justin greis

CASE STUDY: IT RISK MANAGEMENT

HIGH GEAR ENGINE COMPANY

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

High Gear Engine Company (HG) is a global automotive supplier with operations around the world. Founded in 1937, HG specializes in engines for all kinds of automobiles, from high-end sports cars to farming equipment. HG is split into three business units (BU) that operate fairly independently and are marketed under different brand names:

1. *Velocity Engines* – Focuses on high-end sports cars and consumer-grade engines. These products command a premium in the market.
2. *Long Haul Motors* – Produces diesel and large engines for semi-trailer trucks. Long haul is known well known in the market for its durability and is a recognized leader in the trucking industry.
3. *Bigger Digger Power and Motor* – Specializes in mining equipment engines and motors. They supply to the major mining and industrial equipment manufacturers and often "white label" their engines as their customers' brand.

HG is located in Detroit, Michigan and has over 75 plants, performance labs and manufacturing facilities worldwide. Like most automotive suppliers and original equipment manufacturers (OEM), HG was hit hard by the economic downturn of 2008. Faced with bankruptcy, HG was forced to reduce its employee headcount and close several global locations. However, in the recent five years business has turned around and orders have picked up to the point that factories are re-opening and the company is once again profitable with global revenues totaling just over $9 billion (US). HG is planning for 17% compounded annual revenue growth and has a healthy (and growing) profit margin of 15%. HG is now ready to begin its path to growth which will require major change in the technology environment. This includes upgrading its technology infrastructure and applications that have been deferred for almost a decade. Three weeks ago, a new CIO (Sara Miller) was appointed by the board and has commissioned two projects:

1. *IT Strategy and Roadmap* – To determine the technology vision for the future and how the organization will get there. This strategy is very important since HG is in growth mode but does

not have the technology resources in place to achieve its goals. The executive committee (aka c-suite), the board of directors, and ultimately the shareholders are all looking to Miller to clearly lay out a vision and a plan for rapidly elevating HG's antiquated technology capabilities.

2. *IT Risk Management Analysis* – To "uncover the hidden risks lurking in the technology environment," as Miller put it. Miller knows that executing on a transformative IT strategy of this scale is fraught with risk, and with systems and applications this old, there is much work to be done.

Miller has brought in your team to execute the second initiative, the IT Risk Management Analysis, to determine the various IT risks that exist in HG IT and how to mitigate them. Miller has a presentation to the executive committee in 3 months and knows the timing will be tight given the size and global scale of the organization. She needs to understand the scope and approach of how you will go about assessing the risks and managing them to closure. She has emphasized that the two projects are her biggest priorities and she needs to know if there are any show-stoppers preventing her from achieving the goals as outlined in the strategy. Miller plans to use the IT risk management analysis to:

- help prioritize her strategic initiatives,
- justify the business case for the spend she is asking for from the executive committee,
- identify any critical "show stoppers" that will stand in the way of HG's technology modernization efforts, and
- establish clear goals and metrics for herself, the IT organization and HG as a whole.

Your team has just arrived on-site and have one week to prepare a scope and approach document for how to execute the engagement. Your time line is three months to get all field work complete and help Miller present her strategy and risk analysis to the executive committee and the board of directors. Miller did an initial scan of the environment and compiled some risks she saw based on her own inquiry and observation of the environment. Miller's preliminary observations are outlined below with a few key questions she has as a result of her interviews with key stakeholders in the organization.

HG INFORMATION TECHNOLOGY

At its peak, the HG IT department was 800 strong with dedicated teams for each business unit and centralized team to run the shared corporate IT systems. Long ago HG IT was a very decentralized organization with CIOs for each of the business who had dual reporting lines to the president of each business unit and to the global CIO of HG. There was a lot of redundant systems and duplication of effort. HG had 3 of every system and each business unit was as different and ran completely differently: three supply chain systems, three financial systems, three engineering departments and product lifecycle management systems, and the list went on. In fact, it took a mandate from the CEO to get every business unit on to one email, calendar, instant message system, and domain name. The leadership knew that centralizing and consolidating functions would yield cost savings and efficiencies but it would also remove autonomy and the freedom to guide their own technology decisions. But there was little desire to do so since all business units were growing very fast, beating analyst estimates and were happy the way things were. Then, 2008 hit and HG was forced into bankruptcy.

