CERN

Engineering
Data
Management
System

EDMS Document No.
Enter EDMS Doc #

CERN Div./Group or Supplier/Contractor Document No.
GS/SMS

Date:26/06/2013

CRITICALITY AND RISK FOR RECURRENT ACTIVITIES

Abstract

This document describes a pragmatic comprehensive approach to risk management for services provided by IT and GS, integrated with the service catalog, and supported by the CERN service management system.

Prepared by :	***Checked by :***	
R. Martens **CERN –GS/SMS** Reinoud.Martens@cern.ch	**C. Delamare (GS)** **D. Foster (IT)** **S. Lettow (DG)** **M. Moller (IT)** **T. Pettersson (GS)**	

History of Changes

Rev. No.	*Date*	*Pages*	*Description of Changes*
1	30/07/2012		Added Appendix 1 on the implementation in service-now Changes to clarify what information is associated to business services and what to functional services, plus how we derive the criticality of a function from the criticality of related services.
2	7/9/2012		Changes in number of threats (reduced from 12 to 7) and their description, on suggestion by D. Foster and T. Pettersson. Improvement in Criticality criteria to take into consideration the 'CERN reputation' aspect. (Suggestion by external consultant).

Table of Contents

1. INTRODUCTION

The aim of a Risk Management process is to support better decision making through a good understanding of risks and their likely impact to the business.

Risk Management involves the identification, selection and adoption of countermeasures justified by the identified risks to assets in terms of their potential impact upon services if failure occurs, and the reduction of those risks to an acceptable level.

During a review of CERN services following an ISO20k approach, we found that we are weak in many areas related to Risk Management:

- Business Continuity and Availability
    - No structured approach to risks analysis.
    - In general no business continuity plans (no prioritization in case of problems).
    - Lack of tests when a recovery possibility exists.
    - No measurement of end user availability.
- Major Incidents handling and reporting.
    - Major incidents managed in ad-hoc improvisation/crisis mode.
- Security
    - Lack of awareness of the issues.
    - Local pockets of excellence (alarms for FB) but no application level security policy yet.
    - Data security policy in its infancy → no clear guidance.

If we want to tackle these issues, we need for a start have a clear idea on

- the criticality of the services we are responsible for (potential impact of service outage),
- the threats (with associated likelihoods) that we can be confronted with, and
- the vulnerabilities of the services to the threats

This document outlines a proposed light weight risk assessment framework that can be implemented and supported as part of the CERN Service Management System.

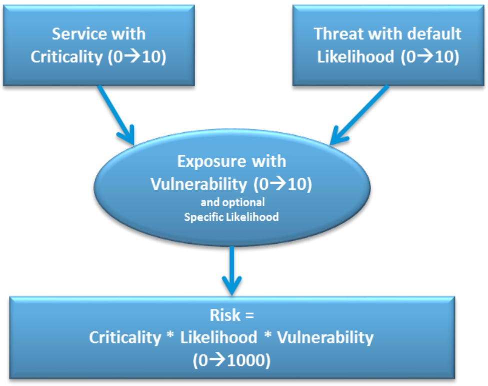
2. HOW

There are two Phases to the process

- Risk Analysis – Understanding the Risks
- Risk Management – Managing the Risks in the "live" environment

Literature shows models that can become exceedingly complex as vulnerabilities are assessed before and after mitigating measures are taken. We suggest simplifying the model to a minimum, by applying a **three step approach**, and incorporating mitigating factors into the vulnerability score.

1. Score each (Customer) Service with regard to its Criticality (or potential Impact) **to CERN**.
   Compute the Criticality of Functions on which the service relies.
2. List Threats and score their Likelihood of occurring
3. Finally assess a Vulnerability score (taking into account existing mitigating factors) on the intersection of a Function and Threat leading to the automatically calculation of the Risk



From this value we can understand whether further Risk Mitigation is required and we can take action - the **Risk Management** Phase.

Note: in comparison with other literature:
Risk is often defined as Probability times Impact. (Risk=Probability*Impact)
The Criticality of a service is the Impact of the service not being available. (Criticality=Impact)
Probability is here broken down into

- A Threat with a Likelihood and
- An Exposure with a Vulnerability

This greatly simplifies the risk assessment (**Probability=Threat*Vulnerability**) as one can think of the threat and the vulnerability separately.

2.1 SERVICES AND CRITICALITY

Below we propose criticality classification guidelines. The “DG scale” is present for ‘backward compatibility’; this was the classification proposed some years ago.
Criticality and Impact reflect the same notion and can be interchanged for the purpose of this document.
The safety risk column was added after feedback from various group leaders demanding not only number of people and cost factors should be considered in the classification but safety aspects are also taken into account.

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	

It must be noted that levels 9 and 10 are outside the scope of the ‘service management system’ and thus outside the scope of this document. A ‘crisis management’ project is ongoing at CERN to cover this area.

These guidelines can also be used to assess the impact of incidents.

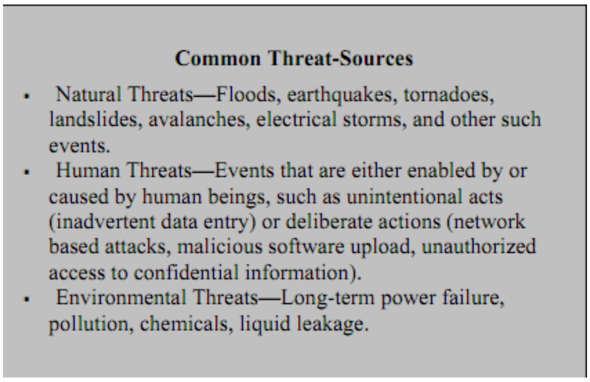
Criticality applies to business services. The CERN service catalogue contains the relations between business services and ‘functions’. Further down we’ll explain how the criticality of a function is derived from the criticality of the related services.

