In Depth Defence applied to Information Systems

Memo

Version 1.1 – 19 July 2004
This document was produced by the DCSSI Advisory Office
(SGDN / DCSSI / SDO / BCS)

Comments and suggestions are encouraged and can be sent to the following address
(see Comment Form at the end of the guide):

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr
Memo on the concept of in depth defence applied to the IS

Contents

INTRODUCTION 5

1.1 STUDY OVERVIEW 5
1.2 DOCUMENT STRUCTURE 5
1.3 BIBLIOGRAPHY 6
1.4 ACRONYMS AND ABBREVIATIONS 7

2 ANALYSIS OF THE CONCEPT 8

2.1 CONCEPTS DESCRIBED IN THE LITERATURE 8
2.1.1 STUDY OF THE MILITARY ARENA 8
2.1.2 STUDY OF THE INDUSTRIAL ARENA 9
2.1.3 STUDY OF THE ISS ARENA 12
2.1.4 CONTEXT ANALYSIS 13
2.2 INTERVIEW RESULTS 15
2.3 CONCLUSIONS FROM THE FIRST PHASE 16

3 IN DEPTH DEFENCE IN ISS 17

3.1 DEFINITION OF THE CONCEPT 17
3.1.1 GENERAL NOTES RELATING TO THE CONCEPT 17
3.1.2 DEFINITIONS 19
3.1.3 GENERAL PRINCIPLES 20
3.2 IMPLEMENTATION OF THE CONCEPT 21
3.2.1 DEPTH OF THE ORGANISATION 21
3.2.2 DEPTH OF IMPLEMENTATION 22
3.2.3 DEPTH IN TECHNOLOGIES 22

4 THE IN DEPTH DEFENCE METHOD 23

4.1.1 STEP ONE: DETERMINE ASSETS AND SECURITY OBJECTIVES 25
4.1.2 STEP TWO: OVERALL SYSTEM ARCHITECTURE 26
4.1.3 STEP THREE: DEVELOP THE DEFENCE POLICY 27
4.1.4 STEP FOUR: QUALIFICATION OF IN DEPTH DEFENCE 28
4.1.5 STEP FIVE: CONTINUOUS AND PERIODIC EVALUATION 30

5 CONCLUSIONS 32

6 APPENDIX APPLICATION OF THE PROPOSED METHOD 34

6.1 OVERVIEW OF THE CASE STUDY 34
6.2 IMPLEMENTATION OF THE METHOD 36
6.2.1 STEP ONE: IDENTIFY THE SECURITY OBJECTIVES 36
6.2.2 STEP TWO: OVERALL SYSTEM ARCHITECTURE 39
6.2.3 STEP THREE: DEVELOP THE DEFENCE POLICY 45
Tables of Figures

FIGURE 1: INES SCALE ........................................................................................................... 9
FIGURE 2: THE THREE BARRIERS ......................................................................................... 10
FIGURE 3: METHODOLOGICAL APPROACHES (SOURCE: [DRA7]) ........................................ 12
FIGURE 4: STRATEGY FOR IDENTIFYING LINES OF DEFENCE ........................................ 18
FIGURE 5: STEPS IN THE METHOD ...................................................................................... 23
FIGURE 6: ISS SEVERITY SCALE ........................................................................................... 25
FIGURE 7: EVALUATION PRINCIPLES ................................................................................... 29
FIGURE 8: DESCRIPTION OF THE TELESERVICE SYSTEM .................................................. 35
FIGURE 9: DESCRIPTION OF THE TELESERVICE SYSTEM ..................................................... 36
FIGURE 10: GENERAL ARCHITECTURE AFTER CONSIDERATION OF SECURITY REQUIREMENTS 39
FIGURE 11: INDUCTIVE APPROACH .................................................................................. 41
FIGURE 12: DEDUCTIVE APPROACH .................................................................................. 42
FIGURE 13: COMBINATION OF APPROACHES ...................................................................... 43
FIGURE 14: MODELLING OF THE "USER/ADMINISTRATION" INTERFACE ......................... 44

Tables of Tables

TABLE 1: SIMPLIFIED BIBLIOGRAPHY INDEX ..................................................................... 6
TABLE 2: ACRONYMS AND ABBREVIATIONS ....................................................................... 7
TABLE 3: STEPS IN THE METHOD ........................................................................................... 20
TABLE 4: ISS SEVERITY SCALE ............................................................................................ 26
TABLE 5: SECURITY SENSITIVITIES BY CRITERION ............................................................... 37
TABLE 6: FEARED EVENT RANKINGS .................................................................................... 38
TABLE 7: PREDICTED INCIDENT RANKINGS ........................................................................ 44
TABLE 8: TABLE OF LINES OF DEFENCE ............................................................................. 45
Introduction

1.1 Study Overview
As in other areas, the greatest danger in the field of information systems security is often to rely either consciously or unconsciously on a false sense of security. A sensible approach would be to manage uncertainty, to maintain an attitude of rational concern and ensure proper vigilance. As part of this role, DCSSI's Advisory Office has conducted a study focusing on the definition and formalisation of the concept of in depth defence applied to the field of information systems security. The purpose of the study is to reach practical, operational findings relating to IS architecture and risk management issues. A large number of French industrial players and experts have been consulted in order to achieve these objectives.

1.2 Document Structure
This document is organised into three main parts, reflecting the approach to the study:
- the first part presents an exhaustive review of current literature relating to industrial and military practice in order to attempt to determine the main principles of in-depth defence;
- the second part sets out the concepts and definitions of in depth defence as applied to ISS;
- The third part defines a method based on the aforementioned principles that can be applied to information systems security;
- The appendix illustrates the method with the help of a real-life case study that was used to develop the assessment procedure.

The conclusion mentions the thought processes involved in the study, identifies its benefits and suggests avenues for further research.
1.3 Bibliography

The table below lists the main reference documents used for this study. Where a reference is cited in this document, the relevant number is inserted between square brackets (the same numbering scheme has been used throughout the study).

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author(s)</th>
<th>Date</th>
<th>Title</th>
<th>Editeur</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Silk Road, LLC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vienna, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1 : Simplified bibliography index
1.4 Acronyms and Abbreviations

The acronyms and abbreviations used in this document are listed in the table below.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>CDES</td>
<td>Commandement de la Doctrine et de l'Enseignement militaire Supérieur (Senior military doctrine and education centre)</td>
</tr>
<tr>
<td>DoD</td>
<td>US Department of Defense</td>
</tr>
<tr>
<td>IATF</td>
<td>Information Assurance Technical Framework</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services (Microsoft internet server)</td>
</tr>
<tr>
<td>INERIS</td>
<td>Institut National de l'Environnement Industriel et des Risques</td>
</tr>
<tr>
<td>INSAG</td>
<td>International Nuclear Safety Advisor Group</td>
</tr>
<tr>
<td>IPSN</td>
<td>Institut de Protection et de Sûreté Nucléaire</td>
</tr>
<tr>
<td>IS</td>
<td>Information System</td>
</tr>
<tr>
<td>SFEN</td>
<td>Société Française d'Energie Nucléaire</td>
</tr>
<tr>
<td>ISS</td>
<td>Information Systems Security</td>
</tr>
</tbody>
</table>

*Table 2: Acronyms and abbreviations*
2 Analysis of the Concept

2.1 Concepts Described in the Literature

2.1.1 Study of the military arena

Vauban developed the emerging concept of in depth defence into a fine art. The invention in the 15th century of metal cannonballs capable of destroying high walls and tall towers led to the construction of much more squat fortifications that took advantage of the depth of the terrain. The underlying concepts are as follows:

- The assets to be protected are \textbf{ringed} by several lines of defence;
- Each line of defence contributes to the \textbf{overall defence};
- Each line of defence plays a specific \textbf{role}, such as: blunting the attack, or hampering or delaying it (e.g. by giving ground to gain time);
- Each line of defence is \textbf{autonomous} (the system is designed to prevent the loss of the previous line from creating a "house of cards" effect): although losing one line of defence may weaken the next line, each line has its own means of defence against the various types of attack (each possible attack process prompts the corresponding defence process);
- Every available means of reinforcing the defence offered by the various lines is used:
  - best use of terrain (fortifications are terrain-based features);
  - bulkheading, to contain breakthroughs and ricochets;
  - intelligence, to prevent surprise attacks.