HG was bought by a private equity firm, Velocity Partners, who instituted austerity measures to reduce costs and save the core of the business. IT was among the biggest departments hit with layoffs and cost reduction measures. Headcount plummeted to a skeleton crew of 300 IT personnel. BU IT personnel were all but eliminated and each plant was given an IT support manager. In many cases, the IT support manager

served all the plants and office locations within a 100-mile radius causing them to be overworked and the business units to be generally unhappy with the level of service it was receiving from IT. BU CIOs were converted to manager liaisons and every position was consolidated to the bare minimum. Times were tough and any non-essential projects and spend were put on-hold. Only projects with guaranteed cost savings or revenue generating potential were approved and every project and key initiative had to go through a rigorous business case process approved by the board of directors which was heavily dominated by the majority owners, Velocity Partners. Thus, routine upgrades, equipment maintenance, and application/system enhancements were all rejected as they did not have a clear benefit that met Velocity's project approval criteria.

The turmoil at High Gear eventually settled over time and HG focused on business recovery and profitability. The cost reduction and business development initiatives were successful and HG won several contracts with new clients that were looking to use the economic downturn to its benefit and strike while their competitors were reeling. As the recession subsided, HG began to grow and expand to meet its growing demand but nearly a decade had passed since the bankruptcy and layoffs and still IT had remained relatively the same: same headcount, same systems, same applications and a growing list of concerns that they were falling behind their competitors.

Even after all the cost-saving measures, HG still operated as three independent business units with one corporate function sitting atop. The BUs dictated the budget and all costs were charged back to each of the three business units in proportion to headcount or revenue percentage; it was a fairly loose and undefined chargeback model. Corporate IT attended to some of the shared functions such as:

Even after all the cost-saving measures, HG still operated as three independent business units with one corporate function sitting atop. The BUs dictated the budget and all costs were charged back to each of the three business units in proportion to headcount or revenue percentage; it was a fairly loose and undefined chargeback model. Corporate IT attended to some of the shared functions such as:

- Information Security
- IT Risk Management
- IT Audit and Compliance
- IT Operations
- Disaster Recovery
- IT Infrastructure
- IT Strategy
- Enterprise Architecture
- IT Financial Management
- Business Analytics and Information Management
- EDI (Electronic Data Interchange)
- IT Program Management
- IT Helpdesk and Support
- Email and Office Productivity
- Telecommunications
- IT Vendor Management

The business units were responsible for the following IT functions:

- Engineering and CAD Systems
- Product Lifecycle Management
- Research and Development
- ERP Systems
- Supply Chain Systems
- Customer Relationship Management Systems
- Business Initiative Program Management
- Manufacturing and Shop-Floor Systems

The lists above are not exhaustive but do represent the majority of the division of responsibility between corporate IT and the business units.

Miller has her work cut out for her. She knows that she will need to centralize core functions of IT for cost-savings, efficiency purposes and to elevate HG's capabilities but she also does not want a cultural coup on her hands if the business units get the sense that they are losing control and autonomy. Miller is a seasoned executive and was brought into HG from another automotive company and has a track record of transforming IT into a leader and business enabler rather than a support function. Because cost is under a microscope, the office of the CIO reports to the CFO (John Vargas). Miller told Vargas her plan and he agreed she was on the right track approaching this from a two-pronged approach: IT strategy and IT risk. Vargas informed the board about Miller's strategy and risk initiatives and gave her the next board meeting to brief them on the findings and recommendations. The board must see a clear path forward and understand how to get there. Vargas and the executive committee know that they must spend money over the next three years to modernize and upgrade HG's IT capabilities but they want to be smart about it. They know they will never get back up to 800 IT personnel but also know that incremental headcount, restructuring and a substantial capital investment will be required.

