Quantitative Risk Assessment with ISAMM on ESA's Operations Data System

Carlo Harpes[(1)], André Adelsbach[(1)], Stefano Zatti[(2)], Nestor Peccia[(2)]

[(1)] Telindus S.A., Security, Audit and Governance Services
81-82, route d'Arlon
L-8009 Strassen, Luxembourg

[(2)] European Space Agency / European Space Operations Centre
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany

ABSTRACT

This paper describes the mathematics behind a quantitative risk assessment method called ISAMM, and results obtained when applying the method to ESA's Operations Data System. ISAMM recurs to the list of security measures of ISO 27002 and attributes to each security control some risk reduction properties. Based on estimates of current risks, on implementation costs of missing security controls, and on risk reduction factors, the economic benefit, the so-called Return on Security Investment (ROSI), is estimated and used to build an action list to improve security. The paper also discusses implementation issues and further steps of an ISAMM project.

1. INTRODUCTION AND CONTEXT

ESOC Darmstadt wanted to improve information security of its Operations Data System in a top-down approach starting with a formal standard risk analysis. A formal standard risk analysis based on ISO/IEC 27002 (formerly ISO/IEC 17799, hereafter referred to as ISO 27002, [1]) security controls was done, followed by a more detailed technological risks and countermeasures evaluation.

ISAMM (*Information Security Assessment & Monitoring Method*) is a methodology of Telindus chosen by ESA, since it comes with an efficient and effective tool to assess both security risk and current compliance with respect to ISO 27002. Furthermore, it delivers an optimized action plan to address the identified risks.

2. ISAMM PRINCIPLES

ISAMM links an assessment of the security risks, expressed in monetary terms as an Annual Loss Expectancy (ALE), with security controls that can most economically contribute to a reduction of the risks.

ISAMM recurs to a state-of-the-art knowledge base with context-dependent risk reducing capabilities of security controls. The knowledge-base can be considered as a matrix containing for each control objective and each of the generic threats (e.g. risk of internal data theft, …, accidental outages due to errors, bugs or bad practice) an estimate of the relative reduction of the risk, provided that this control is implemented.

Thus, we can derive the difference ΔALE of the ALE before and after implementing a security control. Based thereon, the ROSI and relative ROSI are respectively defined as:

$$ROSI = \Delta ALE - Cost \qquad \text{and} \qquad ROSI_{rel} = \frac{\Delta ALE - Cost}{Cost}$$

Both, ROSI and relative ROSI are important indicators to identify the most effective controls (those having the greatest risk reduction capabilities, while having the lowest costs) and to prioritize certain controls. Both calculations are used to evaluate the monetary benefit of each single security control and provide an efficient ordering system for implementation priorities.

3. DETAILED EXPLAINATION OF ISAMM

In the following, we provide a more detailed description of the algorithm calculating the action list.

3.1 Input data

In the current ISAMM assessment we consider a list of 12 generic threats T and a list of 135 security measures M. The latter are the control objectives defined in ISO 27002.

Table 1 - Twelve generic threats considered by ISAMM

Aspect	Threat ID	Description
Confidentiality	C1	Malicious outsiders obtain or access confidential data
Confidentiality	C2	Malicious insiders obtain or access confidential data
Confidentiality	C3	Accidental disclosure of confidential data to insiders
Confidentiality	C4	Accidental disclosure of confidential data to outsiders
Integrity	I1	Malicious modification or alteration by outsiders
Integrity	I2	Malicious modification or alteration by insiders
Integrity	I3	Accidental erroneous modification or alteration
Availability	A1	Denial of service or availability breach caused by malicious persons or code
Availability	A2	lack of resources, know how, supplier support
Availability	A3	Natural disasters as earthquake, flooding, hurricane, lightning, fire, extreme weather conditions or terrorist or industrial (strike) actions
Availability	A4	Day-to day (shorter period) system outages due to nature
Availability	A5	Accidental outages due to errors, bugs or bad practice

In the risk assessment we estimated for each threat T

- the probability of occurrence p_T and
- the expected impact I_T.

In the security measure evaluation, we estimated for each measure M

- The implementation rate or current efficiency e_M. With $\mathbf{e} = (e_1, e_2, ...)$ we denote the current implementation status containing the implementation rates e_1 of the first measure, the rate e_2 of the second measure, etc. In general, e_1 equals 0%, 25%, 50%, 75%, or 100%.
- The residual annual cost required to achieve full compliance $cost_M$ (not including cost of those elements that are already in place), which is estimated according to the following equation:

$$cost_M = \frac{SetupCost}{Lifetime} + SetupCost \cdot SupportRate ,$$

$$SetupCost = IntEffort \cdot IntDailyRate + ExtEffort \cdot ExtDailyRate + HWSW ,$$

where the variables are explained in the Tab. 2.