Today, the in depth defence concept is no longer in the limelight, as defensive manoeuvres tend to be seen merely as the necessary consequence of a position of inferiority, to be used essentially as a means of regaining the initiative. In modern military planning, two principles have taken on great importance:

- Intelligence, which can be used to confirm or disprove assumptions relating to an enemy's activities, detect its intentions, etc.
- Movement (i.e. the dynamic aspect of defence).

The basic principles of in depth defence are:

- \textbf{Intelligence} is the first line of defence, covering everything: from information about actual threats and the detection of activities typical of preparations for an assault, to any detection, not only of overt, identified attacks, but also of any "abnormal" - and therefore suspicious - behaviour;
- There must be multiple, \textbf{coordinated} lines of defence, \textbf{ranked} by defensive capability;
- The loss of a line of defence must \textbf{blunt the attack} (at least indirectly by providing as much information as possible on the attack's source(s) and nature, and on its possible and probable next steps), and \textbf{reinforce} subsequent lines of defence rather than causing them to fail;
- Each line of defence must include counter-measures (even if they only amount to detecting and tracing faults in the event of an attack of an unidentifiable type) for all possible forms of attack (i.e. each line must be \textbf{complete} in and of itself);
- The act of defence does not preclude offensive actions.
2.1.2 Study of the industrial arena

2.1.2.1 Nuclear safety

The concept of in depth defence applied to nuclear safety was born out of the accident on 29 March 1979 at the Three Mile Island plant, where the reactor suffered a partial meltdown as the result of a coolant system failure. It is defined as a system of defence comprising three successive, independent barriers that combine to ensure that the probability of an accident having repercussions off-site is extremely low. The basic idea is that each safety feature should be treated as vulnerable, and as such in need of protection by another feature\(^1\).

The French energy utility EDF also speaks of three lines of defence of different natures:

- Appropriate design (in particular the use of redundancy and diversification);
- Detection of latent faults and incidents;
- Effect mitigation.

The in depth defence approach is applied in conjunction with a risk management system comprising eight standardised risk levels, as illustrated below.

\[\text{Figure 1: INES scale}\]

---

\(^{1}\) The security of nuclear power plants, especially in France, is based on the philosophy of "in depth defence" which is organised around multiple levels of protection comprising successive barriers that combine to ensure that the probability of an accident having repercussions off-site is extremely low. The basic idea is that each safety feature should be treated as vulnerable, and as such in need of protection by another feature." Clefs CEA n° 45 Insert D The three barriers, illustration of the concept of "in depth defence" (Updated March 2002).

\(^{2}\) Source: http://nucleaire.queret.net
The three barriers (i.e. the fuel cylinder, the 20 cm thick reactor vessel and the 90 cm thick containment chamber walls around the reactor\(^3\) are shown in the following diagram.

\[\text{Figure 2 : The three barriers}^{4}\]

\(^{3}\) This chamber is itself lined in modern reactors.
\(^{4}\) Source: [http://perso.club-internet.fr/sorinj/la_surete.htm](http://perso.club-internet.fr/sorinj/la_surete.htm)
2.1.2.2 Transport corporation (RATP)

The in-depth defence principles implemented in the nuclear industry are also found in many industrial complexes subject to major risks. As in the nuclear industry, risks are most often endogenous, and the various barriers are designed to perform a containment role. In [4], J. Valancogne from the transport corporation, RATP, characterises these barriers:

- Barriers can be technological, procedural or human in nature. They can also be "composite", meaning that they have more than one of the above attributes;
- Barriers can be either static or dynamic (a containment chamber is a static barrier, whereas an automatic control device that opens a valve is an example of a dynamic barrier); dynamic barriers (which open and close) can be:
  - technological, human or composite,
  - close to obstruct the aggression as it occurs, or conversely, open to allow flows to pass if they are non-aggressive,
  - act on different time scales,
  - succeed or fail,
  - embody various operating principles (intrinsic, probabilistic, etc.);
- They can act directly on the aggressive element, on the flow or on the element to be protected.

A barrier's efficiency does not depend solely on its design; maintenance and the barrier's evolution over time are two more very important aspects. A fault tree can be produced for each barrier. The example of the disaster at the Union Carbide plant in Bhopal shows the successive failure of three barriers designed to prevent the accident, mainly as a result of procedural and maintenance vulnerabilities. J. Valancogne also emphasises the importance of feedback, and specifically, the value of analysing incidents (as in the nuclear industry). Furthermore, as the system is subject to evolve over time, the effectiveness of its defences must be periodically reassessed.

2.1.2.3 Chemical industry

A particularly interesting paper entitled "Analyse des risques et prévention des accidents majeurs" (DRA-007) (Risk analysis and prevention of major accidents) [43] has been published by INERIS (Institut national de l'Environnement Industriel et des Risques). This document is the final report (Sept. 2002) from the "Assurance" project, which set out to conduct a comparative analysis of risk analysis methods and safety strategies used in Europe, using a case study of a real-life chemical plant as its starting point. The overall approach included the following phases:

- Risk identification;
- Risk classification:
  - Severity classes based on effects (lethal, irreversible, etc.);
  - Frequency/probability of occurrence depending on the number of barriers;
  - Risk acceptability matrix (according to severity and frequency), with permitted, acceptable and critical zones;
Qualitative analysis. The methods used can be divided into three categories:
- Inductive analytical methods (most methods, including HAZSCAN, SWIFT, HAZOP and APR) are predicated on a top-down analysis of the accident sequence (i.e. working from the causes to the consequences);
- Deductive analytical methods (e.g. fault trees) are based on a bottom-up analysis of the accident sequence (i.e. working from the consequences to the causes);
- Methods based on the systematic identification of causes of emissions, which centre on expert judgement and feedback (e.g. national guidelines or audit tables).

Quantitative analysis. The methods used can be divided into two categories, as shown in the diagram below:
- probabilistic approach;
- deterministic approach.

![Diagram of Methodological Approaches](source:[DRA7])

Conducting a comparative analysis of the deterministic and probabilistic approaches to risk reveals that neither is ideal for managing the ISS risk. One alternative solution would be to base such a strategy on the concept of defensive barriers and in depth defence, which is the basic principle behind the safety strategies implemented at nuclear and industrial facilities in France. In INERIS's view, the defensive barrier-based approach allows risk management to be presented in a more transparent manner. This transparency makes awareness campaigns more likely to be perceived positively by associations and the general public.