2.2 THREATS AND LIKELIHOOD

Likelihood it happens (in spite of our Prevention)		Factor	Frequency	DG scale
No (once > 10 years)	Impossible	1	Less than once in a lifetime	1
	Almost impossible	2	Once in a lifetime	1
	Very unlikely	3	More than 25 years	1
Maybe (once in 5-10 years)	Unlikely	4	Every 25 years	2
	Little plausible	5	Every 10 years	2
	Plausible	6	Every 5 years	3
	Likely	7	Every 2.5 years	3
Yes (once < year)	Very likely	8	Every year	4
	Almost certain	9	Every month	4
	Certain	10	Every day	4

Threat and likelihoods can e.g. depend on location (e.g. an Earthquake is more likely in Italy or Japan than in Sweden possibly) or other factors. We considered it useful to define a 'default' likelihood for threats, in order to simplify the risk assessment. Likelihood of an earthquake to CERN is the same for all services at CERN.
The DG scale was again added for reference only.

Below you can find a proposed list of threats and their associated proposed likelihood levels.
It is suggested the values are set once (by voting of a team of experts), and may be reviewed whenever necessary.



Common Threat-Sources

- Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage.

Threat	Nature	Likelyhood	Event	On what	By what	Mitigation/Prevention	Frequency	Financial / Image loss
T1	Disaster	4	Flood, Storm, Earthquake, Fire destroys part of infrastructure, Plane Crash	All assets	Nature / GOD	Backups / Disaster recovery plan	Every 25 years	>100 Million
T2	Confidentiality / Legal / Reputation	6	CERN is legally reponsible (software disseminated) or confidential personnel data is disseminated; Confidential information falls in the 'wrong' hands. CERN infrastructure is used as platform to propagate or launch cyber attacks, or disseminate intellectual property protected material.	Storage media; Network; All data (including physical files); IT infrastructure	Externals and possibly (ex) internals	Procedures, Physical protection, Encryption	Every 5 years	1M
T3	Inside Attack (Intentional Malicious Acts / Fraud / Hacking)	5	Disgruntled Employee intentionally alters data/files/settings/etc.. Or steals resources necessary to provide a service. An attack from 'inside'.	All assets	Internals and possibly (ex) internals	Guards, Physical protection, Special monitoring	Every 10 years	?
T4	Terrorist Attack	1	Physical sabotage, bomb, gas, etc..	All assets	Terrorists	Guards, Physical protection	Less than once in a lifetime	>100 Million
T5	External Attack (Hacking, Computer Virusses)	6	Sql Injection ; Buffer overflows, etc… cause File corruption	Desktop and servers	Externals and possibly (ex) internals	Firewall; AntiVirus; Enforced Procedures (for password policy, etc..)	Every 5 years	
T6	Material Failure / Loss of Tool / Function / Data	8	Wrong manipulation; Software bug; Material Failure (CPU/Disk/Network/Power/Machine failure; but also a falling tree, a collapsing roof, heating or airconditioning stops due to lack of maintenance etc..)	All assets	Power Spikes; Old Age; Weather (Cold/Hot/Wind/Rain/Snow)	Redundancy, Preventive Maintenance, Backups	Every year	?
T7	Single point of failure / No plan B / Strike	6	One person having essential knowledge is absent; one critical piece of equipment has breaks without spare; You can't obtain service from elsewhere on short notice; Support teams stop working	Support or Service	Illness, personnel turnover, component not produced anymore; Bad Contract/CERN Staff Relations	Redundancy	Every 5 years	

2.3 VULNERABILITY

Vulnerability is the level to which an Asset (Service/Function) is exposed to a Threat.
As mentioned earlier if a certain region in Italy is exposed to an earthquake with a certain likelihood (say once every 5 years), certain buildings (assets) are possibly designed and build in such a way that their 'vulnerability' to this threat is less than for other buildings. This 'vulnerability' is expressed on a scale of 1 to 10 following these proposed criteria.

Vulnerability of an asset to a threat (after mitigation); the chance a threat if it happens 'breaks' the asset?		
Not	Impossibly	1
	Improbably	2
	Unlikely	3
Maybe	With difficulty	4
	Possibly	5
	Likely	6
	Probably	7
Yes	Quite easily	8
	Easily	9
	Immediately	10

The vulnerability value incorporates the mitigating measures already taken to reduce the 'exposure'. E.g. if a house has been reinforced to withstand earthquakes its vulnerability will be lower than a house without this reinforcement.

2.4 RISK

Risk is now a simple multiplication of Criticality, Likelihood, and Vulnerability.

Once the result known, the risk can be classified in so called risk classes.
Depending on the risk class, mitigating measures might need to be implemented to reduce the exposure.

Risk Class	**Threshold**	
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

The following page shows a prototype of what the result of such a risk assessment could look like. On this spread sheet one can set the thresholds for risk classes, and obviously all other parameters mentioned in this document.

Vulnerability (Capability to protect / detect & react fast; Is this Asset exposed to this Threat; Likelyhood this Threat 'happens' to this Asset)

Not	Impossibly	1
	Improbably	2
	Unlikely	3
Maybe	With difficulty	4
	Possibly	5
	Likely	6
	Probably	7
Yes	Quite easily	8
	Easily	9
	Immediately	10

Enter the Vulnerability level… the Risk will be calculated

Threat*Vulnarability = Probability
Probability*Impact = Risk

Risk = Threat * Vulnarability * Impact --> 1<Severity<1000
If Risk > 200 --> Mitigation

