



# **Risk and Criticality for Service Management in Service-Now**

**Risk = Threat \* Vulnerability \* Criticality**

V 1.0 October 2012

# All lazy functional managers need to know



The screenshot shows the CERN service portal homepage. A red arrow points to the URL `cern.ch/service-portal` (1). Another red arrow points to the 'Edit' button on the 'Stores Urgency Counter' page (3). The page title is 'Stores Urgency Counter (GS-IS-SO)' and it includes a description: 'Delivery of urgent orders and manage material return.' and keywords: 'urgent orders, demandes urgentes, 54.50.40.900.1, counter, guichet des urgences, Central store Magasin central, material return, materials returned, retour de...'

The screenshot shows a search services menu with the following items: 'Services', 'CERN Service Portal - [red arrow] (2)', 'CERN Service Desk: x77777', 'Search in CERN', 'CERN Search - [red X]', and 'Document Server (CDS) - [red X]'. A red arrow points to the 'CERN Service Portal' link.

- Find your function from the service portal..
1. Click link on cern homepage and search for your function(s)
  2. Option 2: Search portal from CERN homepage
  3. Click Edit on your function's page in the portal
  4. Scroll to the bottom of the page and select the Risks tab
  5. Click a 'risk name' you want to edit
  6. Change the vulnerability (optionally add Description)
  7. Save or Update → That's ALL!!!! (thanks for your attention)

The screenshot shows the 'Functional Element Risks' page. A red circle highlights the 'Functional Element Risks (8)' tab (4). Below the tabs, a table lists various risk names, with one selected (5):

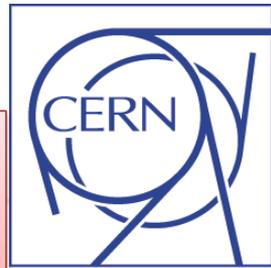
Risk name	Threat	Vulnerability	Risk	Risk Class
<a href="#">Material Failure / Loss of Tool / Function / Data for Stores Urgency Counter</a> (5)	Material...			
<a href="#">External Attack (Hacking, Computer Virusses) for Stores Urgency Counter</a>	External...			
<a href="#">Confidentiality / Legal / Reputation for Stores Urgency Counter</a>	Confide...			
<a href="#">Disaster for Stores Urgency Counter</a>	Disaste...			
<a href="#">Terrorist Attack for Stores Urgency Counter</a>	Terroris...			
<a href="#">Inside Attack (Intentional Malicious Acts / Fraud / Hacking) for Stores Urgency Counter</a>	Inside /...			
<a href="#">Single point of failure / No plan B / Strike for Stores Urgency Counter</a>	Single /...			

The selected risk is shown in a detail view (6):

- Risk ID: RISK0007284
- Risk name: Material Failure / Loss of Tool / Function / Da
- Risk: 192
- Risk Class: 4
- Applies to: Functional Element: Stores Urgency Counter
- Business criticality: 4 - Limited
- Threat: Material Failure / Loss of [red arrow]
- Vulnerability: Likely [red arrow]
- Description: [red arrow]

At the bottom, the 'Update' button is highlighted (7).

# All lazy service-owners need to know



- Criticality determines the impact of a service outage for **THE BUSINESS** (CERN as a whole).
- The higher the criticality, the more effort is necessary to mitigate risks.

The screenshot shows the CERN Service Portal interface. At the top left, a red arrow points to a green circle with the number '1' next to the URL 'cern.ch/service-portal'. In the top right, a red circle with the number '2' is next to the 'CERN Service Portal' link in the navigation menu. Below the main header, the 'Storage Service for Projects & Experiments' page is shown. A red circle with the number '3' highlights the 'Edit' button. On the left, a form for 'Personnel Support Service' is visible. A red circle with the number '4' highlights the 'Business criticality' dropdown menu, which is open to show options from '1 - Nil' to '10 - Catastrophic'. At the bottom of the form, a red circle with the number '5' highlights the 'Update' and 'Save' buttons.