2.1.3 Study of the ISS arena

Three types of document are used:
- Documents that simply call for common sense: defence should not be limited to the system's perimeter, or rely on a single type of resource;
- Documents that use the term, mostly published in the USA from 1998 onward, and in particular, documents dealing with the security of the US department of defence's information systems;
- A number of more methodological documents were detailed in the report produced during phase 2:
  - [13] aims to provide a simplified method for use by small organisations;
  - [31] more closely resembles a qualitative risk analysis;
  - [3] uses a counter-example to promote the case for in depth defence;
  - [7], published by the NSA, originated the concepts used by the US DoD.
2.1.4 Context analysis

It is necessary to begin by allowing for the differences in context between the three studied industries. The following points appear to be relevant:

- **The element of surprise:**
  - In the military arena, tacticians systematically seek to leverage the element of surprise in military manoeuvres.
  - In the nuclear industry, designers clearly attempt to minimise the element of surprise, even though it must not be overlooked;
  - In information systems security, surprise is part of the environment inasmuch as novel forms of attack will always exist (currently, the initiative is not with the defender);

- **Intelligence:** good intelligence reduces uncertainty regarding enemy actions by confirming or disproving assumptions, and avoids the adverse effects of being caught by surprise; intelligence activities should not be dissociated from planning activities;

- **Cooperation between the various lines of defence:**
  - In the military arena, planners and tacticians systematically look for synergies between different resources: including an additional means of defence should provide a greater benefit than just the sum of the non-independent lines of defence;
  - In the nuclear industry, considerable emphasis is given to the independence of the various lines of protection with regard to threats (causes of failure);
  - In information systems security, the addition of protective features appears to be closely linked with the presence of threats, which are tackled on an individual basis.

- **The (internal or external) origin of threats:**
  - The notion of "close protection" clearly illustrates this principle: an enemy may have penetrated the full depth of the defence system, meaning that each individual combatant has to provide their own close protection, irrespective of their broader role;
  - In industrial environments, external threats such as terrorist attacks are taken into account, as well as internal threats posed by the industrial process itself;
  - In information systems security, too, there is the "global" aspect of an attack that can come from either within or outside the system; the depth of the defence system must consequently be defined in several dimensions; This means that the depth of defence must take account of the organisation, the implementation and the technologies used and not simply provide perimeter defence between the system and the "outside".
The minimum requirements for providing in depth defence include:

- Multiple independent lines of defence, in the sense that each line is capable of defending itself against all forms of attack (i.e. the loss of the preceding line is planned for, and there is no presumption that the preceding line exists). A more accurate term would be autonomous or complete lines of defence, i.e. lines that are able to respond to any type of threat. A principle of military doctrine requires each line to also contribute to an overall defensive system that is stronger than the sum of its parts; (this principle is not given the same importance in industrial environments, where greater emphasis is placed on the independence of the various barriers).

- Cooperation between lines of defence, without which the concept becomes nothing more than a series of successive barriers whose strength is not dependent on the preceding barrier (allowing them to be attacked one after the other);

- The loss of a line must strengthen the remaining defences, not weaken them (this point is a corollary to the previous point, but is included here to emphasise the dynamic aspect of the defensive system).

The concept of in depth defence originated in military circles. The expression was subsequently adopted by the nuclear industry, which developed it into a method. The concept gradually became more widespread, being used in industry (e.g. by chemical producers) and transportation (RATP). In industry, in depth defence provides a means of adding a deterministic aspect to probabilistic risk analyses and modelling systems at component level. The concept has subsequently been applied to information systems security, primarily in the US, but has not been developed to any great extent, as it appears to combine various notions relating to the word "depth" in the sense of multiple redundant or complementary resources. However, there would appear to be two slightly different approaches, one stressing the global aspect, the other emphasising the system's components. References to risk analysis are more explicit in the latter of these two strategies.
2.2 Interview Results

The interview with military personnel highlighted the importance of:

- The intelligence factor, which had already been mentioned, but which must be further emphasised;
- A dynamic approach and forward planning;
- The notions of responsibilities at each level.

These three points should be included in any in depth defence-based approach to information systems security by taking the following principles into consideration:

- When setting up a barrier, it is important to specify:
  - the control point that determines whether the barrier is intact or has failed (intelligence function);
  - the information that must be collected in order to establish that an attacker intends to target the barrier;

- When developing the overall policy, provision should be made for barrier failures. This implies:
  - providing dynamic countermeasures;
  - planning the possible courses of action in each scenario;

- Information systems security should be the concern of all employees, not just specialists; managers should be appointed for every tier:
  - at individual level (immediate protection), via a charter, procedure manual, etc.;
  - for each unit in the organisation (close protection), via an appropriate security file including procedures and one or more elementary emergency plans;
  - at organisational level (strategic protection), with emergency plans with a broader scope, e.g. multi-service plans, backup sites, etc.

The concept of in depth defence should be looked upon in the industrial environment as a logical extension of effective risk control:

- Once a security objective has been defined (e.g. "prevent an accident or off-site release", etc.), a risk analysis is conducted using established methods; it can be seen that in depth defence combines the deterministic and probabilistic approaches; applied together, these two strategies make it possible to identify and implement barriers (using a deterministic approach at the design stage) then evaluate their probability of failure (by applying a probabilistic approach);

- It is then possible to rank the various potential incidents on an overall scale, which provides some major benefits in terms of training and awareness:
  - scale of common values,
  - depicts defence in layman's terms,
  - easily determines the severity of an incident, which depends on which barriers are breached;

- Lastly, whenever a barrier is breached, preventive and corrective measures are triggered, with planning pursued all the way to the final phase when the feared event occurs.
2.3 Conclusions from the First Phase

Within the scope of the specified in depth defence criteria, no complete solution relating to information systems security was identified. The principles applied in the military and industrial fields do offer some interesting ideas, however. The military arena is similar to information systems security in terms of the concepts of attack and defence, and the industrial environment exemplifies the disciplined approach and all-round, systematic and quantitative perspective that tends to be lacking in the IT field.

It is immediately apparent that:

- The expression "in depth defence", as currently used in relation to information systems security, does not reflect a revolutionary break with existing principles that already being applied;
- Enhancing current information systems security principles to incorporate the benefits of the in depth defence methods applied in the industrial and military sectors should enable the definition of a true in depth defence method geared more to defence than security.
3 In depth defence in ISS

3.1 Definition of the Concept

3.1.1 General notes relating to the concept

The use of multiple independent barriers is the most universal principle enshrined in the in depth defence concept, and is applied in the military and industrial fields as well as information systems security.

The other principles are developed to different extents according to individual circumstances. Furthermore, whereas the concept remains the same throughout the industrial world, it is important to recognise that this is not the case in the area of information systems security.

It emerges, however, that the concept of barriers i) relates only to the protecting component (restriction, bulkheading) and ignores other essential parameters, and ii) is over-dependent on the threat, making it difficult to implement in information systems security contexts involving non-specialist decision-makers and users, mainly because of the number and technical nature of the barriers.

In contrast, the concept of "lines of defence", although very arbitrary, appears to be a richer, more easily-conveyed concept.

In the case, for example, of a workstation protected against internet-based hacking by a FireWall and by antivirus software, the antivirus application acts as the second barrier to any attempt to plant malicious code by breaking into the system, but becomes the first barrier if the malicious code is carried in an email message, which the FireWall allows through. In the area of information systems security, the means of protection (in this case the firewall) act more as filters than as genuine barriers (cf. 3.1.2) such as found in the nuclear industry.

It is not possible to establish a direct relationship between barriers, lines of defence and severity levels, owing to the sheer number of threats and forms of defence. However, the concept of "lines of defence" can be employed to group barriers together for "communication" purposes, and to correlate them with severity levels\(^5\). In this context, a line of defence represents a transition between two severity levels, implying the need for a corresponding planned response.

