diagram to map each phase of the VLM process to key activities and stakeholders).
  - Segmentation strategy for HealthNext's vendor landscape based on the parameters defined (use Exhibits Four and Five).
  - 5 questions (to be included in the risk assessment questionnaire) for each risk area identified for HealthNext (use Exhibit Seven) along with examples of documents that can be attached as proof.
  - A plan of action for performing a risk assessment (use Exhibit Three) on the three vendors (described in the case) and then developing a strategy for remediating the identified risks based on the final risk ratings (use Exhibit Eight).
  - A framework for monitoring and tracking compliance requirements communicated to vendors
  - An analysis of the costs involved in setting up this program (hardware, software, training and reporting and personnel costs).
  - Types of KPIs (Key Performance Indicators), KRIs (Key Risk Indicators) and reports to help create visibility and oversight for the VRM program.

YOUR TASK FOR THIS CASE – ALL OTHER TEAMS

CASE STUDY EXECUTIVE BRIEFING

As noted above, Currie has organized a meeting with the CIO and department heads from Procurement, Legal, and other business units to discuss her vision on setting up a formal VRM program. In order to make for a productive meeting, Currie wants to distribute materials prior to the meeting that the attendees can use to prepare but Currie also wants to be able them as a guide during the meeting. Currie has asked you (the consultant) to develop the executive briefing materials and informed you that a single slide placemat with text and visuals that analyzes the case and illustrates what the high-level plan is going forward would work really well.

GENERAL CASE STUDY GUIDANCE

At a minimum, the solution to your case study should include the criteria below. Though not mandatory, you may use this as a format and general flow for your case study.

- A clear and concise background of the facts of the case.
- Key issues, observations and complicating factors that contribute to the root cause business problem at hand.
- A clear statement of the business problem to be solved.
- An overview of the solution and its components. The solution should address the key tasks outlined for you in the case.
- Demonstration of sufficient analysis that led you arrived at your solution.
- Clear recommendations for how the solution should be implemented or deployed.
- A timeline for execution of your recommendations.
- A budget or cost model for implementing your solutions. Be sure to include the cost to build and deploy your solution and the cost to run and operate your solution after it is built.
- An analysis of the risks, issues, key assumptions and any mitigating factors you will employ to minimize the likelihood and/or impact.

You have been asked for a lot of detailed information to solve this case. The trick will be to package this up into a digestible executive presentation your audience can understand. Detailed supporting information can be included in an exhibit in the appendix of your presentation.

Your case study solution should also include:

- Citation of key sources in the form of end notes cited in your appendix.
- Application of standards and leading practices that help to inform your solution.

A few tips and tricks for solving this case:

- Company financials have intentionally not been provided to you for this case. To build your model about sizing of the company, please conduct your own independent research and find similar peer companies.
- Feel free to make assumptions that support your conclusions. Be sure to state your assumptions in an exhibit in your appendix. Your assumptions should not significantly alter the facts of the case; rather, they should support the recommendations by filling in the missing pieces of information in the case.
- You should NOT simply copy/paste from COBIT or any of the other standards. The key is to use the standards to help you solve the case. Remember: standards are NEVER the answer on their own; they must be applied to the business problem.