- Find your service(s) from the service portal..
1. Click link on cern homepage and search for your service(s)
  2. Option 2: Search portal from CERN homepage
  3. Click Edit on your service's page in the portal
  4. Select appropriate criticality in Business Criticality drop down
  5. Save or Update → That's ALL!!!!!! (thanks for your attention)



# For the ones that want to know more:

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Criticality}$$

Criticality (impact if we 'loose' the service)					
		Factor	DG scale	Criteria to help in the classification of criticality	Safety Risk
Minor	Nil	1	1	very few people affected; people can work on 'other' activities; workaround exists; cost < 1KCHF; safety is not affected; only visible in small contained area; no reputation issue	Nil / Very Limited
	Hardly visible	2	1	several people affected; cost <5KCHF; safety is not affected; not visible outside CERN; no reputation issue	
	Very limited	3	1	small group of people affected; cost <10KCHF; safety is not affected; not visible outside CERN; no reputation issue	
Average	Limited	4	1	considerable number of people affected (>20); cost <20KCHF; possibly affecting people outside central services; no reputation issue	Limited
	Visible	5	1	considerable number of people affected (>50); cost <50KCHF; possibly affecting people outside CERN; CERN reputation possibly slightly affected	
	Significant	6	1	considerable number of people affected (>100); cost <100KCHF; seriously affecting considerable population inside and outside CERN; CERN reputation possibly affected	
Major	Very significant	7	2	considerable number of people affected (>500); cost <400KCHF; seriously affecting very significant population inside and outside CERN; CERN reputation most likely affected	Significant
	Important	8	2	large number of people affected (>1000); cost <1MCHF; very seriously affecting large population inside and outside CERN; significant risk to CERN reputation	
Critical	Disastrous	9	3	large number of people affected (>1000); cost <10MCHF; affecting very large population inside and outside CERN; putting survival of CERN at risk; possible serious injuries	Major
	Catastrophic	10	5	large number of people affected (>1000); cost >10MCHF; affecting large population inside and outside CERN; putting survival of CERN at big risk; possible loss of life	



# Criticality in Service-Now (Service Element)

Welcome: Reinoud Martens Admin

Business Services

- CERN Service Catalog
  - Service Elements
  - Functional Elements
- My Assignments
  - My Service Elements
  - My Functional Elements
- Configuration
  - Functional Element Parameter
- Reports
- Functional Element colors
- Service Element colors
- System Import Sets
- Import Set Tables
  - JDBC ORACLE CSC Service Element
  - JDBC ORACLE Element Links Relati
  - JDBC ORACLE Elements Links Rela
  - JDBC ORACLE Service Element Info

Service Element = Required field

This Service Element contains 4 relationship with impact A. Please consider changing any of them to have a proper configuration with only one relationship with the

Name: Personnel Contract Lifecycle Service

Customer Service: Personnel Support Service

Customer Group: Personnel Contract Lifecycle Service Customers

Service Owner Group: Personnel Contract Lifecycle Service Owners

Lifecycle phase: Retired

Visibility: CERN

Service hours:

Support hours:

Operational hours:

Portal URL Alias: personnel-contract-lifeyc

SLA notifications:

Business criticality: 4 - Limited

General description: This service provides support on all contract-related matters from contract preparation to signing, updating, modifying, extending and terminating contracts.

Capacities:

Business criticality options:

- 1 - Nil
- 2 - Hardly visible
- 3 - Very limited
- 4 - Limited
- 5 - Visible
- 6 - Significant
- 7 - Very significant
- 8 - Important
- 9 - Disastrous
- 10 - Catastrophic

6 - Significant  
considerable number of people affected (>100); cost <100KCHF; seriously affecting considerable population inside and outside CERN; CERN reputation possibly affected

Defined on Service Element level, maintained by service-owner

1. Select the service from the 'My Service Elements'
2. Select appropriate criticality from drop down menu
3. Hovering over menu options shows hints
4. Save your changes (Save or Update button on bottom of screen).



# Criticality: alternative route to your Service Element

Home > Search: stores > Material Request Service

Reinoud Martens Admin [Log out] Français

## CERN Service Portal

easy access to services at CERN

Search:

stores

[Home](#) [News](#) [Navigate Catalogue](#) [Contacts](#) [My Profile](#) [Site Guide](#) [Service Status](#)

### Contacts

#### Central Stores and Stores Urgency window

Phone: + 41 22 767 3902  
Location: 73/R-002  
Working days from 07:30 to 11:50 and from 13:00 to 16:15

#### Special clothes & shoes stores

Phone: + 41 22 767 3902  
Location: 73/R-002  
Working days from 13:30 to 15:30

#### Stores: chemical products

Phone: +41 22 767 3109

### SE Material Request Service Edit 1

This service is responsible for handling material requests including materials supply. Features provided include market surveys and price enquiries, handling of contracts for standard items as well as orders for non-standard items including.

