Risk / Control Matrix

This is a case assignment reviews the risk assessment and control Activities of the COSO internal control framework and then illustrates how this is accomplished in a highly integrated computerized enterprise business environment. The Monitoring Activities layer of the COSO framework are then illustrated in this same business environment.

Product

SAP ERP
GBI
Release 6.04

Level

Undergraduate
Graduate

Focus

Internal Controls

Authors

Edward Beaver

Contributors

Richard Flanagan
John Calnan

Version

1.0

MOTIVATION

This scenario deals with examining the business functions and processes involved in selling goods to another company (B to B sales) and the business risks and internal controls controls that should be in place in order to safeguard the company's assets and the integrity of the company's financial records.

PREREQUISITES

Before you use this case study, you should be familiar with navigation in the SAP system.

You should also be familiar with:
> basic internal controls
> Order to Cash Process

NOTES

This case study uses the Global Bike Inc. (GBI) data set, which has exclusively been created for SAP UA global curricula.

Assignment Overview

The scenario follows a logical approach to analzing business process risks and non-security internal controls to address or mitigate these risks consistent with the COSO internal control framework. There are 5 steps in this process / exercise. Part 6 of the assignment relates to each team member's work in support of the team submission for this and other prior exercise.

Part 1: Analyze and define the key risks that exist for the Order to Cash (OTC) process at GBI

Part 2: Guided by the risks you identified (esp. the High Severity and High Likelihood / Frequency risks) identify the key controls that will be used in the OTC process.

Part 3: Link the Risks from Part 1 to the controls in Part 2.

Part 4: Complete definition of the controls (classifications, links to assertions, etc.)

Part 5: The control activity description is not sufficient to assure the control process and related auditing process is understood and active. In Part 5 (leveraging some examples in the Appendix) you must write auditable control process documentation for 1 manual and 1 automated (configuration) control identified.

Part 6: This is an individual team member part of the exercise (vs, team submitted for all other parts). Specifical you'll anwer a couple questions about your work as a team to complete this a other exercises.

Risk Assessment and Other Controls

GBI is very concerned about security and information assurance. Due to the passage of the Sarbanes-Oxley law, GBI realizes that solid financial accounting controls are extremely important for the corporation. Originally GBI trusted the process and the people completing the tasks in the process as effective enough internal controls.

However, after implementing the ERP sytem at GBI, there is realization that a thorough review of the process, risks, controls, etc. is needed to truly assure GBI has the internal controls necessary to satisby the requirement of the Sarbanes-Oxley lay and many others laws and regulations.

An organization must do a detailed assessment of the risks involved with any business process and then determine the likelihood of that risk occurring and the severity of the risk if it should occur. These factors will then be used to decide what controls should be implemented in order to mitigate the risk.

To complete the definition of the controls, detailed documenatation of the manual process that is used must be created. For configuration controls, a review / auditing process must be created. This documentation is required to assure each control is fully understood, taught, active and auditable.

This ddocumentation in total is needed by GBI to assure good process operation that can be audited and certified in control by the auditors of GBI.

Company Background

Global Bike Inc., (GBI) is a world class bicycle company serving the professional and "prosumer" cyclists for touring and off-road racing. GBI's riders demand the highest level of quality, toughness and performance from their bikes and accessories.

Product development is the most critical element of GBI's past and future growth. GBI has invested heavily in this area, focusing on innovation, quality, safety and speed to market. GBI has an extensive innovation network to source ideas from riders, dealers and professionals to continuously improve the performance, reliability and quality of its bicycles.

In the touring bike category, GBI's handcrafted bicycles have won numerous design awards and are sold in over 10 countries. GBI's signature composite frames are world-renowned for their strength, light weight and easy maintenance. GBI bikes are consistently ridden in the Tour de France and other major international road races. GBI produces two models of their signature road bikes, a deluxe and professional model. The key difference between the two models is the type of wheels used, aluminum for the basic model and carbon composite for the professional model.

GBI's off-road bikes are also recognized as incredibly tough and easy to maintain. GBI trail bikes are the preferred choice of world champion off-road racers and have become synonymous with performance and strength in one of the most grueling sports in the world. GBI produces two types of off-road bike, a men's and women's model. The basic difference between the two models is the smaller size and ergonomic shaping of the women's frame.

GBI also sells an accessories product line comprised of helmets, t-shirts and other riding accessories. GBI partners with only the highest quality suppliers of accessories which will help enhance riders' performance and comfort while riding GBI bikes.