APPENDIX

EXHIBIT ONE: ESTABLISHING A VRM PROGRAM

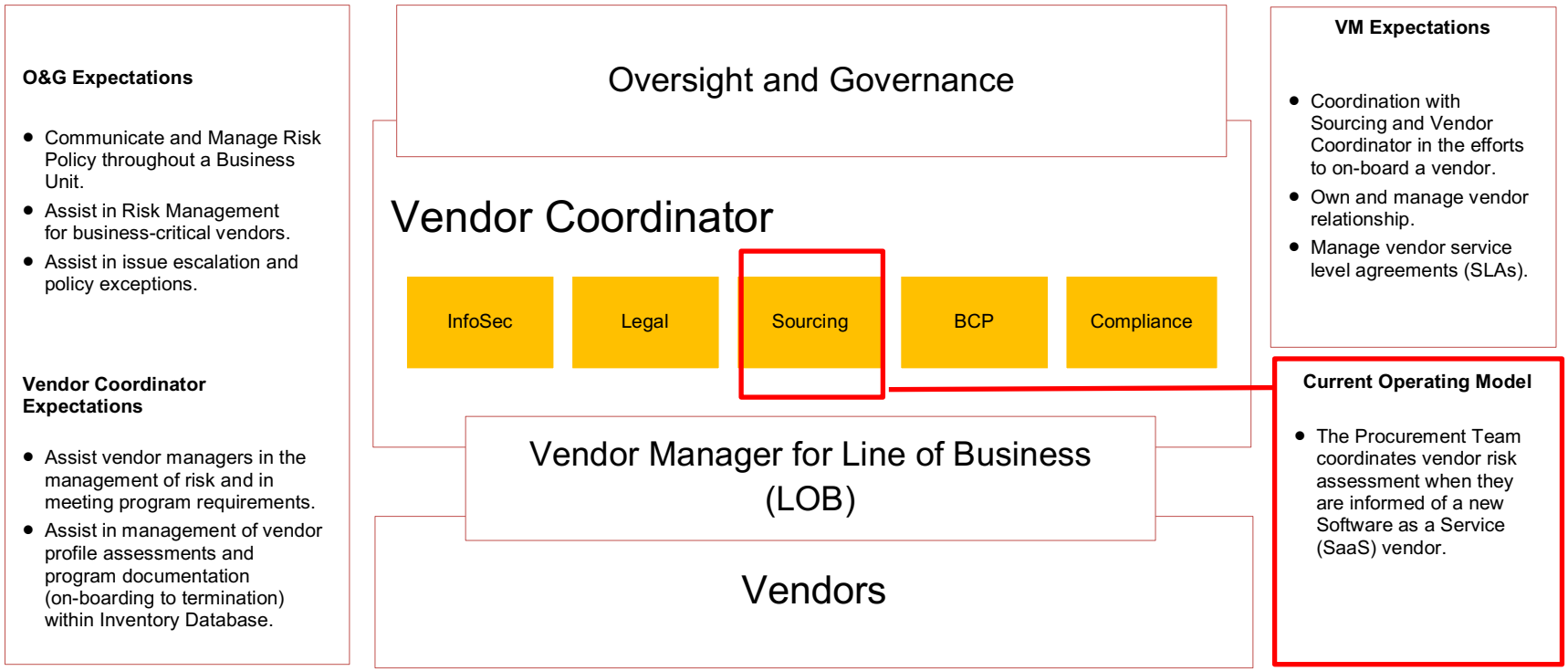


EXHIBIT TWO: END TO END VENDOR LIFECYCLE MANAGEMENT (VLM)