Risk Class	Threshold	
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

Risk

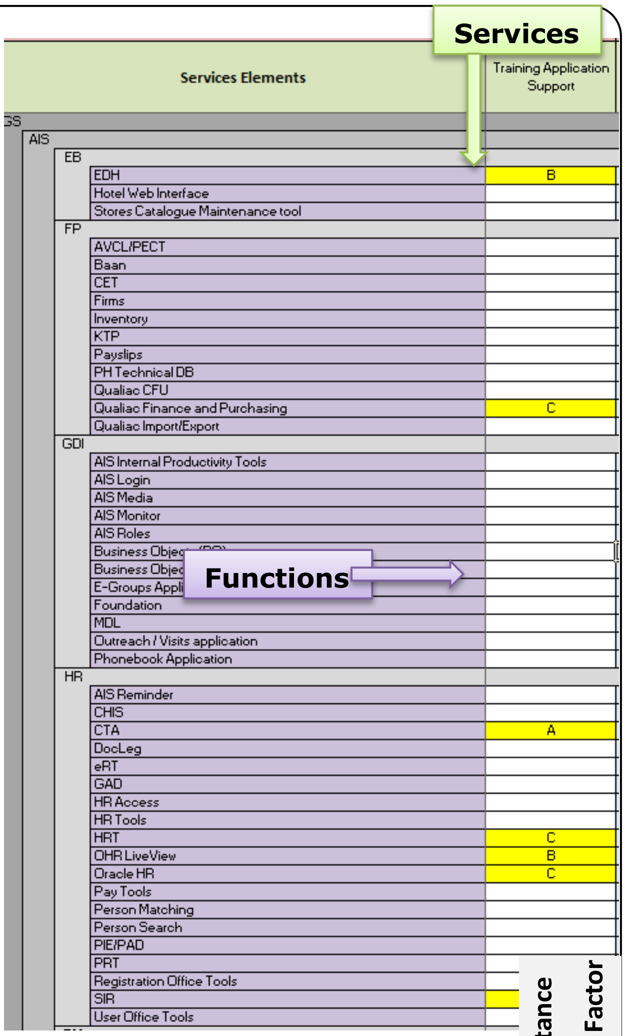
Threats →	Loss of data :5		Virusses :6		Hacking :6		Material Failure :8		Disaster :4		Confidentiality / Legal / Reputation :6		Loss of Tool / Function :8		Strike :7		Terrorist Attack :1		Intentional Malicious Acts / Fraud :5		Single point of failure :6		No plan B available :5	
Functions	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk	Vulnerability	Risk
Catalogue Maintenance	4	60	2	36	4	72	2	48	6	72	1	18	3	72	3	63	4	12	1	15	6	108	2	30
EDH	4	160	5	240	6	288	2	128	6	192	6	288	3	192	3	168	4	32	5	200	2	96	6	240
Hotel Web Interface	4	100	4	120	7	210	2	80	6	120	8	240	3	120	3	105	4	20	7	175	4	120	2	50
AVCL/PECT	4	120	2	72	4	144	2	96	6	144	6	216	3	144	3	126	4	24	6	180	4	144	2	60
Baan	4	140	2	84	4	168	2	112	6	168	2	84	3	168	3	147	4	28	4	140	4	168	2	70
CET	4	140	2	84	4	168	2	112	6	168	2	84	3	168	3	147	4	28	4	140	3	126	2	70
Firms	4	80	2	48	4	96	2	64	6	96	5	120	3	96	3	84	4	16	4	80	4	96	2	40
Inventory	4	60	2	36	4	72	2	48	6	72	2	36	3	72	3	63	4	12	4	60	4	72	2	30
KTP	4	100	2	60	4	120	2	80	6	120	7	210	3	120	3	105	4	20	6	150	4	120	2	50
Payslips	4	80	2	48	4	96	2	64	6	96	8	192	3	96	3	84	4	16	6	120	2	48	2	40
PH Technical DB	4	60	2	36	4	72	2	48	6	72	3	54	3	72	3	63	4	12	4	60	2	36	2	30
Qualiac CFU	4	100	2	60	4	120	2	80	6	120	8	240	3	120	3	105	4	20	4	100	2	60	2	50
Qualiac Finance and Purchasing	4	160	2	96	4	192	2	128	6	192	7	336	3	192	3	168	4	32	6	240	2	96	2	80
Qualiac Import/Export	4	140	2	84	4	168	2	112	6	168	2	84	3	168	3	147	4	28	4	140	2	84	2	70
Addressage Courier	4	60	2	36	4	72	2	48	6	72	2	36	3	72	3	63	4	12	4	60	2	36	2	30
AIS Login	4	120	2	72	4	144	2	96	6	144	2	72	3	144	3	126	4	24	4	120	2	72	2	60
AIS Media	4	160	5	240	4	192	2	128	6	192	2	96	3	192	3	168	4	32	4	160	2	96	2	80
AIS Monitor	4	20	2	12	4	24	2	16	6	24	2	12	3	24	3	21	4	4	4	20	4	24	2	10
AIS Roles	4	120	2	72	4	144	2	96	6	144	2	72	3	144	3	126	4	24	4	120	3	108	2	60
Business Objects (BO)	4	120	2	72	4	144	2	96	6	144	2	72	3	144	3	126	4	24	4	120	2	72	2	60
Business Objects Support Contract	4	120	2	72	4	144	2	96	6	144	2	72	3	144	3	126	4	24	4	120	2	72	2	60
Confluence	4	60	2	36	4	72	2	48	6	72	2	36	3	72	3	63	4	12	4	60	4	72	2	30
E-Groups Application	4	120	2	72	4	144	2	96	6	144	7	252	3	144	3	126	4	24	4	120	2	72	2	60
Experiments & Institutes	4	120	2	72	4	144	2	96	6	144	3	108	3	144	3	126	4	24	4	120	2	72	2	60
Foundation Data	4	160	2	96	4	192	2	128	6	192	8	384	3	192	3	168	4	32	4	160	4	192	2	80
Foundation Other Applications	4	80	2	48	4	96	2	64	6	96	4	96	3	96	3	84	4	16	4	80	2	48	2	40
Gescle	4	100	2	60	4	120	2	80	6	120	3	90	3	120	3	105	4	20	4	100	2	60	2	50
Gesloc	4	120	2	72	4	144	2	96	6	144	3	108	3	144	3	126	4	24	4	120	2	72	2	60
Graybook	4	80	2	48	4	96	2	64	6	96	2	48	3	96	3	84	4	16	4	80	2	48	2	40
Identity Management	4	100	2	60	4	120	2	80	6	120	6	180	3	120	3	105	4	20	6	150	2	60	2	50
JIRA Software Development Tool Suite	4	60	2	36	4	72	2	48	6	72	2	36	3	72	3	63	4	12	4	60	2	36	2	30
MDL	4	80	2	48	4	96	2	64	6	96	6	144	3	96	3	84	4	16	4	80	2	48	2	40
Phonebook Application	4	100	2	60	4	120	2	80	6	120	6	180	3	120	3	105	4	20	4	100	2	60	2	50
Safety (SOS)	4	60	2	36	4	72	2	48	6	72	5	90	3	72	3	63	4	12	4	60	2	36	2	30
Telephone Administration Application	4	80	2	48	4	96	2	64	6	96	7	168	3	96	3	84	4	16	4	80	2	48	2	40
Vertical Line-of-business Applications	4	20	2	12	4	24	2	16	6	24	7	42	3	24	3	21	4	4	4	20	4	24	2	10
Visits	4	80	2	48	4	96	2	64	6	96	6	144	3	96	3	84	4	16	4	80	4	96	2	40
AIS Reminder	4	60	2	36	4	72	2	48	6	72	3	54	3	72	3	63	4	12	4	60	2	36	2	30
CHIS	4	100	2	60	4	120	2	80	6	120	7	210	3	120	3	105	4	20	4	100	2	60	2	50
CTA	4	140	2	84	4	168	2	112	6	168	3	126	3	168	3	147	4	28	4	140	2	84	2	70
DocLeg	4	120	2	72	4	144	2	96	6	144	7	252	3	144	3	126	4	24	4	120	4	144	2	60
eRT	4	100	7	210	5	150	2	80	6	120	8	240	3	120	3	105	4	20	4	100	3	90	2	50
GAD	4	60	2	36	4	72	2	48	6	72	7	126	3	72	3	63	4	12	4	60	5	90	2	30
HR Access	4	140	2	84	4	168	2	112	6	168	7	294	3	168	3	147	4	28	6	210	6	252	2	70
HR Tools	4	100	2	60	4	120	2	80	6	120	7	210	3	120	3	105	4	20	4	100	5	150	2	50
HRT	4	140	2	84	4	168	2	112	6	168	7	294	3	168	3	147	4	28	4	140	4	168	2	70
OHR LiveView	4	80	2	48	4	96	2	64	6	96	7	168	3	96	3	84	4	16	4	80	5	120	2	40
Oracle HR	4	160	2	96	4	192	2	128	6	192	7	336	3	192	3	168	4	32	4	160	4	192	2	80
Pay Tools	4	60	2	36	4	72	2	48	6	72	7	126	3	72	3	63	4	12	6	90	5	90	2	30
Person Matching	4	20	2	12	4	24	2	16	6	24	5	30	3	24	3	21	4	4	4	20	4	24	2	10
Person Search	4	20	2	12	4	24	2	16	6	24	5	30	3	24	3	21	4	4	4	20	4	24	2	10
PIE/PAD	4	100	2	60	4	120	2	80	6	120	6	180	3	120	3	105	4	20	4	100	3	90	2	50
PRT	4	100	4	120	4	120	2	80	6	120	6	180	3	120	3	105	4	20	4	100	4	120	2	50
Registration Office Tools	4	100	2	60	4	120	2	80	6	120	6	180	3	120	3	105	4	20	4	100	4	120	2	50
SIR	4	100	2	60	4	120	2	80	6	120	6	180	3	120	3	105	4	20	4	100	3	90	2	50
User Office Tools	4	120	2	72	4	144	2	96	6	144	7	252	3	144	3	126	4	24	4	120	3	108	2	60
APT Resource Planning	4	100	2	60	4	120	2	80	6	120	4	120	3	120	3	105	4	20	4	100	2	60	2	50
EVM (integrated in APT)	4	100	2	60	4	120	2	80	6	120	4	120	3	120	3	105	4	20	4	100	2	60	2	50