For purposes of this assignment, we will focus on the process involved in sales of in-stock, standard, off-road bicycles. GBI uses an open invoice system to bill its customers; that is, the customer is billed and must pay for each order separately as opposed to the customer being billed periodically for all orders made during that period (usually referred to as cycle billing).

Standard Order to Cash Business Process

Tasks within business processes may vary considerably depending on the level of automation and the associated technology. For instance, in a manual system, the task of recording a transaction may be accomplished by either entry into a journal or by the "filing" of a copy of a multi-copy form. In an automated system, "recording" entails the "filing" or storage of the transaction in the AIS. This is sometimes accomplished by pressing a "save" button after entering the transaction into the system. The order of the tasks will also differ depending on the extent of automation within the system.

Assume that GBI has recently converted from a manual system to a process the leverages the use of an ERP system (e.g. SAP). The company uses the following 24 steps when they sell standard goods to the customers. Note for organization and process optimization purposes, GBI has chosen to define 4 sub-processes within the broader Order to Cash (OTC) process.

Sub-Process: Order Receipt & Handling (OR&H)

1. A customer sends a purchase order for off-road bicycles to a GBI employee.
2. A GBI employee compares the customer's purchase order to determine if the customer's master data is in the system and is correct.
3. If the customer master data is not in the system or is incorrect, then the master sales and distribution data (such as company address, contact person, phone numbers, etc.) for the customer is entered or maintained in the ERP system.
4. If the customer master data is not in the system or is incorrect, then the financial data (such as banking information and GBI reconciliation account number) for the customer is entered or maintained by a GBI employee in the ERP system
5. If the customer master data is not in the system or if the customer would like to change credit terms or limits, then a GBI employee checks the credit rating of the customer and assigns a credit limit and credit terms in the ERP system.
6. A GBI employee creates a sales order in the ERP system.
7. If during creation of the sales order an ATP failure exists (e.g. inventory not available) A GBI employee reviews the order requirements with Supply Chain planning to determine best decision (e.g. adjust plans, notify customer of valid delivery date, etc.).
8. A GBI employee creates order acknowledgement & sends to the customer using ERP system.

Sub-Process: Material Flow (MF)

9. A GBI employee creates a delivery document in the ERP system and prints picking ticket to fill the customer's order.
10. A GBI employee physically picks the goods (the bicycles) from the picking ticket.
11. A GBI employee creates a packing slip and a mailing label using the ERP system.
12. A GBI employee puts the packing slip into a reinforced packing container with the goods, seals the container and adheres the mailing label to the container.
13. A GBI employee moves the goods from the inventory control area to the shipping dock.
14. A GBI employee prints a shipping manifest using the ERP system.
15. A GBI employee places the goods to be shipped on the truck.
16. A GBI employee gives the shipping manifest to the truck driver.
17. A GBI employee records that the goods have been shipped in the ERP system.

Sub-Process: Customer Invoicing (CI)

18. A GBI employee creates invoice with remittance advice in ERP system & sends to customer.

Sub-Process: Payment Receipt and Handling (PR&H)

19. A GBI employee receives the payment from the customer with the returned remittance advice.
20. A GBI employee records the payment from the customer in the ERP system.
21. A GBI employee takes all of the payments for that day and creates a deposit slip for the bank.
22. A GBI employee deposits the cash in the bank.
23. A GBI employee records the bank deposit.
24. A GBI employee reconciles bank deposits, cash receipts and ERP system balances daily.

Important Note – You are not allowed to change the above business process. That is, you cannot add, delete or modify any of the steps above.

Part 1 – Risk Analysis and Definition

In this part of the assignment you are required to review and analze the entire Order to Cash (OTC) process as practiced by GBI and identify the key risks to the GBI business during operation of this process. The current OTC process design was outlined in the prior section.

Using what you're learned in class and in prior exercises (e.g. Exercise 4) analyze the Order to Cash (OTC) Process design and outline the **key risks** to the GBI business. Focus in Part 1 only on the risks (what could go wrong).

Record your risks in the '*Part 1 - GBI Risks*' tab in the exercise submission spreadsheet. Record columns A through F in this Part 1 step (other columns will be addressed in future parts of the exercise). In analyzing and recording these risks you must:

- Identify at minimum 25 risks in the process
- Identify at minimum 4 risks in each of the sub-processes of the overall OTC process. These sub-proccesses are:
  - **OR&H**: Order Receipt and Handling
  - **MF**: Material Flow (shipping)
  - **CI**: Customer Invoicing
  - **PR&H**: Payment Receipt and Handling

Below are the definitions of the columns to be completed.