**Keywords**  : logistics, materials provision, materials supplies, standard items, non-standard items, SCEM, CERN catalog, stores catalog, material request, logistique, provisions, fournitures, matériel standard, CERN catalogue, requête matériel, Urgency Window, Urgency counter, Stores Urgency window, gas, gaz, aftersales, apres-vente, Retour de matériel Bossard, Distrelec, Farnell, Lyreco, Radiospares, SFS, store, stores, magasin central stores Stores Urgency, Stores urgency window Safety masks, Safety mask

### Service Element Requirements

Name: Material Request Service 2

Customer Service: Material and Storage Service

Customer Group: Material Request Service

Service Owner Group: Material Request Service

Lifecycle phase: Operation

Visibility: CERN

Service hours:

Support hours: Working Days From 07:30 To 11:50 And From 13:00 To 16:15

Operational hours: Alltime

Portal URL Alias: material-request

SLA:

Business criticality: 4 - Limited 3

General description:

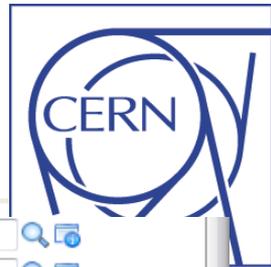
This service is responsible for handling material requests including materials supply. Features provided include market surveys and price enquiries, handling of contracts for standard items as well as orders for non-standard items including.

Capacities:

You can also get to your service via the service portal.

1. Service-Owners have an Edit option on their service pages.
2. This opens the service element maintenance page
3. From where the Criticality field can be changed.

# Criticality in Service-Now (Functional Element)



Name:	Stores Urgency Counter	Functional Manager Group:	Stores Urgency Counter Functional Manager
Organic Unit:	GS-IS-SO	1st Line Support Group:	Service Desk
Organic Group:	GS-IS	2nd Line Support Group:	Stores Urgency Counter 2nd Line Support
Delivered by Organic Unit:		3rd Line Support Group:	Stores Urgency Counter 3rd Line Support
Lifecycle phase:	Operation	4th Line Support Group:	Stores Urgency Counter 4th Line Support
Visibility:	CERN	OWH Support Line:	Stores Urgency Counter OWH
Portal URL Alias:	stores-urgency-counter	Ticket visibility:	Restricted
SLA notifications:	<input type="checkbox"/>	Business criticality:	4 - Limited
General description:	Delivery of urgent orders and manage material return.	Keywords:	urgent orders, demandes urgentes, 54.50.40.900.1 , counter, guichet des urgences, Central store Magasin central, material return, materials returned, retour de matériel, reprise de matériel , commander, commande, matériel sous garantie, téléphones, telephones sous garantie, Material Return, manage material return.proforma invoice, guichet d'urgences
Worklog:			
Related Items:	Show 4 Levels		
Downstream relationships	Upstream relationships		
Stores Urgency Counter	Stores Urgency Counter Material Request Service		
<input type="button" value="Update"/>	<input type="button" value="Save"/>	<input type="button" value="Delete CI"/>	

1. Calculated from Service-Element criticality  
Read only, can not be changed.
2. Depends on relationships



# Threats, Vulnerabilities and Risks in Service-Now

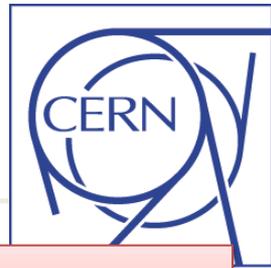
Out of the box “Governance, Risk and Compliance” (or GRC) module

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Criticality}$$

Risk name	Threat	Vulnerability	Risk	Risk Class
Material Failure / Loss of Tool / Function / Data for Stores Urgency Counter	Material Failure / Loss of Tool / Functi...	Likely	192	4
Disaster for Stores Urgency Counter	Disaster	Unlikely	48	4
Single point of failure / No plan B / Strike for Stores Urgency Counter	Single point of failure / No plan B / St...	With difficulty	96	4
Confidentiality / Legal / Reputation for Stores Urgency Counter	Confidentiality / Legal / Reputation	Improbable	48	4
Inside Attack (Intentional Malicious Acts / Fraud / Hacking) for Stores Urgency Counter	Inside Attack (Intentional Malicious Act...	With difficulty	80	4
External Attack (Hacking, Computer Virusses) for Stores Urgency Counter	External Attack (Hacking, Computer Virus...	With difficulty	96	4
Terrorist Attack for Stores Urgency Counter				

1. Select Risks tab at bottom of functional element page
2. Risk Name is concatenation of Threat and Functional Element (calculated field)
3. Risk = Threat \* Vulnerability \* Criticality (calculated field)
4. 4 Risk Classes depending on Risk Level (calculated field)

Risk Class	Threshold	Description
I	300	Intolerable risk
II	200	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
III	100	Tolerable risk if the cost of risk reduction would exceed the improvement gained
IV		Negligible risk



# Editing a Risk

A risk record will be pre created for all combinations of function and threat (for existing functions);  
Functional managers can correct or delete these records (if irrelevant), and also add risk records when appropriate.