3. FUNCTIONS AND SERVICES

Criticality is defined on business service level, and it represents the 'business impact'; the 'what' view.
To assess the exposure to a threat we need to understand the implementation details (the 'how' view, or function view).
The service-catalogue brings the What and How worlds together.

The service catalogue exposes the relationship between functions (e.g. EDH) and services (e.g. Training Application Support). These relationships have an 'importance' that can be A, B or C. A means the service completely relies on the function, if the function stops, the service is severely impacted (e.g. CTA is the training application, one can see that without CTA, the Training Application Support function is heavily impacted). C means there is a dependency, but the service can run for a while without the function being available (e.g. without Qualiac the training sessions cannot be billed to the participants, so there is an impact; however the training service can easily run without this billing feature for some time).

As mentioned, criticality is set on the business service level. The assessment of vulnerability to threats is performed on the function level (one needs knowledge on how things work to assess exposure to e.g. computer viruses).



Services Elements			Training Application Support
GS			
AIS			
	EB		
		EDH	B
		Hotel Web Interface	
		Stores Catalogue Maintenance tool	
	FP		
		AVCL/PECT	
		Baan	
		CET	
		Firms	
		Inventory	
		KTP	
		Payslips	
		PH Technical DB	
		Qualiac CFU	
		Qualiac Finance and Purchasing	C
		Qualiac Import/Export	
	GDI		
		AIS Internal Productivity Tools	
		AIS Login	
		AIS Media	
		AIS Monitor	
		AIS Roles	
		Business Objec	
		Business Objec	
		E-Groups Appli	
		Foundation	
		MDL	
		Outreach / Visits application	
		Phonebook Application	
	HR		
		AIS Reminder	
		CHIS	
		CTA	A
		DocLeg	
		eRT	
		GAD	
		HR Access	
		HR Tools	
		HRT	C
		OHR LiveView	B
		Oracle HR	C
		Pay Tools	
		Person Matching	
		Person Search	
		PIE/PAD	
		PRT	
		Registration Office Tools	
		SIR	
		User Office Tools	

Thus: once the criticality of services is determined, the criticality of the functions is computed as the maximum of the criticality of related services times a weight factor depending on the importance of their relationship (as shown to the right).