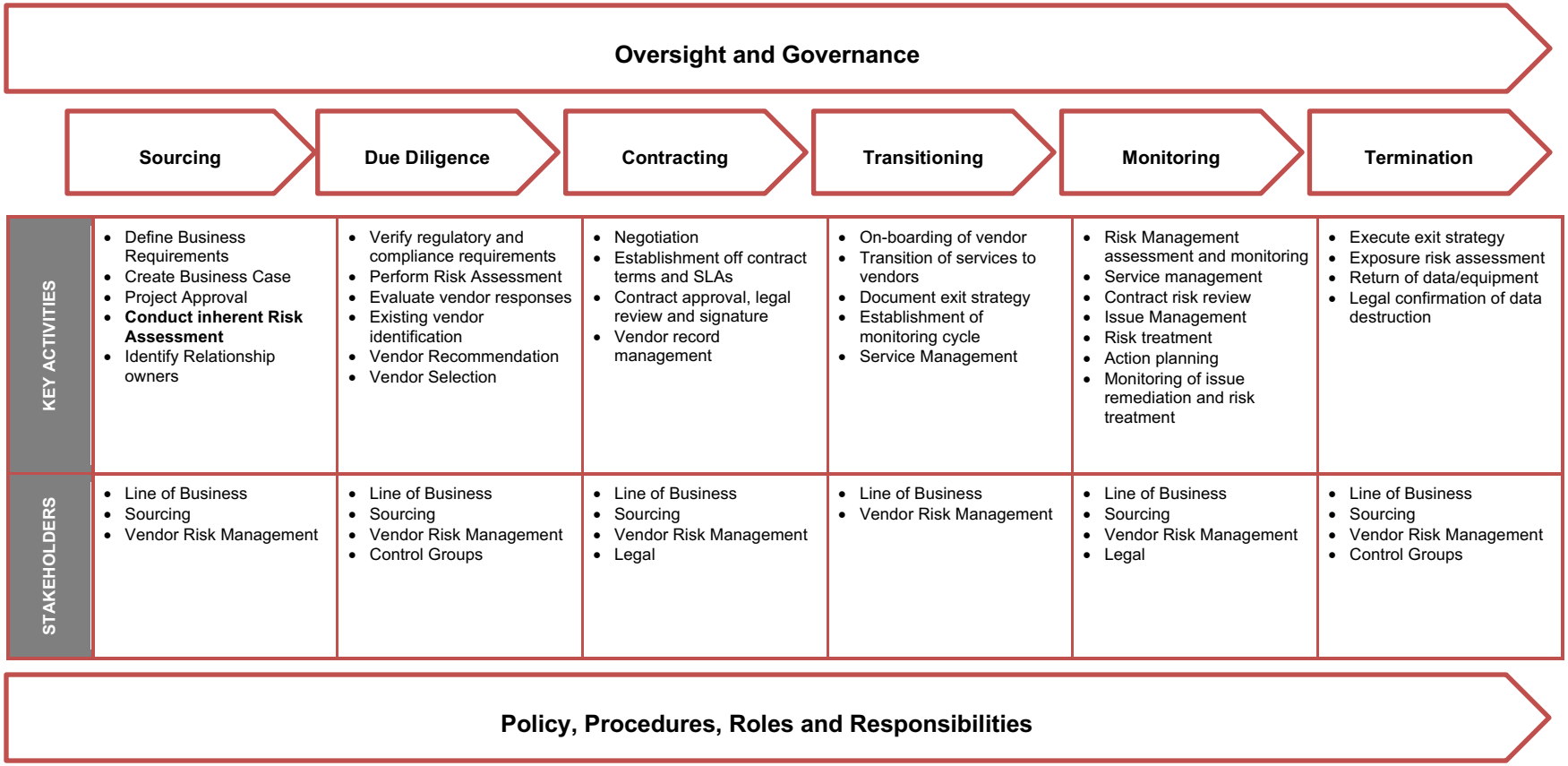
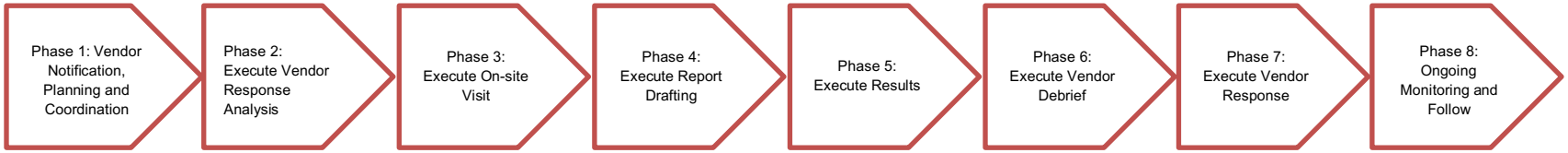


EXHIBIT THREE: VENDOR SECURITY RISK ASSESSMENT (VSRA)



Phase 1: Vendor Notification, Planning and Coordination	Phase 2: Execute Vendor Response Analysis	Phase 3: Execute On-site Visit	Phase 4: Execute Report Drafting	Phase 5: Execute Results	Phase 6: Execute Vendor Debrief	Phase 7: Execute Vendor Response	Phase 8: Ongoing Monitoring and Follow
Reconcile vendor master list, schedule on-site visits **Input** • Leadership determines vendor list, approves project documents and initiates vendor communication **Output** • Vendor Master List • Schedule onsite visit • Vendor Communication • External Memo • Preliminary Agenda • Assessment Preparation List • Questionnaire	Review completed questionnaire, compare to expected results and complete preliminary assessment evaluation **Input** • Completed vendor questionnaire **Output** • Vendor On-site agenda • Evaluated vendor responses • Preliminary Vendor Security Assessment Evaluation Report	Complete on-site visit, perform a walkthrough of the facilities and discuss information security program highlighting identified areas of concern **Input** • Vendor On-site agenda • Evaluate vendor responses (manually and with automated tool scoring) • Preliminary Vendor Security Assessment Evaluation Report **Output** • Documented on site visit results	Develop and prioritize preliminary findings report according to risk, log risks into risk register/tracking tool and assign risk owner. **Input** • Documented on-site visit results **Output** • Draft Vendor Security Assessment Evaluation Report • Risks entered into Risk management tool • Meeting scheduled with Business Shareholders	Review vendor evaluation reports with stakeholders **Input** • Draft Vendor Security Assessment Evaluation Report • Risks from Risk Management Tool **Output** • Final Vendor Security Assessment Evaluation Report	Discussion of Final Vendor Security Assessment Evaluation Report with vendors led by business stakeholders **Input** • Final Vendor Security Assessment Evaluation Report **Output** • Agreement on risk findings and commitment from vendor to create mitigation action plan	Vendor prepare an action plan in response to risk findings and submits to business stakeholders **Input** • Final Vendor Security Assessment Evaluation Report **Output** • Vendor Action Plan • Business stakeholder review response • Risks updated with action steps in Risk Management Tool	Track risk mitigation detail in the Risk Tracking Tool. Follow up with the business stakeholders to monitor the mitigation plan **Input** • Vendor Action Plan • Business stakeholder review response **Output** • Additional risks and mitigation details entered into the Risk Management Tool