The proposed strategy sets out to determine what barriers\(^6\) should be set up, according to the threats posed and the assets to be protected, before determining the severity levels of the security incidents that would result from any breaches in said barriers with a view to grouping them by severity level, thereby revealing the lines of defence. These facilitate communication

\(^5\) The proposed gravity levels are indicated earlier in the chapter.

\(^6\) The term "barrier" (see definition earlier in the chapter) is taken here as being synonymous with "security measure" (human, procedural, technological) in accordance with the generic definition of this term proposed by Mr Valancogne, allowing the term "line of defence" to retain a more general and "descriptive" meaning. This therefore differs from the meaning given to these two terms by the CEA.
initiatives aimed at decision-makers and users, but are no substitute for barrier studies by security specialists. This approach is illustrated in the diagram below.

![Diagram](image)

**Figure 4: Strategy for identifying lines of defence**

It is important to proceed by iteratively combining the resource-oriented deductive approach with the threat-oriented inductive approach. This iterative design process ceases when it becomes possible to validate the architecture and means of protection, and determine the residual risks (by qualifying the studied system).

Note that barriers are associated with threats (hence the need for an inductive approach) but that the severity levels of security incidents depend on the resources implemented (which requires a risk analysis and a deductive approach). The two approaches (i.e. inductive and deductive) complement each other, and should be reiterated until an acceptable level of protection is obtained. At that stage, the architecture and the means of protection deployed to counter the risks can be validated, and the system qualified in order to reveal the residual risks.

It should also be noted that a barrier (and therefore a line of defence) can cover more than one threat, and that any breach will result in an incident, the severity of which is determined by the number of lines of defence still unbreached and the value of the assets to be protected. Thus, there is a dual representation of the method:

- One intentionally simple, all-round representation for decision-makers and users (expressed in terms of lines of defence and the severity scale shown in the diagram);
  
  ![Simple Diagram]

  This representation is important for **awareness-raising** purposes.

- A second, more detailed representation, designed for specialists, using special models of critical processes for each main threat; with this representation it is almost always useful to break down the various levels, with different subdivisions for different planning variants (to allow for scenarios involving consecutive barriers and incidents of different severities as shown in the previous diagram).

  ![Detailed Diagram]

  This representation is important for the purpose of **qualifying** the method (a schematic representation of the various security measures associated with a particular threat in order to protect an asset is produced at the scenario-building stage, in order to: i) determine what barriers must be set up, based on an iterative process of inductive and deductive analysis repeated until the necessary protection level is achieved, and ii) to assess the severity of security events according to the criticality of the asset to be protected and the number of unbreached lines of defence.)
The specific modelling performed for critical assets and the main threats lets engineers establish a direct link, thereby detecting security vulnerabilities more easily and enabling them to be evaluated.

3.1.2 Definitions

The following definitions are based on the analysis of the in depth defence concept and related principles.

The severity of a security event measures either the event's actual impact, depending on the asset's criticality (in cases where an event has a direct consequence on an asset), or its potential impact on the threatened asset, depending on the number of unbreached lines of defence as well as the asset's criticality (in cases where the event affects an asset's means of defence rather than the asset itself).

The method includes a scale of severity levels, to allow comparison between security incidents. User managers are responsible for assessing the severity level of a given security incident, according to the incident's impact on the asset to be protected.

A barrier is a security feature capable of protecting part of the information system against one or more threats. Barriers can be human, procedural or technical in nature, and either static or dynamic, manual or automatic. There must be an associated means of monitoring its status.

A line of defence is a series of barriers, organised by scenario or scenario family, which when breached generates an incident, the severity of which depends on the number of unbreached barriers still remaining between the threat(s) and the protected asset(s), and on the value of said asset(s). In other words, a particular security incident will have a related severity level, reflecting the abstract line of defence breached. In order to constitute a true line of defence rather than just a series of means of protection, a line must have detection/watch and notification resources and mechanisms.

The in depth defence of an information system is an all-round dynamic defence with several coordinated lines of defence covering the system's full depth. The term "depth" must be understood in the widest sense, i.e. in the organisation of the IS, in its implementation and finally in the technologies used. It then consists of allowing action to be taken to neutralise attempted security breaches, at least cost, through risk management, an intelligence system, response planning and continuous feedback-driven enhancement. This in depth defence serves two purposes: i) enhance the protection afforded to the information system by adopting a qualitative approach capable of checking that the defence system is complete and effective, ii) provide a useful communication tool that helps decision-makers and users understand the severity of a security incident.

In information systems security, a barrier (in the form of a resource or system) is assigned to one or more threats and installed in a particular position (between the source of the attack and the asset to be protected). A barrier may protect multiple assets, although not necessarily in the same way. Consequently, the lines of defence should be analysed for each asset (or group of assets) and for each threat (and as such, for each category of security incident). The granularity of this analysis varies according to the degree of risk involved (determined by the asset's criticality and/or the threat's probability of occurrence). The analysis combines the threat-based inductive approach and a subsequent deductive approach based on the resources that must be protected.
3.1.3 General principles

The concept of in depth defence thus obeys the following main general principles. Each of these principles can exist in isolation but it is their combination that gives the depth of defence.

<table>
<thead>
<tr>
<th>Title</th>
<th>Nature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensiveness</td>
<td>Defence must be comprehensive, meaning that it must include all aspects of the information system:</td>
</tr>
<tr>
<td></td>
<td>a) organisational aspects;</td>
</tr>
<tr>
<td></td>
<td>b) technical aspects;</td>
</tr>
<tr>
<td></td>
<td>c) implementation aspects.</td>
</tr>
<tr>
<td>Coordination</td>
<td>Defence must be coordinated, meaning that the means implemented act:</td>
</tr>
<tr>
<td></td>
<td>a) as a result of a warning and dissemination capability;</td>
</tr>
<tr>
<td></td>
<td>b) following a correlation of incidents.</td>
</tr>
<tr>
<td>Dynamism</td>
<td>Defence must be dynamic, meaning that the IS has a security policy that identifies:</td>
</tr>
<tr>
<td></td>
<td>a) a response capability;</td>
</tr>
<tr>
<td></td>
<td>b) a plan of action;</td>
</tr>
<tr>
<td></td>
<td>c) a scale of severity.</td>
</tr>
<tr>
<td>Adequacy</td>
<td>Defence must be adequate, meaning that each (organisational or technical) means of protection must have:</td>
</tr>
<tr>
<td></td>
<td>a) its own means of protection;</td>
</tr>
<tr>
<td></td>
<td>b) a means of detection;</td>
</tr>
<tr>
<td></td>
<td>c) response procedures.</td>
</tr>
<tr>
<td>Completeness</td>
<td>Defence must be complete, meaning that:</td>
</tr>
<tr>
<td></td>
<td>a) the assets are protected according to their criticality;</td>
</tr>
<tr>
<td></td>
<td>b) each must be protected by at least three lines of defence;</td>
</tr>
<tr>
<td></td>
<td>c) feedback is formalised.</td>
</tr>
<tr>
<td>Demonstration</td>
<td>Defence must be demonstrated, meaning that:</td>
</tr>
<tr>
<td></td>
<td>a) defence is qualified;</td>
</tr>
<tr>
<td></td>
<td>b) there is a certification strategy;</td>
</tr>
<tr>
<td></td>
<td>c) certification follows the life cycle of the information system.</td>
</tr>
</tbody>
</table>

The "minimum number of barriers" aspect of the principle of completeness is derived from a pragmatic approach originating from the nuclear sector: it is considered that one of the three barriers is affected by the incident or the attack having triggered the incident, that one of the remaining two happens to be defective, with the result that the consequences are definitely limited by the third.
3.2 Implementation of the concept

In depth defence thus aims to control the information and the system that supports it by balancing and coordinating the dynamic and static lines of defence throughout the full depth of the information system, i.e. in the organisational, implementational and technological aspects. The purpose is not to provide a selection of in depth defence tools or details of good or best practice, but to illustrate by means of examples exactly what an in depth defence system can be in practice. For a coherent, structured approach depends on following the methodology proposed in the following chapter.