Importance	Weight Factor
A+	1
A	1
B	0.5
C	0.2

Function.Criticality = $\text{Max}_{\text{(For all related services)}}$ (Service.Criticality * Relation.Weight_Factor)

Once the Risks are established for the Functions, one can assess the exposure of a Service to a Threat by inspecting the related functions and applying the same weighting principle the other way around: $\text{Service.Risk}_{\text{(For a Threat)}}$ = $\text{Max}_{\text{(For all related Functions and a Threat)}}$ (Service.Criticality * Threat.Likelihood * Vulnerability * Relation.Weight_Factor)

In fact we use the Service Criticality instead of the Function Criticality in the formula and weight the vulnerability with the weight factor of the importance of the function for the service.

4. SUGGESTED NEXT STEPS

The various notions presented in this document are now supported by the service management system.
The concepts were validated by GS and IT management.
The business service criticality should be defined by the customer, however in absence of a customer we propose that this assessment is done by peers, and validated by major stakeholders.
The threat list can also be validated by a team of people that could determine the likelihood values through a ‘voting’ process.
The vulnerability values should be proposed by the ‘specialists’ of each function as these people know the implementation details necessary to make the correct assessment. The values should be vetted by a small group of experts in order to guarantee coherency across the board.

5. CONCLUSION

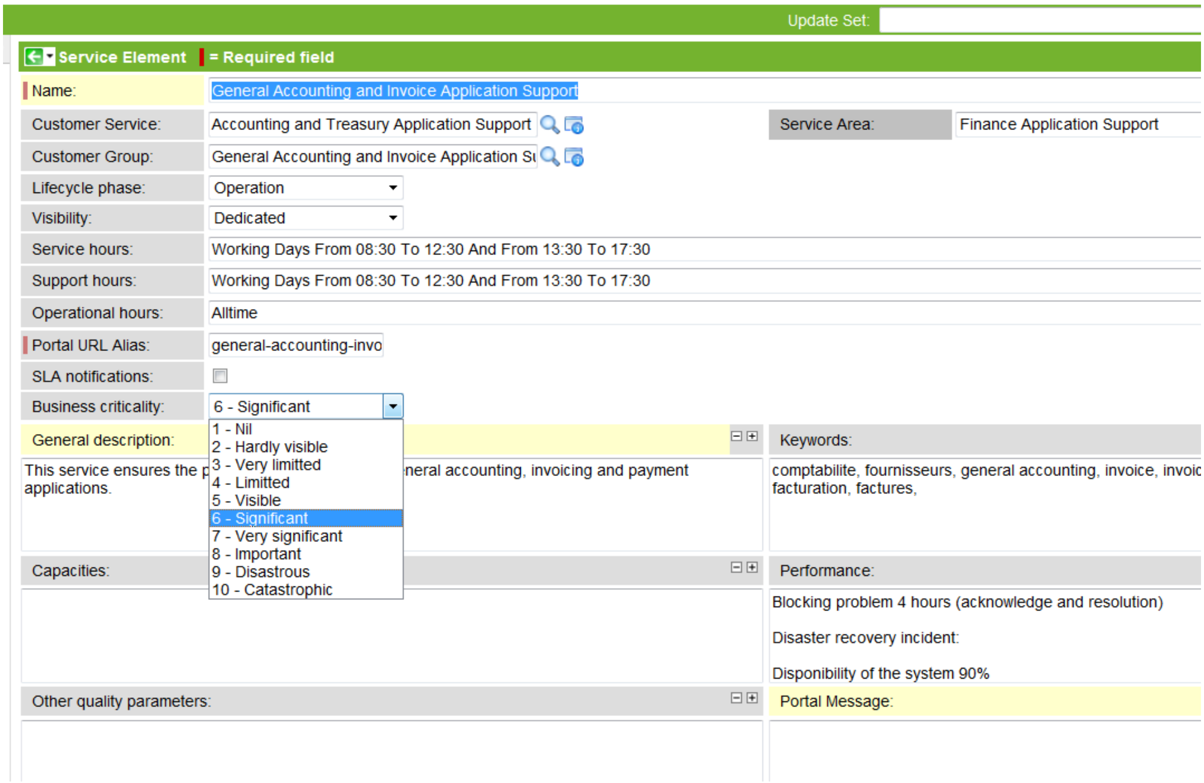
This light weight risk assessment would constitute a significant improvement to the maturity of CERN’s service management system, although it’s just a first step to improve the situation in the areas of business continuity and availability management.
An agreed classification of Criticality (Impact) is also necessary to implement major incident handling.

APPENDIX 1: IMPLEMENTATION

Practical implementation in Service-Now of the concepts presented in this paper.

Service-now contains a “Governance, Risk and Compliance” (or GRC) module. This module can be used out of the box, with very minor changes

The Criticality of a Functional and Service are stored as ‘Business Criticality’ attributes of a service element (Read/Write) and functional element (Read only computed attribute).



Update Set:

Service Element | = Required field

Name:	General Accounting and Invoice Application Support		
Customer Service:	Accounting and Treasury Application Support	Service Area:	Finance Application Support
Customer Group:	General Accounting and Invoice Application Su		
Lifecycle phase:	Operation		
Visibility:	Dedicated		
Service hours:	Working Days From 08:30 To 12:30 And From 13:30 To 17:30		
Support hours:	Working Days From 08:30 To 12:30 And From 13:30 To 17:30		
Operational hours:	Alltime		
Portal URL Alias:	general-accounting-invo		
SLA notifications:	□		
Business criticality:	6 - Significant		

Business criticality options: 1 - Nil
2 - Hardly visible
3 - Very limitted
4 - Limitted
5 - Visible
6 - Significant
7 - Very significant
8 - Important
9 - Disastrous
10 - Catastrophic

General description:

This service ensures the p … neral accounting, invoicing and payment applications.