EXHIBIT FOUR, PART 1: SAMPLE SEGMENTATION BASED ON CLASSIFICATION OF DATA HANDLED

Classification of Data Handled by Vendor	Examples of Type of Data Handled by Vendors	Examples of Vendor Business Relationship
Tier 1 Vendor **(Highly Confidential)**	• Protected health information • Medical records • Patient information • Treatment and condition information • Credit card information • Member address • Phone Number • Biometric information • Email address • Date of Birth	• Outsourced software development • Outsourced software maintenance and support • Customer Member helpdesk • Claims processing • Mail/Envelope stuffing and fulfillment
Tier 2 Vendor **(Confidential)**	• Payroll information • Employee performance data • HR and personnel records • Proprietary and trade secrets • Proprietary code and business logic • Investigation • Tax information • Employee Social Security Numbers (SSNs) • Highly sensitive reports	• Payroll and check printing services • Benefits administration services • Tax compliance services • HR consulting and outsourcing services • Mission critical consultants and contractors
Tier 3 Vendor **(Internal use Only)**	• Reports • Assessments • Findings and recommendations • Strategy and roadmap documents • Internal company memorandums • Budgets, projections and financial performance data • Departmental memos and reports	• Professional services firms • Consultants and advisory firms • Professional service contractors • Law firms • Business and operational operators
Tier 4 Vendor **(Public Distribution)**	• Marketing and promotional material • Mailing and solicitations • Public relations • Campaigns and outreach • Telemarketing • Surveys • Advertising material • Web and Media	• Advertising agency • Event marketing firms • Web designing and digital media services • Printing and graphic design • Marketing and survey companies