Links (2) | Activities (2) | Provided goods and products | Functional Element Categories | Functional Element Parameters | Questionnaires (3) | Knowledge | **Functional Element Risks (8)**

Functional Element Risks ▾ **New** Go to Risk name ▾  🔍

▸ Risks

	Risk name	Threat	Vulnerability	Risk	Risk Class
<input type="checkbox"/>	Inside Attack (Intentional Malicious Acts / Fraud / Hacking) for Stores Urgency Counter	Inside Attack (Intentional Malicious Act...	Quite easily	160	3

← Risk Update Save Delete

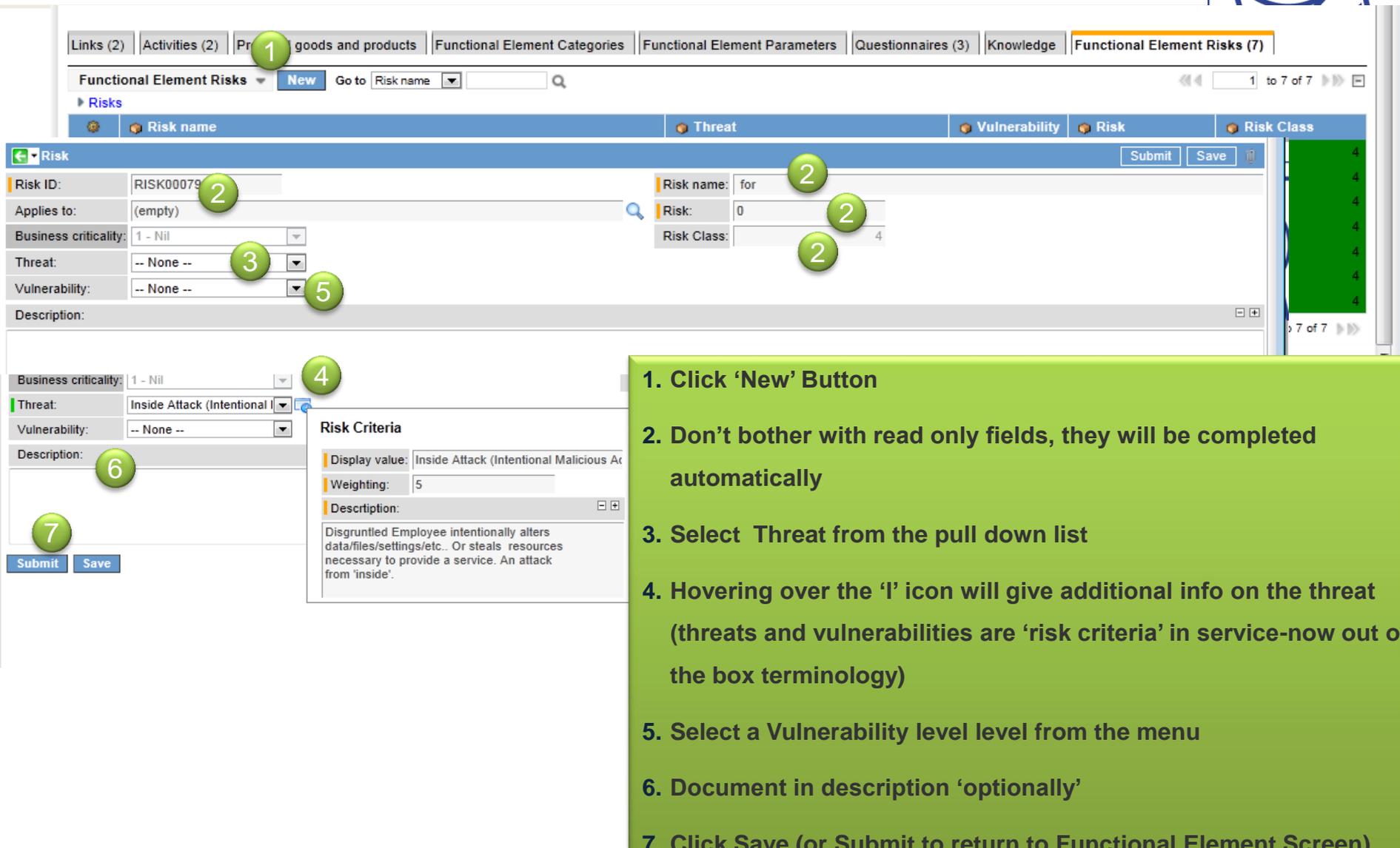
Risk ID:	RISK0007910	Risk name:	Inside Attack (Intentional Malicious Acts / Fraud / Hacking) for Stores Urgency Counter
Applies to:	(empty)	Risk:	160
Business criticality:	4 - Limited	Risk Class:	3
Threat:	Inside Attack (Inter...)		
Vulnerability:	Quite easily		