Keywords:

comptabilite, fournisseurs, general accounting, invoice, invoic facturation, factures,

Capacities:

Performance:

Blocking problem 4 hours (acknowledge and resolution)

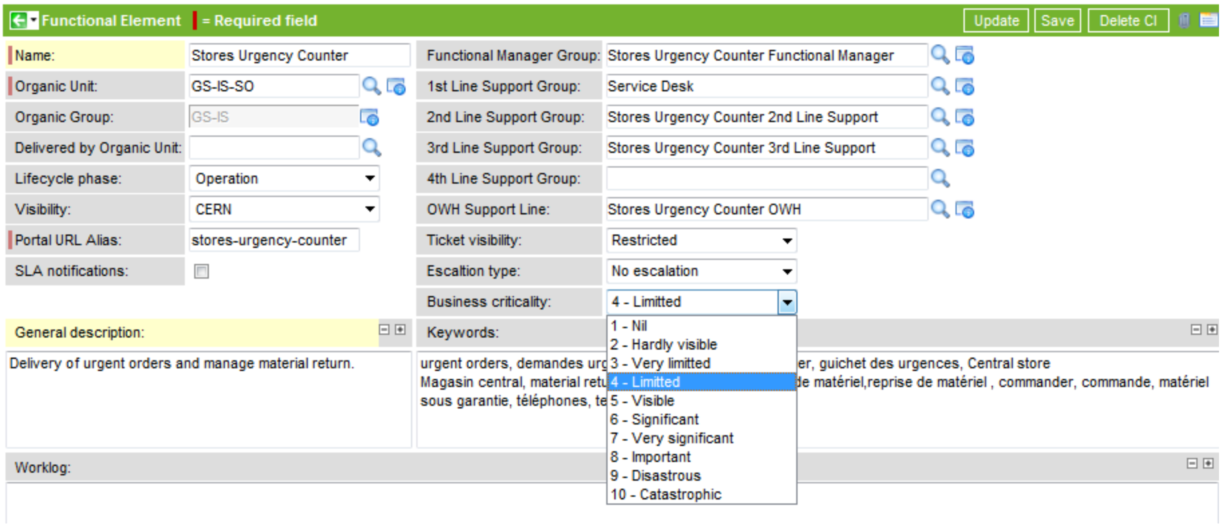
Disaster recovery incident:

Disponibility of the system 90%

Other quality parameters:

Portal Message:

The function’s business criticality is calculated and is ‘read only’.



Functional Element | = Required field

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:	
Visibility:	CERN	OWH Support Line:	Stores Urgency Counter OWH
Portal URL Alias:	stores-urgency-counter	Ticket visibility:	Restricted
SLA notifications:	□	Escaltion type:	No escalation
		Business criticality:	4 - Limitted

Business criticality options: 1 - Nil
2 - Hardly visible
3 - Very limitted
4 - Limitted
5 - Visible
6 - Significant
7 - Very significant
8 - Important
9 - Disastrous
10 - Catastrophic

General description:

Delivery of urgent orders and manage material return.

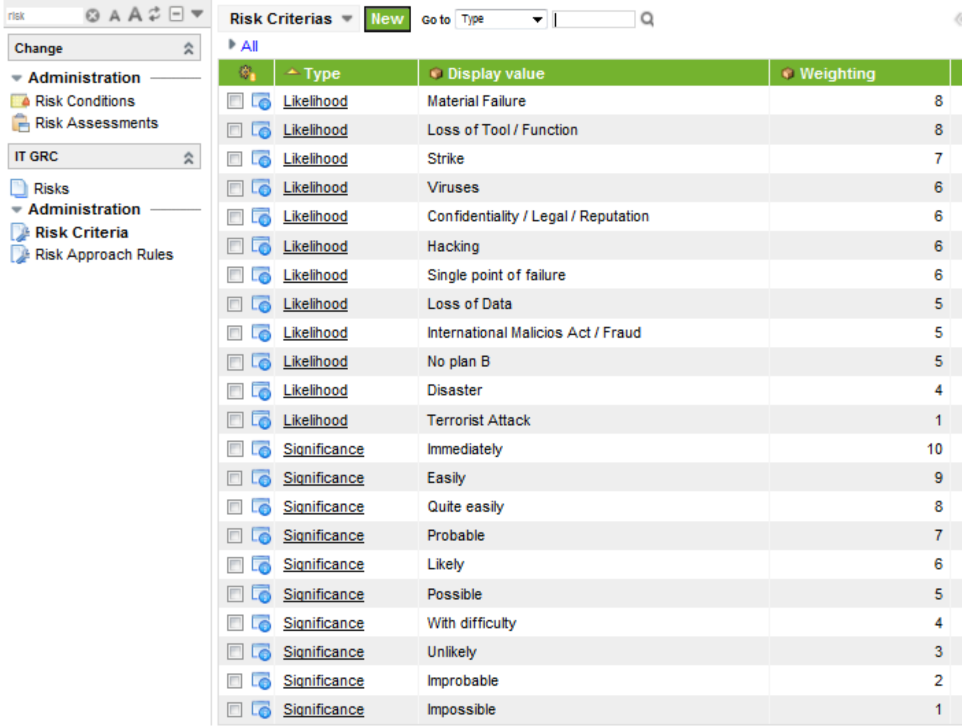
Keywords:

urgent orders, demandes urg … er, guichet des urgences, Central store
Magasin central, material retu … de matériel,reprise de matériel , commander, commande, matériel
sous garantie, téléphones, te

Worklog:

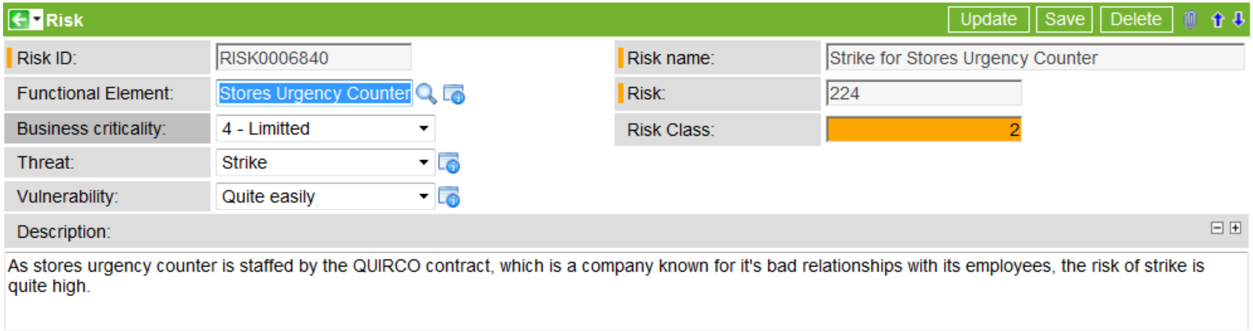
The Threats are implemented as “Risk Criteria’s” (of type Likelihood) with a weight. Adjusting this weight will impact all the associated risks.