EXHIBIT FOUR, PART 2: SAMPLE SEGMENTATION BASED ON CLASSIFICATION OF DATA HANDLED

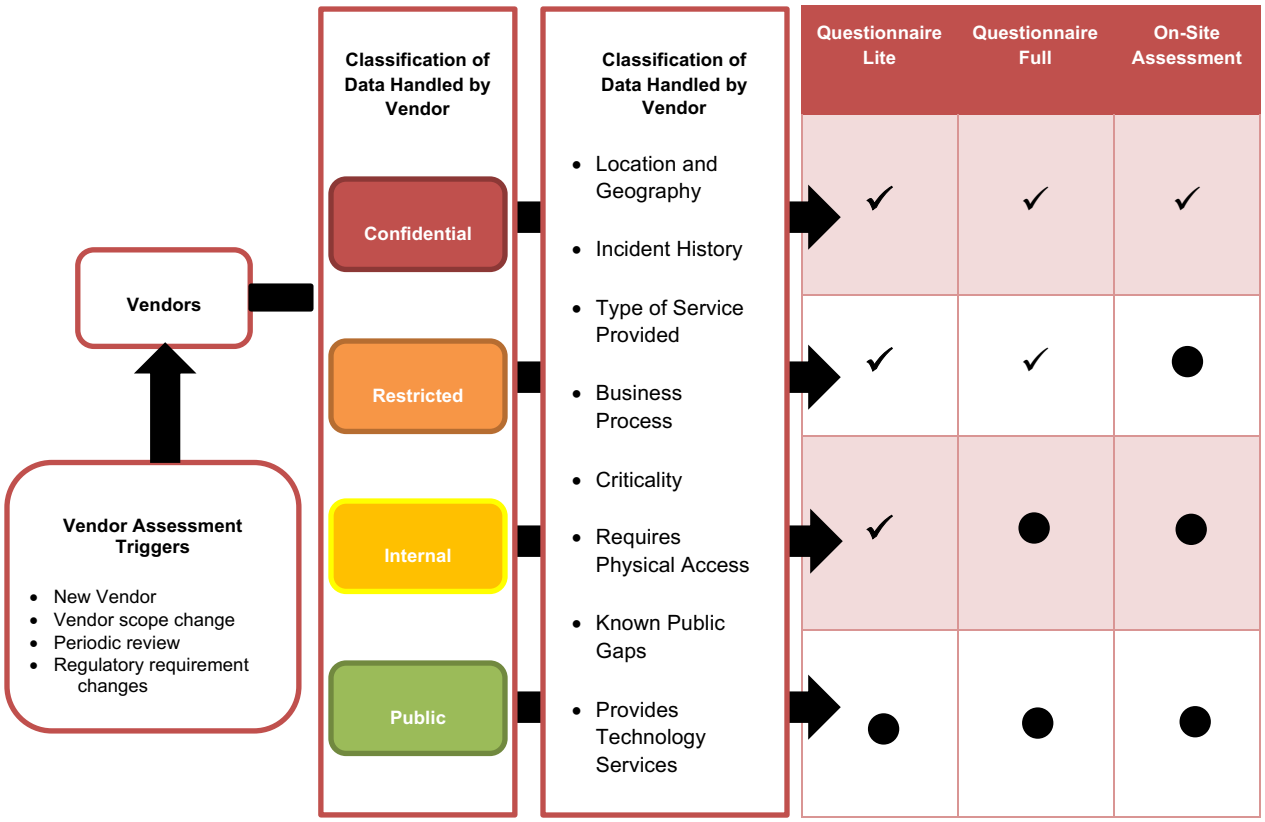


EXHIBIT FIVE: SAMPLE SEGMENTATION BASED ON CRITICALITY AND BUSINESS IMPACT

Tier	Criticality/ Business Impact	Risk (e.g. Legal, Regulatory, Financial)
High	• Relationships are critical to organization's business operations and/or long-term success. • May include fully integrated activities. • Vendor relationship is likely to provide a competitive advantage. • Time to replace/transition vendor would be > 6 months. • Vendor has direct access to facilities, systems and networks.	• Vendor has delegated functions monitored by regulatory agencies (e.g. Center for Medicare & Medicaid Services (CMS)). • Vendor has control or access to PHI or PII (HIPAA compliance). • Vendor has delegated responsibility for financial controls (Sarbanes Oxley (SOX) compliance). • Vendor is providing services in countries that are in the top 15 of the Foreign Corrupt Practices Act (FCPA) Corruption chart. • Vendor is located or providing services in a location that is frequently prone to natural disasters.
Moderate	• Relationships are important to category operations and long-term goals. • Potential value from developing long term relationships. • Vendor relationships is likely to provide an operational advantage. • Time to replace/transition vendor would be < 6 months but > 30 days. • Vendor has limited access facilities, networks/systems.	• Vendor shared functions monitored by regulatory agencies. • Vendor has no access to PHI or PII, but has access to confidential information. • Vendor has indirect impact on financial controls via systems and/or process (SOX compliance). • Vendor is located in or is providing services in countries that are listed within the Top 16-25 on the FCPA Corruption Chart. • Vendor is located or providing services in a location that is potentially prone to natural disasters.
Low	• Standard most common type of relationship. • Common supplier of non-unique goods and services. • Short term transactional relationship. • Largely cost/delivery driven performance management. • Time to replace/transition vendor would be < 30 days. • Relatively easy to replace without impacting business.	• Vendors does not provide services that are monitored by regulatory agencies. • Vendors does not have access to PHI or PII or Confidential Information. • Vendor has no responsibility for or impact on financial controls (SOX compliance). • Vendor is located in or is providing services in countries that are not listed within the Top 25 on the FCPA Corruption Chart. • Vendor is not located or does not provide services in a location that is at risk for a significant natural disaster.