Table 2 - Agreed parameters to estimate costs of compliance to ISO 27002.

Variables	Description
IntEffort	Number of internal man days needed to make the control to be fully compliant
ExtEffort	Number of external man days needed to make the control to be fully compliant
IntDailyRate	Cost (€ per day) for one internal man day to make the control compliant (i.e. what is the cost of internal human resources per day of work?)
ExtDailyRate	Cost (€ per day) for one external man day to make the control compliant (i.e. what is the cost of an external human resources per day of work ?)
HWSW	Total cost of hardware and software
SupportRate	The cost of maintenance per year, expressed in percent of **SetupCost**
Lifetime	Lifetime of a control expressed in years, i.e., after this amount of years, the control has to be re-implemented and initial investment has to be repeated

3.2. The ISAMM Knowledge Base

ISAMM's knowledge base is a matrix containing for each threat and each security measure the expected relative reduction $r_{T,M}$ of threat *T*'s risk if the measure *M* is implemented.

The risk reduction factors have been estimated after analysing the strength of each suggested control. More precisely, the preventive, detective, impact limitative and corrective properties of each control on each threat have been quantified. Then, based on this quantification, the effect of the control on each threat is estimated. Finally, risk reduction parameters can be either estimated optimistically, pessimistically, or neural. The risk reduction parameters can therefore be weighted by an additional parameter, called "mode", and calculated as a function of all these inputs.

Example of risk reduction factors

We consider two security controls and their risk reduction capabilities. More concretely, we have chosen the ISO control CTRL75 (Access control policy), which is the top security control in the context of ESA and CTRL126 (Identification of applicable legislation).

CTRL. ID	RISK REDUCTION FACTORS $r_{T,M}$ (%)											
	C1	C2	C3	C4	I1	I2	I3	A1	A2	A3	A4	A5
75	10	20	2	4	10	20	4	4	0	0	0	4
126	0	2	2	4	0	2	4	2	2	0	2	2

3.3. Terms and formulas

The annual loss expectancy ALE_T for a specific threat T can be derived from probability of occurrence and impact of the threat:

$$ALE_T = p_T \cdot I_T .$$

Based on the *ALEs* for specific threats, the *overall ALE* can be defined as the sum over all threats:

$$ALE = \sum_T ALE_T .$$

Define $ALE_T^{(\mathbf{x})}$ as the annual loss expectancy of threat T given an implementation status $\mathbf{x} = (x_1, x_2, ...)$, where x_1 is the implementation rate of the first security control, x_2 of the second, etc.

Of particular interest is the theoretic quantity $ALE_T^{\mathbf{0}}$, the ALE provided that no security control would have been implemented. We call this the *maximum ALE*.

By definition of risk reduction and implementation rate, the ALE corresponding to a given implementation status **x** can be derived from this maximum ALE:

$$ALE_T^{\mathbf{x}} \quad = \quad ALE_T^{\mathbf{0}} \cdot \prod_M \left(1 - r_{T,M} \cdot x_M\right),$$

and the overall annual loss expectancy for implementation status **x** is obtained by summing over all possible threats :

$$ALE^{\mathbf{x}} \quad = \quad \sum_T ALE_T^{\mathbf{x}} \quad = \quad \sum_T \left(ALE_T^{\mathbf{0}} \cdot \prod_M \left(1 - r_{T,M} \cdot x_M\right)\right).$$

Now we have to consider how to find $ALE_T^{\mathbf{0}}$. Recall that ISAMM estimates the expected impacts and probabilities for the *current* implementation rate of security controls (current compliance level). Thus, if $\mathbf{x} = \mathbf{e}$, we know the values of $ALE_T^{\mathbf{x}}$ from the risk assessment phase, which allows us to extract the maximum ALE.

$$ALE_T^0 \quad = \quad \frac{ALE_T}{\prod_M \left(1 - r_{T,M} \cdot e_M\right)}$$

To conclude, we are able to derive the overall *ALE* for *any* implementation status **x**, based on ISAMM's knowledge base – the parameters $r_{T,M}$ – and the estimate of the current ALE and the current implementation status **e**.