Description:

Update Save Delete

1. Name, Risk and Class fields are automatically 'calculated'
2. To edit, click on the 'I' icon or the 'Risk name'
3. Adjust Vulnerability and add comments (description);
4. You can change the Threat but you risk to create 'duplicates'  
(another risk record with the same threat will likely exist already).
5. Hit Update or Save (depending where you want to go)
6. To Delete a risk, click the Delete button.

# Entering a new Risk



1. Click 'New' Button

2. Don't bother with read only fields, they will be completed automatically

3. Select Threat from the pull down list

4. Hovering over the 'i' icon will give additional info on the threat (threats and vulnerabilities are 'risk criteria' in service-now out of the box terminology)

5. Select a Vulnerability level level from the menu

6. Document in description 'optionally'

7. Click Save (or Submit to return to Functional Element Screen)



# Reporting and reference data

Welcome: Reinoud Martens Admin | Update Set: Default | Logout

1. Filter field: risk

2. Risk Criteria: Administration, Risk Conditions, Risk Assessments, IT GRC, Risks, Administration, Risk Criteria, Risk Approach Rules, System Import Sets, Import Set Tables, partial risk, Risk Assessments from DEV, risk list, Risk PRDO

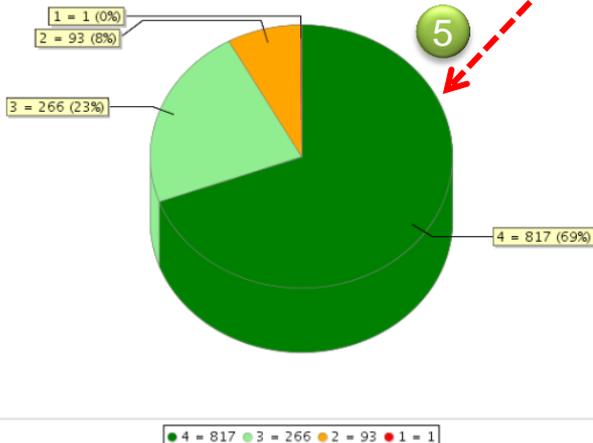
3. Filter: Functional Element Organic Group Name starts with GS > Functional Element Lifecycle phase = Operation

4. Filter: Functional Element Organic Group starts with GS and Functional Element Lifecycle phase is Operation

Functional Element	Risk name	Description	Vulnerability	Risk	Risk Class
Access Cards	Disaster for Access Cards		Unlikely	60	4
Access Cards	Terrorist Attack for Access Ca		Impossible	5	4
Access Cards	Inside Attack (Intentional Malic				
Access Cards	for Access Cards	Could be attractive target..mitigating m...	Quite easily	200	3
Access Cards	Single point of failure / No plan		With difficulty	120	3
Access Cards	Material Failure / Loss of Tool		Likely	240	2
Access Cards	External Attack (Hacking, Con		With difficulty	120	3
Access Cards	Confidentiality / Legal / Reput		With difficulty	120	3
Access Control Systems Design	Material Failure / Loss of Tool		Likely	192	4
Access Control Systems Design	External Attack (Hacking, Con		With difficulty	96	4
Access Control Systems Design	Confidentiality				
Access Control Systems Design	Disaster for Ac				
Access Control Systems Design	Terrorist Attac				
Access Control Systems Design	Inside Attack (				

5. Right-click context menu: Sort (a to z), Sort (z to a), Ungroup, Group By Risk name, Bar Chart, Pie Chart, Personalize, Export (Excel, CSV, XML, PDF), Update Selected, Update All, Import XML

1. Type 'risk' in filter field
2. Risk Criteria show the list of possible Threats and Vulnerability levels (reference data)
3. Select 'Risks' to get a full list of all risks existing in service-now (you can see only for GS we already have close to 1200 risks identified)
4. Use filtering and sorting as usual, and export to excel with right click on 'blue report bar' (see reporting training material for more details)
5. Pie charts etc can be easily made with right click a column....



**COURAGE 😊**