TAS France – Risk Assessment

This document is a partial version for marketing purpose.

The whole and updated version is for internal use only.

1. Overview

The single most important requirement of an information risk management program is that an organisation should be aware of the risks it faces when managing its information. This does not automatically imply that all information assets shall be considered critical and secured, but rather that the organisation is aware of which assets are important and what the attendant risks are. Once the business is aware of the risks it faces, it can manage them in the most convenient and cost effective manner.
The difficult part of an information risk management program is to identify the risks the business faces in the first place. This is not a simple matter for most managers, as there are a large number of factors to take into consideration. This is where a formal risk assessment process comes in handy, as it sums up all of the risks affecting information and enables a clear definition of the most important or pressing countermeasures to take.
This document is about the risk assessment process in place at TAS France. This process is very important, as it assists the company in identifying and evaluating all risks its systems are facing and in justifying a range of complementary security measures to meet those risks. This document will be reviewed at least annually and updated, modified or amended as required by TAS France's Directeur Général. Furthermore, a risk assessment as described in this document will be performed at least annually and upon significant changes to the environment.

2. Scope

This risk assessment applies to all TAS France premises.

3. Risk Assessment Process

3.1. Assets

The risk assessment process put in place at TAS France starts with an evaluation of all mission critical assets and systems the company possesses. Assets are listed according to TAS France's core business goals and its commitments to its customers. The following assets have been identified:

- The whole infrastructure;
- The IT equipment;
- Service level commitments.

3.2. Threat Lifecycle

Recall that risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. TAS France's methodology to assess risks is based on the threat lifecycle and how threats are managed during their lifecycle:

- Before the threat occurs:
    - Threats are identified based on:
        - The experience of TAS France personnel and observed events in the past;
        - TAS France's current data analysis and monitoring tools;

        - External data and documented threats from specialized organisations and businesses;
        - Trends and prospective visions or forecasts.
    - Threats are ranked according to the hereunder severity and probability grid.
    - Threats are tested via monitoring and/or contracts with providers and/or training.

- When the threat occurs:
    - A threat occurrence is observed using monitoring and alerting tools and devices.
    - The immediate severity of the threat is ranked with real time monitoring tools and on-site professionals.
    - The threat is stopped with physical, manual or automatic procedures.

- After the threat occurred:
    - Damages are measured with monitoring tools and manual/visual procedures.
    - Damages are repaired and resilience measures implemented according to the hereunder three levels of resilience (level1, level2, level3).
    - Risk management committees are organized after each threat occurrence, to analyse past occurrences and anticipate next threats, and furthermore at least once a year, to evaluate and update the risk management strategy and action plans.

3.3. Measurement and Update

The risk level is identified according to the grid below, which is provided with a colour code: threats highlighted in green are considered low risk, orange-highlighted threats are moderate, while red boxes denote high-risk threats.

Risk Assessment		**Threat Severity**		
		Low	Moderate	High
Threat Probability	Low	1	4	7
	Moderate	2	5	8
	High	3	6	9

Risks are ranked according to two threat dimensions:

- *Severity*, depending on the damages to critical assets caused by threats exploiting vulnerabilities related to the risk;
- *Probability*, depending on the frequency with which vulnerabilities related to the risk have been exploited in the past or are forecast to be exploited in the future.

The following table contains a brief description of the level-bands used above:

Severity	**High**	High damage to assets, mostly unrepairable, large rebuild necessary

	Moderate	Moderate damage to assets, mostly reparable, partly to rebuild
	Low	No damage to assets, no rebuild, just service delivery check
Probability	**High**	Frequently observed or documented threat, several times a year
	Moderate	Documented or anticipated threat but not observed in the last 5 years
	Low	Documented or anticipated threat but never observed

4. Results

The results of TAS France's risk assessment are presented as a risk assessment grid, which comprises 14 columns and is updated every year:

A. **Ranking**: Threats are ranked from 1 to 12, where 1 denotes the highest risk and 12 the lowest risk.
B. **Threats**: Threat description.
C. **Assets**: Affected assets are identified according to section 3.1.
D. **Last assessment**: The date of the last assessment.
E. **Risk change**: Here YES means that the risk value has changed since the last assessment, while NO means that the risk value has remained the same.
F. **Risk mitigation**: How the risk is mitigated.
G. **Alerting method**: How the risk is detected.
H. **Review / test method**: How the risk mitigation method is reviewed or tested.
I. **Review / test frequency**: How often the risk mitigation method is reviewed or tested.
J. **Last review / test**: Date on which the last review / test was done.
K. **Level 1 resilience**: The first observed result of our resilience policy for restoring normal operational conditions once the threat occurs.
L. **Level 2 resilience**: The next observed result, if level 1 resilience fails.
M. **Level 3 resilience**: The next observed result, if level 2 resilience fails.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Ranking	**Threats**	**Assets**	**Risk assessment**	**Last assessment**	**Risk change**	**Risk mitigation**	**Alerting method**	**Review / test method**	**Review / test frequency**	**Last review / test**	**Level 1 resilience**	**Level 2 resilience**	**Level 3 resilience**
1	Internet outage	Service level commitments	7	31/03/2018	No	Multi operator transit	Network monitoring	Network dashboard and transit alerts	Real time	18/04/2018	Multi operators dynamic routing	Multi operators manual routing	BCP BRP
2	Flood	Whole infrastructure	7	31/03/2018	No	Building features	Humidity sensors	Regular sensors check	Bi-annual	18/04/2018	BCP BRP		
2	Physical intrusion: theft / vandalism / terrorism	IT equipment	7	31/03/2018	No	Intrusion protection devices	Video recorder / alarms	Visual check / tools / monitoring	Real time	18/04/2018	Security firm contract	Local restore	BCP BRP
2	Cyber criminality	IT equipment	7	31/03/2018	No	Intrusion protection policies and software	Network monitoring and intrusion detection tools	Automatic security scans and transit alerts	Real time	18/04/2018	Intrusion blocking procedures	Local restore	BCP BRP
5	Hardware breakdown	IT equipment	6	31/03/2018	No	Redundancy	Hardware monitoring	Availability tests	Real time	18/04/2018	Local redundancy	Local restore	BCP BRP
5	Software breakdown	Service level commitments	6	31/03/2018	No	Software update	Software monitoring	Availability tests / Editors update checks	Real time	18/04/2018	Local redundancy	Local restore	BCP BRP
7	Fire	Whole infrastructure	4	31/03/2018	No	Security standards	Fire detection system	Maintenance contracts	Bi-annual	18/04/2018	Fire extinguishing system (Argo 55)	BCP BRP	
8	Power variation	IT equipment	3	31/03/2018	No	UPS	UPS monitoring	Maintenance contracts	Yearly	18/04/2018	Redundant UPS	BCP BRP	
8	Power outage	Service level commitments	3	31/03/2018	No	UPS and power generator	UPS and power generator monitoring	Maintenance contracts	Yearly	18/04/2018	Power generator	Refuelling process	BCP BRP
10	Earthquake	Whole infrastructure	2	31/03/2018	No	Building features	Hardware and software monitoring	Availability tests	Real time	18/04/2018	Local restore	BCP BRP	
10	Temperature	IT equipment	2	31/03/2018	No	Climate control	Temperature sensors	Regular sensors check	Bi-annual	18/04/2018	Redundant cooling equipment (gas and water)	BCP BRP	
12	Accident	IT equipment	1	31/03/2018	No	Internal security policy	Video recorder	Education session	Yearly	18/04/2018	Local redundancy	Local restore	BCP BRP