3.2.1 Depth of the organisation

Giving depth to an organisation in the sense of in depth defence could first of all consist in defining a chain of responsibility from end to end, i.e. from the user to the security manager. This continuity within the organisation is achieved through regular, tested awareness-raising and training actions.

This chain of responsibility must be known to all and be supported by procedures for reporting incidents and for issuing security notices or alerts. Like all lines of defence, those installed from an organisational point of view must be monitored and backup procedures provided.

In depth organisation also consists in providing feedback so that everyone can benefit from other people's experience. Such feedback also provides an opportunity to upkeep the security baseline throughout the life cycle of the IS which is not only dependent on the technologies used but also on the people and skills available. The feedback must differ according to whether it is system users or operators are concerned. It may be wise to allow for feedback to be provided anonymously, or at least outside any functional hierarchy.

The security baseline of the information system must be validated at the highest level and known to all. This means that the security baseline will only play its role if it affects the organisation throughout its entire depth. Security must be everyone's concern and not a specialist niche.

The organisation must continuously and dynamically seek to assess its level of security against security objectives resulting from a risk analysis. The organisation must have the ability to either monitor itself or call upon a third party to evaluate its level of security.

The information system operates within a physical environment with which it continually interacts. These actions must be monitored and emergency procedures put in place.

The notion of integrating security within projects also indicates a certain maturity. Finally, security certification and the ability of the organisation to re-examine it according to the environment, the life cycle of the systems and security incidents are key points of in depth defence.
3.2.2 Depth of implementation

Security implementation must be based on validated and proven policies. This also assumes that the users participate directly in incident reporting and are informed about security alerts.

Defence in depth of the information system requires a dynamic policy of tool and document baseline updates. Without such updates and calling into question of security procedures, the defence provided would risk to be somewhat illusory.

Any tools that are implemented must be administered, monitored and inspected. This is achieved in particular by analysing the trace data that serves to detect incidents. A line of defence must be monitored, whatever its type.

The maintenance policy must also have depth by diversifying suppliers, verifying and testing contracts while ensuring that they comply with the security objectives.

3.2.3 Depth in technologies

In depth defence therefore consists in countering threats with coordinated and separate lines of defence. At a technology level, for example, this may mean preventing a compromised network service gaining the highest level of access to the whole system. Within this context, giving administrator rights to all of the users of a system is contrary to in depth defence. For protection of information it can also mean that application level encryption is not in itself sufficient and that it may be necessary to also protect the IP layer.

A consequence of in depth defence is therefore that security is not based on one aspect but on a coherent system. This means that in theory there must not be any single item on which the entire system depends. Defence must not therefore depend on one technology or one product, regardless of quality. As a barrier, a security product must be monitored, protected and have a response plan in case of incident.

It is necessary to seek to reduce the system's exposure to the various threats. This means, for example, creating enclaves by means of firewalls and intrusion detection systems. Within this context of least exposure, the services offered must systematically be limited according to strict necessity.

Providing depth in technologies also means defending up to the user workstation by installing firewalls on and a regularly updated antivirus application of a different type to that installed on the e-mail gateway. These tools must be accompanied by user training to raise awareness that technology alone is not enough and that vigilance must be maintained whatever the tools deployed.
4 The In depth defence Method

This method allows a contracting authority to take account of the principles of in depth defence as defined above (see paragraph 3.1.3). In particular, it provides the possibility of qualifying a system and, in a way, of measuring its level of defence. In order to achieve this objective, the method assumes that a risk management analysis has been performed beforehand. Finally, this method forms part of the process of integrating the ISS within projects.

The method for applying the concept of in depth defence to information systems security includes the following steps:

1. Determine assets and security objectives. The results from this step provide the basis for building the in depth defence. The security objectives can be used to classify impacts according to the severity scale, in turn enabling security incidents to be expressed in relation to the scale; this makes it possible to use an incident table in conjunction with a diagrammatic representation of the information system and its lines of defence as a communication tool.

2. Specify the system's organisation and overall architecture (i.e. the depth of the defence system). The control points and evaluation points are defined during this step. It should be conducted as near to the start of a project as possible; this step reveals the necessary barriers, security incident severity levels (based on the number of residual barriers) and lines of defence.

3. Develop the defence policy, in two parts: the first part organises intelligence, and the second organises the corresponding defensive response (inter-reaction and planning). This step defines the operational defence policy and identifies the control points. The defence policy should make it possible to monitor the system, centralise security event data for inclusion in management charts and enable decisions to be made regarding the choice of response. This is a more dynamic, organisational step than the previous step.
4. The global consistency of the system together with the additional measures taken in previous steps should provide a high level of protection. This level must then be **provable**. The objective of this step is thus to qualify the information system for the in depth defence criteria.

5. Continuously and periodically evaluate the defence on the basis of attack methods and feedback. This step corresponds to the inspection and audit part. Update the defence on the basis of the evaluation results and to take any system evolutions into account. This step amounts to security upkeep maintenance. It should lead to the granting of certification which must remain consistent with the changes to the system throughout its life cycle.
4.1.1 Step one: determine assets and security objectives

The first step consists in the conventional actions of: identifying the assets to be defended and determining their criticality (in the risk analysis that will subsequently be used to quantify the defence value; for the purposes of graduating alert levels, a component's reliability must be weighted to reflect the consequence of its loss).

By the end of this first step, the various actors in the model have been identified and the security needs specified.

This step lends itself particularly well to the use of methods like EBIOS. "The EBIOS method contributes to the preparation of the contracting authority's tasks. It is used to determine the scope of study while maintaining a global view of the system in its context, to express needs (linked to the assets to be protected), to identify threats and to define a project plan and responsibilities."\(^7\)

The diagram below shows the proposed scale of severity for classifying security events according to their impact on the information system. This scale is based on the INES scale. However, the INES scale differentiates between incidents and accidents according to whether or not the event has an off-site impact. This distinction is irrelevant in the field of information systems security. The proposed scale is therefore based solely on the event's impact.

![ISS severity scale](image)

**Figure 6: ISS severity scale**

This severity can be measured in many different ways: in certain cases it will involve measuring an economic loss, in other cases it will be a court appearance. This is why it must be understood that the severity of an incident must be determined on the basis of a risk management analysis and not simple situation assessments.

---

\(^7\) Expression of needs and identification of security objectives – Memo – 4 February 2004 version
This step involves specifying the severity level of the main feared events (for example using the risk factors studied in the risk analysis) for the various assets that must be protected. It is important for the analysis performed at this stage to be the fruit of combination and mutual validation of a resource-based deductive approach and a threat-based inductive approach, and that human factors are also taken into account. The scenarios developed during this step will be modelled in the next step.