MILLER'S PRELIMINARY OBSERVATIONS

Miller's first three weeks were spent interviewing all the major business and IT stakeholders in the company. She managed to talk to a good cross section of people with knowledge and background on the company and came up with some preliminary observations to consider when putting together your plan of attack:

- ***No one is accountable for information security.*** The information security function is viewed as a part time job and is bundled together with IT Audit, IT Compliance and IT Risk Management. No one seems to be formally thinking about the threats to HG's information assets such as engineering designs, new product information, sensitive employee/customer information, and confidential legal, strategy and merger/acquisition information.
- ***Connectivity is a problem.*** As applications have become more web-based and internet-based, they have put a strain on the infrastructure and internet bandwidth. Peak hours of traffic are the worst and several company executives have complained that their email took one hour to download during peak hours of 8:00 AM – 10:00 AM. Something has to be done, especially if more cloud-based applications are to be adopted.
- ***There are too many ERPs and they are expensive to maintain.*** The application portfolio consists of roughly 235 ERP systems when you count the different versions, instances and regional implementations. This number only includes formal ERP systems and not any of the supporting business support systems, spreadsheets, transactional systems or databases that feed the ERP systems. If you could those, the number has been estimated as high as 3,000 but no one really knows. These ERP systems frequently go down and troubleshooting them takes precious personnel away from their core responsibilities. And because enhancements, upgrades and changes have not been made in years, many of the processes that would automate simple tasks (such as approvals, workflow and task management) are done manually outside the system. No one really knows how much this is costing the company but everyone knows they are unhappy with the current state.
- ***IT audit issues are piling up.*** Because of the headcount reduction years ago, much of the process maturity was lost. Users are informally provisioned and de-provisioned access, developers have access to the production environment and no one is quite sure if there is a formal disaster recovery (DR) plan in place. The person who wrote the DR plan is long-gone and HG IT has not found time or resources to dedicate to fixing it. The external auditor has indicated that if these issues are not fixed before the financial year-end, HG is at risk of a "Significant Deficiency" on their IT General

Controls related to their financial reports. This would have a potential impact on stock price and investor confidence in the HG brand.

- ***Manufacturing and shop floor systems are old and causing the production line to stop.*** The manufacturing and shop floor systems have been neglected for over a decade. Even when HG was at its peak, patches were not applied and systems were left to run on their own. Preventive maintenance did not exist and the systems were not touched unless something went wrong. Recently, three production lines went down for two days each (two Velocity lines and one Bigger Digger line) for various reasons. In the case of Velocity, a vendor mandated patch had been pushed out to the robotics system but it was not compatible with Windows 2000, which is widely used in production facilities despite the fact it is no longer supported. When the patch was pushed out, the line simply came to a halt. It was estimated that HG lost $5 million per day in revenue and contractual fines because they were not able to ship the orders for the just-in-time manufacturing required by its customers. Bigger Digger's production line outage is still unknown and no one can explain why it happened. They have been noticing their production line computer systems "acting up" and doing strange things (e.g. restarting, going to strange websites, and popping up with adware, etc.) but no one yet understands the root cause. Eventually, the plant manager just went to Best Buy, bought a new computer, had the IT support manager install the necessary software and the line went back up again. The plant manager was praised for his quick thinking and troubleshooting but Miller knows this cannot happen again.
- ***PCs and operating systems are old and unsupported.*** The company still runs on Windows XP and most computers are over 5 years old. Employees regularly complain about the slowness of their PCs, especially as new corporate IT mandated software is installed. Windows XP is no longer supported by Microsoft so HG is paying expensive third-party fees to support it while they get their strategy together to upgrade the PCs and the operating systems at the same time. Miller even found out that some of the executive team went out and bought Apple Macs and Microsoft Surfaces just so they didn't have to deal with the sluggish corporate PCs.
- ***No one understands how the applications and business systems work except the vendor.*** When the austerity measures were put in place, Velocity Partners brought in an off-shore vendor to take over application development and maintenance. Most of the internal IT resources who understood how the applications and systems worked were let go. Now that the vendor has been in place, HG is at their mercy for any fixes or enhancements. These are often done incorrectly or with little quality assurance. Additionally, the vendor has admitted they are short-staffed so there is a large back-log of changes and enhancements that only they can make. The vendor has also raised their rates several times over the years. What started as a cost savings measure is now proving to be expensive and all HG can do is pay whatever they ask because they are the only ones who know how it works.

The observations list is not meant to be exhaustive; Miller provided it to your team as background so you can incorporate these into your plan and approach. As bad as the problems are, she knows your team will find more as you interview others and survey the organization. She is interested in your thoughts on some quick wins to address the observations but knows we must go through the formal process and your team's recommended methodology for assessing and mitigating IT risk.