Vulnerabilities were implemented as “Risk Criteria’s” (of type Significance) with a weight.



	Type	Display value	Weighting
□	Likelihood	Material Failure	8
□	Likelihood	Loss of Tool / Function	8
□	Likelihood	Strike	7
□	Likelihood	Viruses	6
□	Likelihood	Confidentiality / Legal / Reputation	6
□	Likelihood	Hacking	6
□	Likelihood	Single point of failure	6
□	Likelihood	Loss of Data	5
□	Likelihood	International Malicios Act / Fraud	5
□	Likelihood	No plan B	5
□	Likelihood	Disaster	4
□	Likelihood	Terrorist Attack	1
□	Significance	Immediately	10
□	Significance	Easily	9
□	Significance	Quite easily	8
□	Significance	Probable	7
□	Significance	Likely	6
□	Significance	Possible	5
□	Significance	With difficulty	4
□	Significance	Unlikely	3
□	Significance	Improbable	2
□	Significance	Impossible	1

Risks are now defined as the combination of a threat and a functional service. In the example below ‘Strike’ for ‘Stores Urgency Counter’. The Vulnerability (Significance) is the only attribute that needs to be set on this level. The Risk and Risk Class are automatically calculated.

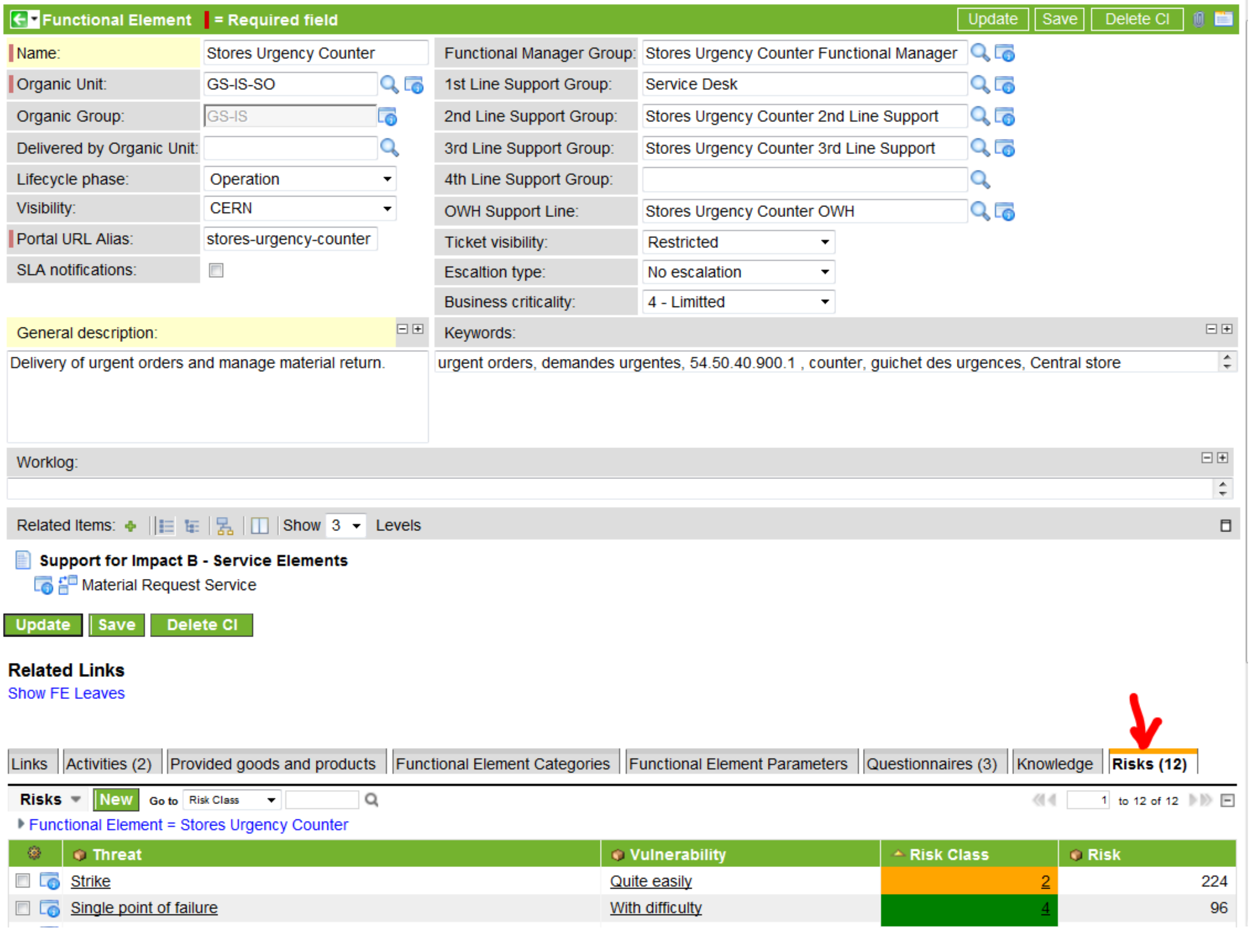


Risk ID:	RISK0006840	Risk name:	Strike for Stores Urgency Counter
Functional Element:	Stores Urgency Counter	Risk:	224
Business criticality:	4 - Limitted	Risk Class:	2
Threat:	Strike		
Vulnerability:	Quite easily		

Description:

As stores urgency counter is staffed by the QUIRCO contract, which is a company known for it's bad relationships with its employees, the risk of strike is quite high.