### 4.1.2 Step two: Overall system architecture

The purpose of this step is to determine the depth of the defensive system and to make choices regarding organisations, technologies and security procedures. The method recommends making these choices and identifying the points most vulnerable to the various threats by firstly adopting an inductive approach (the most natural and commonly used), starting from the threat and providing the lines of defence up to the asset to be protected. The ISS expert then develops a deductive approach working from the asset to be protected towards the threat in order to provide any more lines of defence that may be required and identify the most exposed points of the system.

The following points are identified in this section:

- Divide the system into zones according to the risks, actors, the organisation's key functions (information system "town planning"). this breakdown is based on the principles of independent entities and bulkheading;
- Identify the required technical, procedural and human barriers;
- Classify zones according to their sensitivity, and establish the rules for moving between zones (the issue of classifying the information and measures to be taken in order to interconnect domains with different security levels should be addressed during this step);
- Divide zones into trusted domains, and introduce a general system of full-depth organisational bulkheading;
- Specify what elements are private and shared in each domain and between domains.

It appears essential in this step to:

- Establish a table of the measures taken in order to clearly show the means of defence throughout the organisation's depth;
- Model critical systems in order to evaluate them;
- Rate incidents (barrier breaches) on the overall severity scale, based on the aforementioned impact classification; this data can then be used in operational policy-making to graduate actions and specify lines of defence. (Barriers are transposed into lines of defence during this step).
This step should normally be conducted upstream of any project, i.e. a security study should be included in the project management. If the system already exists, the following method is appropriate:

- Analyse the information system's technical and functional topology;
- Identify the existing barriers;
- Model the most important processes (by modelling the critical data and main threats in order to highlight the barriers);
- Evaluate the architecture already in place, to identify any changes that may be required in order for it to conform to the method's criteria (e.g. introducing additional barriers).

4.1.3 Step three: Develop the defence policy

This step consists of two sub-steps:

- Determination of an all-round, coordinated defence:
  - detect (determine control points and attack detection points);
  - centralise information;
  - correlate events;
  - alert;

- Planning:
  - determine the scope for reconfiguring the system to provide normal operation (fault-tolerant system delivering identical performance) or degraded-mode operation (e.g. local operation only, inferior performance, etc.);
  - response plans (plan possible actions for each feared event, e.g. a service continuity plan, but also network reconfiguration, use of backup resources, etc.)

The overall defence can be defined in terms of three aspects - organisational, implementation and technological – which embody the lines of defence deployed in the zones specified during the previous step. Ideally, each line of defence should have three security functions: protection, detection and response. The defence policy should determine the severity of each possible severity incident, in order to leverage the method's "teaching" value in promoting awareness among employees. Incident severity levels are determined by a process of deduction based on the number of remaining unbreached lines of defence.

The severity of an incident depends more on the means of defence still intact than on those that have been compromised. For example, an internal attack may bypass several barriers that would have to be penetrated by an external attack. According to the principles of in depth defence previously defined:

- There must be a minimum of three lines of defence.

---

8 For this section the reader can usefully refer to the best practices published by the DCSSI:
- **BEST PRACTICES FOR ISS RISK MANAGEMENT** – Using the results of the EBIOS® method to study an existing system – 2 February 2004 version;
- **BEST PRACTICES FOR ISS RISK MANAGEMENT** – Using the results of the EBIOS® method to study a future system – 13 January 2004 version;
- 9 For this section the reader can usefully refer to the best practices published by the DCSSI: **BEST PRACTICES FOR ISS RISK MANAGEMENT** – Using the results of the EBIOS® method to produce an ISSP – 21 March 2003 version.
The number of lines of defence must be appropriate for the risk (i.e. probability of occurrence and criticality of the protected asset).

The defence must be both global (with all resources helping to achieve the same security objective) and coordinated. This need for coordination mainly applies to intelligence and response resources, which respectively make it possible to specify the actual threat by analysing multiple data relating to an attack in progress, and to reconfigure the means of defence upon detecting an alternative means of defence, including filtering capabilities. Note that this coordination concerns barriers rather than lines of defence.

Defence is rendered dynamic by planning responses to anticipated security breaches. Incidents and accidents must be classified according to the severity scale, and must in all cases trigger a reaction, whether technical (automatic response), procedural (application of the relevant procedure or plan) or human (decision, initiative, etc.). Response plans must be graduated in the same way as security breaches, so that more draconian measures are taken at higher severity levels. In in depth defence planning, it is important to ensure that the defence system can respond to multiple incidents simultaneously.

The non-technical measures to be taken include planning for legal action against third parties, and sanctions against employees guilty of infringing company regulations (with the relevant supporting evidence being provided by technical personnel).

4.1.4 Step four: qualification of in depth defence

This step involves the qualification (validation of organisation and architecture) of the system, based on two approaches: the first is a qualitative process while the second is a deductive approach that studies the relevant scenarios.

4.1.4.1 The qualitative approach

This formal approach aims to ensure compliance with the principles of defence-in-depth previously defined (paragraph 3.1.3). It also ensures compliance with the method as formalised within the organisation.

This part thus resembles a quality strategy. It is very similar to chapter 7 ("rationale") of ISO 15408 (common criteria) which demonstrates the completeness of the security objectives for the threats identified.

4.1.4.2 The proof-based approach

The qualification method must be consistent with the all-round defence-in-depth method, as it was built. In particular, it should incorporate the results obtained in the course of the various steps.

This method is illustrated in the following diagram, which is explained below.
The first step, which consists in identifying the security objectives, enables potential impacts to be rated on the severity scale according to the stakes involved, and makes it possible to identify the measurement elements required in order to classify risks.

Step two (system architecture) yields a security incident classification based on which components failed.

Step three, which consists in preparing the defence policy, identifies the control points that will be used to continuously assess the defence system during this stage of the qualification.

Thus, the method revolves around:

- An information systems security risk analysis method, coupled with a means of rating the risks affecting main components and security functions on the aforementioned severity scale, which makes it possible to classify security incidents;
- Modelling the application of in depth defence to the main risks and analysing the most important or probable scenarios (in particular, "envelope" scenarios). These scenarios are iterative; they make it possible to identify barriers and evaluate the defence by applying the "failed component" method until the defence's robustness has been satisfactorily demonstrated.
- Rating security incidents on the aforementioned severity scale, according to the risks defined. The control points that check that the system is operating correctly and detect any attacks are identified and then used for continuous and periodic evaluation;
- The evaluations conducted both using traditional audit methods and by evaluating the defences with the help of security incidents and scenarios (to identify any potential consequences);
- The various studies capable of proving the security level attained and promoting awareness of the subject, in order to deploy a in depth defence solution and promote awareness of security incidents among employees (this promotional aspect being facilitated by having a security trend chart that shows incidents on the severity scale).

The defence-in-depth qualification method uses two proof-based analytical methods:
Analysis based on "envelope" scenarios: this approach consists in producing a scenario covering the greatest risk (destruction of the main site) and demonstrating that the other, less extreme scenarios (e.g. inability to enter the main site) are included in the "envelope" case, and that the chosen solution therefore covers them. This approach ensures that the number of barriers is consistent with the severity of the feared event;

"Failed component" analysis. This is performed by postulating a security incident, together with the hypothetical failure of another component selected at random on the path between the incident and the feared event, in order to analyse and check that the residual protection is adequate.

4.1.4.3 Conclusion

Therefore, the method supplements the conventional qualitative all-round analysis with a deterministic quantitative analysis covering the specific cases of high-risk scenarios, using the concepts of envelope scenarios and failed components. This method is well-suited to the "deductive" security principle, which is the norm in the area of nuclear safety, and which should be promoted.