3.4. Basic algorithm

The algorithm defining the action list can be considered as a loop, starting with the current implementation status and putting one by one the implementation rate of different measures to one. In each step of this loop, the following search is done:

1. For each not fully implemented security measure *M*, consider the current implementation status x, and the implementation status x' in which x_M has been set to 1, meaning that the measure *M* has been fully implemented. Then compute the
$$ROSI_M \quad = \quad \left(ALE^{\mathbf{x}} - ALE^{\mathbf{x}'}\right) - Cost_M .$$
2. Find the security measure *M* with the largest ROSI, and add this to the running implementation status (i.e. replace x by the corresponding x').
3. Repeat until the ROSI of the best remaining security measure starts to be negative; in that case the running implementation status is called the optimum security level. This level is optimal in the sense that it is economically justified to implement any measure up to here, and for all remaining measures, the ISAMM estimate shows that an implementation cannot be economically justified.

Note that the risk reduction is computed under the hypothesis that all prior controls have already been implemented. This means that the measures at the end of the action lists (cf. Control 126 in the example below) have smaller indicated ROSI as if they have been implemented before other controls.

In this algorithm, we use the following derived formula to compute the risk reduction of measure *M* based on the 12 ALE situations just before raising the compliance of M from e_M to 100%:

$$(\Delta ALE)_M = \sum_T \left(ALE_T^{before} \cdot r_{T,M} \cdot \left(\frac{1 - e_M}{1 - r_{T,M} \cdot e_M} \right) \right).$$

Example of control's impacts

Below we summarise the ALE reduction and ROSI of control 75 which we have obtained from our ISAMM analysis of ESOC Operations Data System. Note that this control had before implementation a compliance of $e_{75} = 25\%$ and that we suppose it to be the first measure to be implemented, i.e. the ALE before equal the current ALE of the risk assessement. Tab. 3 indicates the values for the formula above.

Table 3 – Example of risk reduction calculation for a given risk situation.

Threat	Probability per year	Impact k€	Current ALE_T k€	Risk Reduction %	Risk Reduction k€
C1	1	2000	2 000	10	154
C2	0,2	2000	400	20	63
C3	0,5	400	200	2	3
C4	0,5	2000	1 000	4	30
I1	0,2	50000	10 000	10	769
I2	0,04	50000	2 000	20	316
I3	0,5	400	200	4	6
A1	0,2	10000	2 000	4	61
A2	0,2	400	80	0	0
A3	0,1	10000	1 000	0	0
A4	2	400	800	0	0
A5	0,5	2000	1 000	4	30
Total		129 600	20 680		1 432

3.5. Extensions of the basic algorithm

The optimisation algorithm, implemented in ISAMM to compute an action plan, can consider some dependencies between controls. We may indicate that a control is a prerequisite for another control. Thus this control max appear in the action list before controls with higher ROSI, simply because it is pushed by the more efficient control to be implemented afterwards.

4. FINDINGS

4.1 Risk Assessment

Given the high value of assets – e.g. of space craft that can be destroyed in case of wrong behavior of the ground segment – the annual loss expectancy is very high, although the frequencies of incidents have been estimated to be rather low compared to common average values. The most significant fraction of the annual loss expectancy stems from loss of integrity, which accounts for about 68%, and availability for about 25%.

Table 4 – Estimated annual loss expectancies of the ESOC Data centre

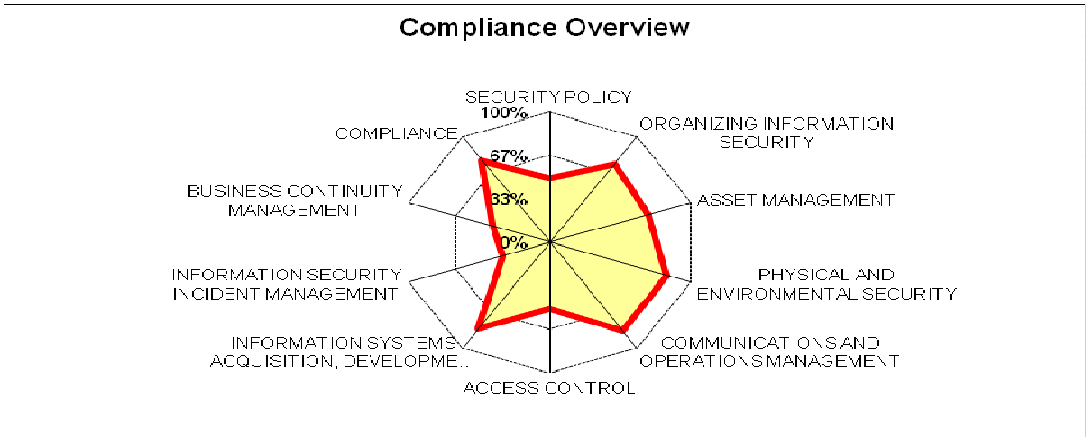
Current ALE	Millons €	%
Confidentiality	1.40	8%
Integrity	12.40	68%
Availability	4.48	25%
TOTAL	18.28	100%

To conclude, it seems adequate to focus on security controls that have high risk reduction capabilities for availability and integrity risks.