Risk #: A unique # assigned to the risk. The # includes the process (OTC) and indicator of 'R' for risk. This column is pre-populated.

Risk Description: Clearly define what the risk is and include enough information that a business person reading can understand how the risk might inpact the GBI business.

Process: Order to Cash

Sub-Process: See above. Note: there can be instances where a risks is associated with more than 1 sub-process. If this is the case, enter all sub-processes the risk is associated with.

Severity of Risk: Indidate using the scale below (also in submission spreadsheet) your assessment of the severity of the risk.

Severity / Impact	
High	Potential for severe fraud, signfificant impact on financial Statement Assertions
Medium	Potential for moderate fraud, moderate impact on financial Statement Assertions
Low	Negligable or minor potential for fraud, Negligable or minor impact on financial Statement Assertions

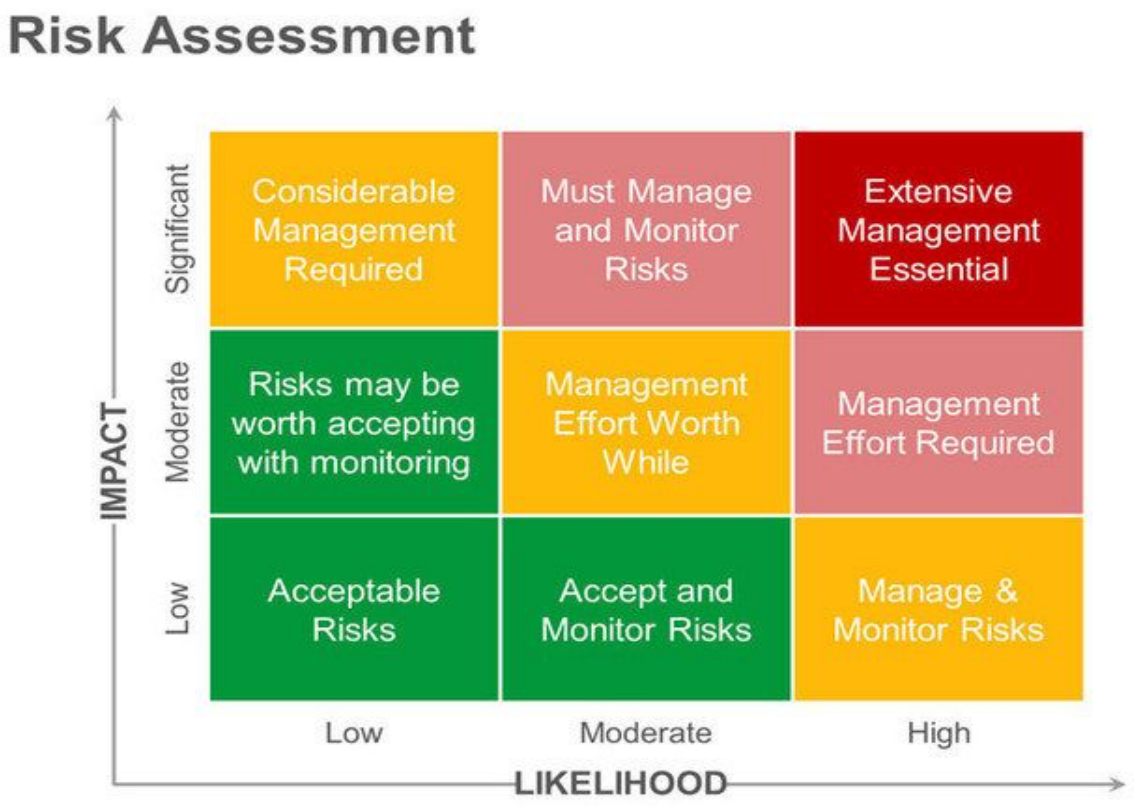
Likelihood (Frequency) of Risk: Indidate using the scale below (also in submission spreadsheet) your assessment of the likelihood / frequence this risk would occur for GBI.

Likelihood / Frequency	
High	Risk is probable / frequent. Likely to occur
Medium	Some manifestations of this risk may occur occasionally
Low	Manifestations of this risk are possible but not likely, remote, improbable

Note: the submission spreadsheet has an example (in grey) of a potential risk for GBI.

Risks have can affect the business in different ways and with different magnitude. The dimensions of Risk Severity or Impact and Likelihood / Frequency of occurant help you discover the total impact of the risk to the business.