The specific qualification of the defence-in-depth concept should therefore verify that the number of lines of defence is consistent with the severity of the feared events identified at the end of the first step, and that any residual risks are acceptable.

The first three steps are iterative rather than sequential. They are re-iterated until the requisite level of security is obtained, as dictated by the criticality of the assets to be protected, the potential threats and the residual risks. This step reveals the residual risks that must be known and accepted.

4.1.5 Step five: Continuous and periodic evaluation

Furthermore, there must be both periodic evaluations (at the time of introduction and at periodic reviews) and ongoing assessment (based on feedback and technology watch data).

The purpose of this step is to systematically assess the defensive system, using:

- Static component studies;
- Dynamic evaluation following an incident (feedback);
- Trend charts;
- Periodic audits;
- Retroaction (see below).

This step is closely related to step five, inasmuch as it contributes to the same goal of updating and reinforcing the defence, using two essential criteria drawn from the example of the RATP transport corporation for cases that are not quantifiable from a cost-benefit perspective:

- Prevent regression;
- Improve if cost-effective.
The results from this step should make it possible to present decision-makers with the measures taken in order to satisfy the security sensitivities specified in step 1 and prove that the stated objectives have been achieved.

An awareness-raising campaign should be undertaken during this step, to group scenarios together and highlight the main lines of defence and the planned response measures.

This step forms part of the life cycle of the system and, as such, must take account of operational upkeep maintenance linked to changes in organisations, technologies and procedures.

This step must lead to the award of security certification, allowing the information system to be declared fit to process information of a given sensitivity level. This certification is intimately linked to the life cycle of the system and is never a permanent decision.
5 Conclusions

The study of in depth defence applied to information systems security reveals that:

- the concept is frequently cited as a common sense concept of redundancy of the technologies used or for drawing together a number of widely-adopted principles, but is not currently being seriously debated within the context of ISS.
- The concept implemented in the industrial world is richer than the risk analysis methods usually used, but remains a pragmatic and therefore easily transposable approach;
- The dynamic nature and easy communicability of the concept make it a useful enhancement for traditional methods with which it is compatible;
- The concept is applied for qualifying actual systems, in particular in the nuclear sector.

Compared with the methods customarily used in information systems security, or described in the literature as being based on the in depth defence method, the proposed method appears to provide a number of improvements. These enhancements include:

- The importance of quantitative analysis in evaluating the system in the future;
- Qualification based on specific models that give an initial evaluation; the use of envelope scenarios appears much more appropriate and feasible than probabilistic analyses;
- The depth of the organisation based on a demonstration of the system's security using scenarios and lines of defence;
- Evaluation according to a severity scale (similar to the INES scale) which is invaluable for awareness-raising purposes;
- The all-round aspect of the defence system;
- The importance of intelligence and monitoring (control points) to preserve maximum freedom of action;
- The dynamic aspect of the defence system, including the watch, alert, response and planning process;
- Defence upgradability by organising feedback (seeking potential consequences, not just causes). Feedback offers a means of validating and updating scenarios, etc.
- demonstration of defence for qualifying an information system.

It should be borne in mind that the term "defence" (rather than security) conjures powerful images and conveys the notions of dynamics, initiative, freedom of action, degraded-mode operation, etc. Its scope extends beyond the simple of introduction passive protective measures.

Applying this concept of in depth defence to information systems also provides an original approach to the problem of system qualification. The transport and nuclear sectors have used this concept to qualify their installation, the ISS should be able to build on this. The principles applying to the ISS identified in this document and the proposed method of implementation could usefully contribute to defining the qualification of an information system.
The concept of in depth defence can be applied to all levels of an information system, both at the macroscopic level as in this document and in more microscopic aspects such as product evaluation or the implementation of an algorithm.

A number of avenues for further study appear promising:

- Developing a software implementation of the method in order to model scenarios and identify lines of defence according to the consequences of the postulated security incidents;
- Formalising the method and cataloguing components, monitoring resources, means of detecting attacks, etc.
- Forming component sets with standard architectures and proven defensive capabilities as a means of capitalising on previous research (e.g. nuclear plants using the same technology); such component sets should be modular, to allow them to be reused;
- Conducting more theoretical research into determining the probability of a component resisting attack, coupled with a concept of security certification or quantitative evaluation.
6 Appendix Application of the Proposed Method

Only the most important specific aspects of the method are discussed in this document.

6.1 Overview of the Case Study

The case study is of a dedicated teleservice system for requesting identity documents via Internet. This teleservice system includes a feature allowing users to check the progress of their request any time.

Users are identified before they are connected (checking of identity, determination of conditions of the request, etc.). Once they are completed, the documents supplied by the teleservice are stored as close as possible to the user's place of residence (town hall or similar) to limit travel distances.

The teleservice system is organised into a number of different services each performing a different function:

- centralising users' requests received via Internet;
- issuing orders to the various departments of the administration to process the request;
- sending the information to an archiving service.

The security study, performed in accordance with the method proposed in this document, therefore only concerns the following information systems:

- **The user interface**, which receives incoming e-mail/Internet orders (this communication system combines an Internet browser and an e-mail system);
- **The interface with other administrations** (wide-area intranet communication system).
- **The interface with the authority** (two interconnected intranets).
From a security perspective, the teleservice system comprises elements with the following characteristics:

- **The actual system** (hardware, software and intranet network);
  - the servers and workstations forming a dedicated network;
  - this system is situated in each administration and under their responsibility;
  - the users are members of the administration personnel;
  - technical support is performed by identified external personnel;

- **The user interface**, by e-mail/Internet (this communication system combines an Internet browser and an e-mail system);
  - the e-mails with attachments arrive at a dedicated workstation connected to the Internet; the attachments are automatically extracted by a tool that checks the validity of the order (agreement between the e-mail address and the user identification number in the order);
  - uses a relatively insecure communication system (Internet);

- **The interface with other administrations** (wide-area intranet communication system):
  - connexion between two networks by VPN Internet;
  - uses a medium secure communication system (VPN Internet);

- **Interface with the depositary** (two interconnected intranets).
  - connection between the two networks (teleservice and archives) via a gateway;
  - members of the administration personnel.
6.2 Implementation of the Method

This case study only deals with the specific security needs of the teleservice system as the "generic" requirements (physical protection, protection of people, etc.) are deemed to be covered elsewhere. Similarly, the system characteristics (performance, etc.) should be examined within the context of the overall project. As described in the implementation of the method, a risk analysis is a pre-requisite for its application, as it would be illusory to seek an in depth defence of assets that have not been identified to protect against threats defined only on the basis of a situation assessment.

6.2.1 Step one: Identify the security objectives

This case study only deals with the specific security needs of the teleservice system as the "generic" requirements (physical protection, protection of people, etc.) are deemed to be covered elsewhere. Similarly, the system characteristics (performance, etc.) should be examined within the context of the overall project.

Step one defines the security sensitivities of the overall system and its various components for each criterion.

The complete teleservice system thus has a high availability requirement that must be achieved through redundancy of the information technology equipment and the systematic presence of backup systems. During its period of operation, it is very probable that one or more components will suffer a hardware, software or other failure. The essential point is the availability of the system itself. This availability requirement is linked to the impact of a
failure on the operation of the system. The intrinsic severity of an incident that might make the system unavailable for a long period is therefore considered "Unacceptable".

