Risk Identification examples:

One can see from the following examples that failure to correctly define your risk will affect control identification, mitigation plan and ultimately reporting. "Garbage in garbage out" analogy. Below, we have provided some examples of "good" and "bad" risk descriptions: ***(Adapted: AUS/NZ Standard 2004)***

Example 1: Good Risk Descriptions

Example Risk – Good Description	
Risk Description	High employee turnover
Causes	▪ Job dissatisfaction ▪ Uncompetitive remuneration
Impacts	▪ Loss of corporate knowledge ▪ Delay in delivery of business objectives

Example Risk – Good Description	
Risk Description	Breach of OH&S Act
Causes	▪ Lack of knowledge of legislative requirements ▪ No compliance program or register
Impacts	▪ Adverse publicity ▪ Fines / penalties

Example Risk – Good Description	
Risk Description	IT failure
Causes	▪ Power outage ▪ Software failure
Impacts	▪ Loss of data ▪ Business disruption

Example 2: Poor Risk Descriptions	Explanation
Example Risk – Poor Description Risk Description: Lack of succession planning Causes: ▪ Lack of handover time ▪ Reluctance to handover information Impacts: ▪ Financial ▪ Business	Lack of succession planning is a lack of a control.
Example Risk – Poor Description Risk Description: Fines Causes: ▪ Breach legislative requirements Impacts: ▪ Financial	Fines are really the impact to the organisation. Also, the reason for identifying the cause is so that you can identify the right controls. This description is so wide that a control is difficult to define, other than "put in place a full compliance program".
Example Risk – Poor Description Risk Description: System not backed up Causes: ▪ IT failure Impacts: ▪ Loss of data	System not backed up is a control failure. Also an IT failure is not the cause of the system not being backed up, poor work practices are.

Example Risk – Poor Description

Risk Description	Lack of succession planning
Causes	▪ Lack of handover time ▪ Reluctance to handover information
Impacts	▪ Financial ▪ Business

Example Risk – Poor Description

Risk Description	Fines
Causes	▪ Breach legislative requirements
Impacts	▪ Financial

Example Risk – Poor Description

Risk Description	System not backed up
Causes	▪ IT failure
Impacts	▪ Loss of data

Issues to Consider in the Risk Identification Process,

1. What are the main objectives of our institution?

What are our strategic objectives?	What are our business objectives?
What are our financial targets?	What are our service delivery targets?
What are our other key targets?	

2. Who are our stakeholders and how can they pose a risk to us and how can we pose a risk to them?

Customers	Communities
Suppliers	Creditors
Employees	

3. How do we create value for stakeholders?

Service delivery	Financial sustainability
Reputation	Compliance
Administration	

4. What are the critical success factors

Core skills	IT systems
Cost containment	Budgeting
Staff retention	

5. What are the institution's critical processes?

Procurement	Processing payments
Distribution	Information management
Administration	

6. What are the potential sources of risk and change that could impact on the above?

Accidents	Cash flow variances	Civil unrest
Contract breach	Crime	Currency exchange rates
Distribution failures	Economy variance	Engineering failures
Environmental incidents	Expense management	Financial difficulties
Fire	Fraud	Human resources failures
Inflation	Interest rate change	Labour relations failure
Medical incidents	Natural perils	Negligence
Procurement failures	Project failures	Quality failures
Social change	Strategy execution	Technology failure

Once the initial risk identification process has been completed, management should already start considering whether any of the risks are interconnected, i.e. is there any correlation between the identified risks?