One can visualise the risks in many ways, but one easy way is to access and correct risks from a tab in the functional element maintenance screen.



Functional Element | = Required field

Update | Save | Delete CI

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:	
Visibility:	CERN	OWH Support Line:	Stores Urgency Counter OWH
Portal URL Alias:	stores-urgency-counter	Ticket visibility:	Restricted
SLA notifications:	☐	Escaltion type:	No escalation
		Business criticality:	4 - Limitted

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

Worklog:

Related Items: Show 3 Levels

Support for Impact B - Service Elements
Material Request Service

Update | Save | Delete CI

Related Links
Show FE Leaves

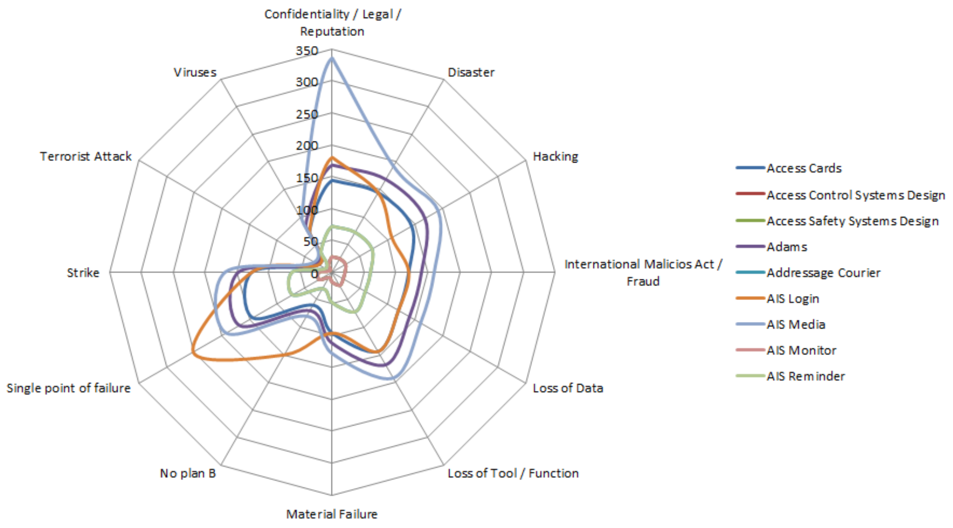
Links | Activities (2) | Provided goods and products | Functional Element Categories | Functional Element Parameters | Questionnaires (3) | Knowledge | **Risks (12)**

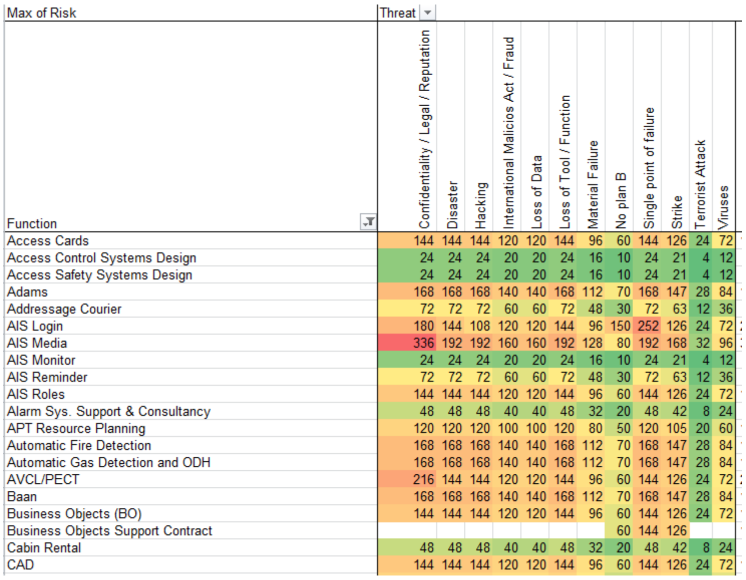
Risks New Go to Risk Class 1 to 12 of 12

Functional Element = Stores Urgency Counter

	Threat	Vulnerability	Risk Class	Risk
☐	Strike	Quite easily	2	224
☐	Single point of failure	With difficulty	4	96

Reports will allow for the analysis and decisions to mitigate risks to bring them below an acceptable threshold.





Max of Risk	Threat											
Function	Confidentiality / Legal / Reputation	Disaster	Hacking	International Malicios Act / Fraud	Loss of Data	Loss of Tool / Function	Material Failure	No plan B	Single point of failure	Strike	Terrorist Attack	Viruses
Access Cards	144	144	144	120	120	144	96	60	144	126	24	72
Access Control Systems Design	24	24	24	20	20	24	16	10	24	21	4	12
Access Safety Systems Design	24	24	24	20	20	24	16	10	24	21	4	12
Adams	168	168	168	140	140	168	112	70	168	147	28	84
Addressage Courier	72	72	72	60	60	72	48	30	72	63	12	36
AIS Login	180	144	108	120	120	144	96	150	252	126	24	72
AIS Media	336	192	192	160	160	192	128	80	192	168	32	96
AIS Monitor	24	24	24	20	20	24	16	10	24	21	4	12
AIS Reminder	72	72	72	60	60	72	48	30	72	63	12	36
AIS Roles	144	144	144	120	120	144	96	60	144	126	24	72
Alarm Sys. Support & Consultancy	48	48	48	40	40	48	32	20	48	42	8	24
APT Resource Planning	120	120	120	100	100	120	80	50	120	105	20	60
Automatic Fire Detection	168	168	168	140	140	168	112	70	168	147	28	84
Automatic Gas Detection and ODH	168	168	168	140	140	168	112	70	168	147	28	84
AVCL/PECT	216	144	144	120	120	144	96	60	144	126	24	72
Baan	168	168	168	140	140	168	112	70	168	147	28	84
Business Objects (BO)	144	144	144	120	120	144	96	60	144	126	24	72
Business Objects Support Contract								60	144	126		
Cabin Rental	48	48	48	40	40	48	32	20	48	42	8	24
CAD	144	144	144	120	120	144	96	60	144	126	24	72