YOUR TASK FOR THIS CASE

SCOPE AND APPROACH FOR CONDUCTING THE ANALYSIS

When your team began the engagement on Monday, you had an initial introductory meeting with Miller and her staff where she described her preliminary observations and gave your team the background. She wanted to know how the next three months would look and what your team would be doing to get her the findings and recommendations she needed. Miller is interested in the:

- *Scope of what you will look at* – Miller wants to know what risks and frameworks you leverage and what. What is the list of risks and what will you look at to conduct the analysis? What questions will you ask and how will you interpret the results? What business units and geographic locations will you cover? What aspects of the business will you cover and how do we know we are being complete and now leaving anything out?
- *Approach you will use* – Miller needs a clear plan for how you will conduct the analysis. What is the timing? How will you apply the framework to get meaningful results? What are the phases of the project? How will you make sure she meets her presentation commitments to the executive committee and board?

Fundamentally, Miller would like to see a kick-off deck that describes the scope of the engagement and how your team will execute it. Miller has suggested that your team use the ISACA RiskIT framework as the basis for your approach; however, she has cautioned you: she does not simply want screenshots of RiskIT. Miller needs to understand how you will apply this methodology and approach to her business circumstance.

THREE "QUICK WIN" RECOMMENDATIONS

Based on Miller's preliminary observations, she would like to see an example of three risks and hear your recommendations for how to mitigate them. This is more so that Miller can get a sense for what she will get as a final work product at the end of the three months. She would rather see a preview of three risks now given the limited information she provided than wait until the end of the engagement only to be surprised or fall short of expectations. Once again, the ISACA RiskIT framework will be integral in your analysis.

Miller has shared that the HG executive team are "very visual" and the more you can summarize your results and recommendations in a visual format, the better this will go. Charts, graphs, infographics, and dashboards have all been well received in the past.

A PROCESS FOR MANAGING IT RISK ONCE THE ANALYSIS IS COMPLETE

Finally, once the initial inventory and analysis of the IT risks is complete, Miller would like to know how she and the IT organization can manage and govern the risks going forward. Miller would like to see a process flow of how new risks will be identified, analyzed and treated so that this activity can continue in the future. She also needs to understand what she should do with the existing risks that your team will identify so that she can manage them and address them. Again, a process flow describing how existing risks are managed will be key here. To summarize, Miller has specifically asked you to cover the people, process and technology recommendations for how to manage IT risk going forward.

- *People* – What resources are necessary to run the IT risk management process? She has asked you to keep it "reasonable" given the cost pressures on the organization.
- *Process* – What does the process look like for identifying, analyzing treating and managing risk? Process flow diagrams (aka swim-lane diagrams) are helpful tools to show how the process and people fit together.
- *Technology* – What tools and systems are required to automate the IT risk management process? Miller has heard a lot about new GRC technology from companies like Archer, MetricStream, ServiceNow, OpenPages and many others. She is not sure what she needs but does not want to "lead with the technology." She has indicated that if she can manage the risks through Microsoft SharePoint, Surveys and/or Microsoft Excel spreadsheets until a more robust tool can be procured, that is fine with her. The key is to understand the processes and which tools may be a good fit in the future to help run those processes.

YOUR TASK FOR THIS CASE – PRESENTING TEAMS

MILLER'S CHALLENGE

Miller's career is riding on this project. If successful, this project will solidify her as a leader in the organization, set the tone for her transformation efforts and establish credibility for your team in the eyes of the board. Miller has shared with you that, "if your team does a good job here, it will mean big things for you in the future!"

You don't want to let her down so you immediately get to work on laying out her asks described above. Remember, this should consist of one deliverable in MS PowerPoint format and concisely address the points described above.

You have one week to present your work and Miller is anxious to hear what you have to say!

YOUR TASK FOR THIS CASE – ALL OTHER TEAMS

CASE STUDY EXECUTIVE BRIEFING

With the decentralized environment at HG, Miller is expected to present a single slide to the other members of the Executive Committee (i.e., C-suite) to promote discussion / insights around the planned key stages of the IT risk management lifecycle. Your task is to provide Miller with a single slide graphic depicting the key stages of the IT risk management lifecycle and that addresses the following:

- The key benefits of each of the lifecycle stages
- Some anticipated challenges that maybe faced when developing and rolling out a centralized IT risk management program (such as getting buy-in from various key stakeholders across HG to consistently adopt a centralized IT risk management regime)

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 time line 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.
- Application of the ISACA RiskIT framework

A few tips and tricks for solving this case:

- 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.