4.2. ISO 27002 Security Measure Assessment

In 2006, the compliance to ISO 27002 best practices is estimated as 71%, which is quite a good score. It can be decomposed as follows.

Table 5 – Estimated compliance to ISO 27002 security controls



The overall costs to implement missing control have been estimated to about 4 Mio € or on average 2.2 Mio € yearly, which is a quite high spending, but still far lower than the estimated annual loss expectancy. These costs are mainly due to the high development and testing cost to update access control in the operations software. Due to the large overall investment to achieve full compliance it is necessary to analyse the benefit of recommendations based on ISAMM.

4.3. Action plan

A targeted compliance of 90% will be obtained after having implemented 46 compliance projects for which a positive Return on Security Investment (ROSI) has been estimated.

The overall set-up costs of these projects are estimated to 2.2 Mio € for set-up, or 1.2 Mio € yearly considering lifetime and maintenance. These projects would reduce the ALE by 11.7 Mio € yearly, considering savings resulting from incidents that have been avoided due to improved security. This results in a relative ROSI of 8,6.

Table 6 – Overview of ALE, Cost and Return on investment

Compliance Level	Current Level	Target Level	Full Compliance
Compliance Rate	**71%**	**90%**	**100%**
ALE	**18'280'000 €**	**6'500'607 €**	**6'200'009 €**
Cost			
internal man days		2'333	2'653
external man days		94	144
HW/SW		955'800 €	2'380'800 €
Total set-up		**2'197'500 €**	**3'822'500 €**
Yearly cost		1'230'405 €	2'107'072 €
Risk Reduction		**11'779'393 €**	**12'079'991 €**
ROSI		10'548'988 €	9'972'920 €
relative ROSI = ROSI/Cost		**8.6**	**4.7**

Risks cannot be completely eliminated but they can be reduced by a large amount via the implementation of adequate security controls. As discussed in the previous section, the yearly cost to reach full compliance to ISO 27002 is estimated as 2 218 405 €.

The ISAMM analysis performed by Telindus, shows that the action plan, proposed to reach an optimal compliance level in terms of ROSI, is at a yearly cost of 1 230 405 € , which is significantly lower.

If put in place completely, the security action plan can reduce the annual loss expectancy by about 11 779 393 € for a yearly implementation cost of 1 230 405 € . The overall ROSI is thus about

$$ROSI = 10\,548\,988\ €$$

$$\frac{ROSI}{Cost} = 8{,}6$$

4.3. Recommendations

The most relevant recommendations of the action plan are:

1) Finalise ISO 27001 certification.
2) Organise treatment of identified risks.
3) Define access control policy and implement workflow enforcing access authorisation based on a formal user registration procedure.
4) Improve visibility of management support for security concerns.

5. CONCLUSION

Based on its ISAMM methodology, a list of projects or actions has been produced to achieve an optimum level of security (from an economic perspective). The actions have been selected according to economic criteria based on an estimate of current risks, compliance rate to ISO 27002, and cost of security projects and Telindus' knowledge base of risk reduction capabilities of security measures.

The estimates have been derived from previous studies and refined during interviews. However they still reveal to be quite rough, but precise enough to establish implementation budgets for security projects.

We consider the ISAMM risk assessment of twelve generic risks as a first step towards a full identification and detailed assessment of information security risks as required by an ISO 27001 Information Security Management System (ISMS). It revealed to be very useful for assessing a global picture of the current risk situation, and it derives good information to establish security budgets. We recommend such an approach rather than starting with a more time-consuming risk assessment methodology [3, 4]. In our approach, the ISAMM phase should be followed by the implementation of the most relevant security improvements. In a next step, an asset identification, a refined, more detailed risk assessment, and a full implementation of an information security management system lifecycle as normalised in [2] should be targeted.

ACKNOLEDGMENT

The authors thank Ruddy Meert the inventor of ISAMM and Jean-François Kin from Telindus for introducing ISAMM's basic principles and knowledge base, which have been used in this study.

REFERENCES

[1] ISO/IEC 17799, Information technology – Security techniques – Code of practice for information security manamgement, 2005-06-15

[2] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements, 2005-10-15.

[3] ENISA, Risk Management:Implementation principles and Inventories for Risk Management/Risk, Assessment methods and tools, June 2006.

[4] ENISA Deliverable, Information Package for SMEs With examples of Risk Assessment / Risk Management for two SME, February 2007s.