EXHIBIT SIX: VENDOR MASTER LIST

#	Vendor Name	Service Provided	Location	Service Provided	Annual Spend
1	Mitchell and Jones	Marketing and Sales	New York, NY	Brand development and global sales	$5M-$10M
2	MedEnt Alliance	Marketing and Sales	Chicago, IL	Market research and sales in the mid-west region	$2M-$5M
3	Home-Run Marketing	Marketing and Sales	Portland, OR	Competitor analysis and benchmarking	$2M-$5M
4	Aluree Medical Inc	Care Management Services	San Diego, CA	On demand equipment and trained personnel to provide surge support	$1M-$2M
5	Print Corporation	Printing and Communications	Indianapolis, IN	Provide and install desk and network printers and maintain paper supply	$1M-$2M
6	EpiHealth Patient Management	Patient Management System	Minneapolis, MN	Patient medical records and electronic health records management system	$5M-$10M
7	HealthInnovation Consulting	Consulting	Charleston, SC	Business strategy, market research and new product development	$5M-$10M
8	Derrick Waltham	Consulting	Boston, MA	IT and network optimization and information security services	$5M-$10M
9	American Rx	Software Services	Los Angeles, CA	SAP hosting and maintenance	$5M-$10M
10	Vront Americas Inc	Software Services	Miami, FL	Payroll processing	$5M-$10M
11	Infinity Cloud Storage	Software Services	Phoenix, AZ	Infrastructure as a Service (IaaS) and Business Continuity services	$2M-$5M
12	Galileo Health	Behavioral Health Services	Hartford, CT	Outpatient psychological services	$1M-$3M
13	Michigan Mailing and Printing Services	Mail Handling	Detroit, MI	Business and legal mail processing and storage facilities	< $1M
14	SysSupport	Call Center	Seattle, WA	Maintain the HealthNext claims help line	$2M-$5M

#	Vendor Name	Service Provided	Location	Service Provided	Annual Spend
15	HealthAssurant	Claims Management	Philadelphia, PA	Claims segmentation and routing services	$2M-$5M
16	Wellness Claims Processing	Claims Processing	Charlotte, NC	Claims Processing system to manage PII and financial information	$2M-$5M
17	CompShell Technology Solutions	Application Development and Testing	Jacksonville, FL	Custom software development and testing and application enhancement	$5M-$10M
18	Insperio Health	Undetermined	Miami, FL	-	-
19	Global Language Services	Translation Services	San Francisco, CA	Legal document translation	$1M-$3M
20	WebTech LLC	Web Development Services	Chicago, IL	Maintain HealthNext's public website	$1M-$3M
21	Personnel Credit VerifServ	Unknown	Los Angeles, CA	-	-
22	HospNation Inc	Application Hosting	New York, NY	Infrastructure and Software as a Service (IaaS and SaaS)	$2-$5M

EXHIBIT SEVEN: VENDOR RISK AREAS

Shown below are the categories for which at least 5 questions should be prepared for the Vendor Assessment.

#	Question Category
1	Risk Assessment and Treatment
2	Security Policy
3	Organizational Security
4	Asset Management
5	Human Resource Security
6	Physical and Environmental Security
7	Communications and Operations Management
8	Access Control
9	Information Systems Acquisition Development and Maintenance
10	Information Security Incident Management
11	Business Continuity and Disaster Recovery
12	Compliance

EXHIBIT EIGHT: VENDOR RISK RATINGS DEFINITIONS

Risk Level	Risk Description
Critical	A critical risk level is assigned to a finding that leads to **Personal Health Information exposure of a HealthNext patient** or **previous un-mitigated/un-remediated exposure**. Critical security risks require **immediate resolution**. These issues increase the likelihood of a potential *Confidential Data* breach or disclosure. A remediation plan from the vendor is expected within seven (7) days and the risk(s) remediated within **30 – 60 days**
High	A high-risk level is assigned to a finding that leads to **potential exposure of PHI** or the **vendor is found to be out of compliance** with a contractual standard between the parties High risk issues require **quick resolution**. A remediation plan from the vendor is expected within seven (7) days and the risk(s) remediated within **60 – 90 days**
Medium	A medium risk level is assigned to a finding that **could lead or has led to a service interruption** affecting HealthNext Medium risk issues that should be **prioritized according to HealthNext business criticality**. A remediation plan from the vendor is expected within seven (7) days and the risk(s) remediated within **90 – 120 days**
Low	A low risk level is assigned to a finding that **could lead to degradation in operational capability or performance**. Lower level risks that do not pose an immediate threat, but **should be addressed as a good business practice**. Remediation of these findings should be prioritized and remediated according to criticality of the business need.