The Risk Assessment chart below in a visual and verbal way indicates the total impact of the risk given different values of Risk Severity / Imact and Likelihood / Frequency. This chart can be useful in defining which risks need internal controls defined vs. those where the risk is acceptable without a defined internal control.



Part 2 – Control Analysis and Definition

In this part of the assignment you are again focused on the Order to Cash (OTC) process as practiced by GBI (see prior sections). Using the risks you outlined in Part 1 and the total impact of the risk (see matrix in prior section), select the key controls you recommend that GBI implement as internal controls for GBI. Use what you have learned in class and in prior exercises (e.g. Exercise 4) to identify potential controls and chose those that will be the most effective (**key controls**).

Record the controls you choose in the '*Part 2 - GBI Controls*' tab in the exercise submission spreadsheet. Record columns A through E in this Part 2 step (other columns will be addressed in future parts of the exercise). In analyzing and recording these controls you must:

- Identify at **minimum 15 controls** for the process
- Indentify at least a mininmum of three (3) controls in each of the sub-processes of the overall OTC process. These sub-proccesses are:
  - **OR&H**: Order Receipt and Handling
  - **MF**: Material Flow (shipping)
  - **CI**: Customer Invoicing
  - **PR&H**: Payment Receipt and Handling
- At least two (2) of the controls must be Automated / Configured controls
- At least one (1) controls must be identified for all Risks identified in Part 1 as High Severity or High Likelihood / Frequency

Below are the definitions of the columns to be completed in the '*Part 2 - GBI Controls*'

Control #: A unique # assigned to the control. The # includes the process (OTC) and indicator of 'C' for control. This column is pre-populated.

Key Control Activity: Clearly define what activity will be completed with implementing this control.

Process: Order to Cash

Sub-Process: see above

Method: What method will be used to implement this control. Options are:

M: Manual – using a defined procedure a person is responsible for completing this activity to implement the control.

A: Automated (Configured) – the ERP system using a configuration parameter will automatically implement the control (Assure the activity occurs).f

Note: the submission spreadsheet has an example (in grey) of a potential risk and control for GBI.

Part 3 – Control Definition: Link to Risks and Assertions

The analysis of Part 1 (identify Risks) and Part 2 (identify controls) cannot be done in isolation of each other. Controls exist to remove or mitigate a risks that exists.

In Part 3 of this exercise, you must link the risks from Part 1 to the Controls identified for Part 2. Record the results of this linkage by providing data in columns G through I in the '*Part 1 - GBI Risks*' tab. Specifically enter the following information in these columns:

Key Control Activity: The key control activity (column B value from the Part 2 – GBI Controls tab) that will address this business risk. Note: more than 1 control can address a given risk.

Control Ref #'s: The control # (column A value from the Part 2 – GBI Controls tab) that will address this business risk. Note: more than 1 control can address a given risk.

How does the Control Address / Mitigate the Risk?: Briefly describe how the control addresses the business risk.

Notes:

- *The submission spreadsheet has an example (in grey) of a potential risk and control for GBI.*
- *A given control may be applicable to addressing more than 1 risk. In this case, the control will be listed only once in the Part 2 tab but multitple times in the Part 1 tab.*
- *A given risk can be addressed, mitigated by more that 1 control. In this case, enter all controls that are applicable in the Key Control Activity and Control Ref #'s column.*
- *Because Part 2 of the exercise only requires you to identify a minimum of 15 controls, not all risks may have a control identified. For risks without a control defined enter a value:*
  - *Acceptable Risk – no controls will be developed*
  - *'TBD' (To Be Determined) in all columns.*
- *Controls must be identified and linked for all Risks identified in Part 1 as High Severity or High Likelihood / Frequency.*

Part 4 – Control Definition Details

This section is to in-progress still.

Part 5 – Internal Control Process and Audit Documentation

This section is to in-progress still.

Question 5.1: Explain the logic behind an ignorance control. If this was the only control for a specific set of risks, do you think that it would be an effective control? Explain your answer.

Question 5.2: Choose one of the tasks under the Periodic and Closing Activities and explain what the task is.

Question 5.5: What is the transaction code and activity description related to the authorization?

Part 6 – Individual Team Member Feedback

This section is to in-progress still.

Question 6.1: Explain the logic behind an ignorance control. If this was the only control for a specific set of risks, do you think that it would be an effective control? Explain your answer.

Question 6.2: Choose one of the tasks under the Periodic and Closing Activities and explain what the task is.

Question 6.5: What is the transaction code and activity description related to the authorization?

This ends the assignment.