The implementation of special information and communication handling measures must satisfy a specific integrity and confidentiality requirement. The risk analysis was able to identify a certain number of risks, due to the fact that the Internet is used. The intrinsic severity of an incident is thus "High" for integrity and "Very high" for confidentiality, the severity of this factor being increased by the presence of external personnel who are liable to increase the risks of indiscretions.

It should be noted that the entire teleservie system requires a high level of security in relation to confidentiality, as the transport part is closely linked to the information handled. Care must be exercised in the case of workstation replacement by the maintainer who may be external to the circuit. Encryption of stored files is a method to consider if necessary.

The means implemented to obtain a satisfactory level of security with the users may depend on their equipment and systems, as the measures taken by each user may differ. We would note however, that in theory they will normally be using a general purpose workstation with Internet access for home use. In this case, preference should be given to standard market solutions.

This point does nevertheless require further study to determine a typology of users and the equipment they intend to use:

- dedicated or general purpose workstation: in theory dedicated;
- connected to a computerised system or not: in theory no;
- Etc.

The requirements are summarised in the following table:

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Availability</th>
<th>Integrity</th>
<th>Confidentiality</th>
<th>Proof and control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual teleservice system</td>
<td>Downtime &lt; 1h</td>
<td>Data not altered</td>
<td>Personal, thus confidential information</td>
<td>Information validity control</td>
</tr>
<tr>
<td>Reception and processing of requests</td>
<td>Downtime &lt; 2h</td>
<td>Data not altered</td>
<td>Confidentiality protected by encryption (data transfers via Internet)</td>
<td>Authentication of sender and proof of receipt</td>
</tr>
<tr>
<td>Communication with other administrations</td>
<td>Downtime &lt; 1h</td>
<td>Data not altered</td>
<td>Confidentiality protected by encryption (data transfers via Internet)</td>
<td>Authentication of sender and proof of receipt</td>
</tr>
<tr>
<td>Communication with depositaries</td>
<td>Downtime &lt; 4h</td>
<td>Data not altered</td>
<td>Confidential information</td>
<td>Historisation and tracing</td>
</tr>
</tbody>
</table>

Table 5: Security sensitivities by criterion
As the method is supposed to provide the means of evaluation, it appears important at this stage of the study to rank the various security objectives. This hierarchical organisation means that incidents can subsequently be rated on the severity scale used as part of the method. The potential consequences of security incidents must be taken into account when ranking security objectives.

Analysing the above table reveals that the assets to be protected are implicitly ranked, in decreasing order of importance, as follows: the actual teleservice system, the request reception system, the system of communication with the administrations and lastly the system of communication with the depositaries.

The security objectives can also be ranked: availability is primordial, and data integrity is considered to be less important than confidentiality. The table below gives an example ranking of potential incidents, as might result from using the method's severity scale.

<table>
<thead>
<tr>
<th>Severity of the feared event</th>
<th>Severe breach of the stated sensitivities in relation to the criterion</th>
<th>Availability</th>
<th>Integrity</th>
<th>Confidentiality</th>
<th>Proof and control</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 – Unacceptable</td>
<td>Teleservice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 – Very Serious</td>
<td>Reception of requests</td>
<td></td>
<td></td>
<td>Teleservice</td>
<td></td>
</tr>
<tr>
<td>3 – Serious</td>
<td>Communication with administrations</td>
<td>Teleservice</td>
<td></td>
<td>Reception of requests</td>
<td>Reception of requests</td>
</tr>
<tr>
<td>2 - Moderate</td>
<td>Communication with depositaries</td>
<td>Reception of requests</td>
<td>Communication with administrations</td>
<td>Teleservice</td>
<td></td>
</tr>
<tr>
<td>1 - Low</td>
<td>Communication with administrations and depositaries</td>
<td>Communication with administrations and depositaries</td>
<td>Communication with depositaries</td>
<td>Communication with administrations and depositaries</td>
<td></td>
</tr>
</tbody>
</table>

Table 6: Feared event rankings

In the example chosen for the purposes of this document, the chain modelling process only concerns the risks relating to the presence of communications with administrations using the Internet channel, and assumes that there is a cryptography mechanism capable of authenticating the other party and guaranteeing data integrity and confidentiality, as well as a request checking application system.
6.2.2 Step two: Overall system architecture

6.2.2.1 Presentation of the overall solution

The diagram below shows the general architecture of the system that results from the consideration of security requirements.

![Diagram of general architecture](image)

The system is designed around the following principles:

- two servers with RAID discs able to switch from one server to the other, a DAT supplies the backup site and a CD writer serves for archiving;
- the confidentiality of exchanges is protected with respect to the outside but not with respect to the depositary. All exchanges are performed from dedicated workstations and backup capabilities are available. Workstations performing exchanges are provided with personal Firewalls;
- generalised antivirus protection is provided (servers and workstations) due to the presence of Internet and floppy disc drives;
- organisational (e.g. controls) and software (information management, archiving, tracing, etc.) measures are implemented.
6.2.2.2 Inductive and deductive approach

The various barriers must now be defined according to inductive and deductive approaches. For these approaches, we find the formalism of the EBIOS method and the common criteria (ISO 15408) in the description of the threat which is characterised by a threat agent using an attack method to compromise an asset. Modelling will be limited here to a threat identified as a main threat by the risk analysis. The critical asset in this case study is the information located on the teleservice server. The threat is thus defined as follows:

- the **source of danger** is a malicious individual seeking to discredit the teleservice system and harm the image of the administration;
- the **attack method** is software entrapment exploiting vulnerabilities associated with the use of the e-mail system;
- The **feared event** is an information systems breach:
  - affecting data integrity: acceptance of a counterfeit request;
  - affecting IS availability through server unavailability;
  - affecting data confidentiality by the release of information.

In the example chosen for the purposes of this document, the modelling of the approaches only concerns the risks relating to the use of the Internet between the users and the teleservice system. In this context, the main risks considered are as follows:

- Major risks resulting in prolonged unavailability of the system, these risks are covered by the presence of a backup site allowing the system to be restarted with all functionalities within 24 hours, even if some may be operating in degraded mode;
- Unavailability of the teleservice system due to equipment failure or human error. This risk is covered by the redundancy of the equipment and manual control procedures;
- Loss of integrity or confidentiality of data during exchanges between the various systems: this risk is partially covered by the use of a method of encryption that authenticates the correspondent, guarantees the integrity of data and protects their confidentiality;
- invalid information entering the teleservice system via the communication channel used to collect user requests.

**Inductive approach**

The first scenario focuses on the reception of a request message by the teleservice system that could be mistaken for a genuine message, and therefore compromise the information systems integrity (see figure 11). Such a message would pass through the firewall that controls access to the workstation, because the firewall allows incoming messages through. The barriers then implemented are:

- **barrier No. 11**: the application that extracts the messages from the workstation messages checks that the request is valid and correctly made;
- **barrier No. 12**: the application verifies the signature to authenticate the sender, and verify the integrity of the request;
- **barrier No. 13**: the application checks the legitimacy of the request (rights, initial request, renewal, etc.)
- **barrier No. 14**: the application records the request together with errors or refusals and starts processing as required.
The second scenario studies the case of an unauthorised access that introduces malicious code. This scenario involves a destructive virus risks compromising information system availability.

- **barrier No. 21**: the workstation is provided with a personal firewall that is configured to only accept message type input and output flows. It should be noted that this barrier is ineffective against malicious code sent by e-mail;
- **barrier No. 22**: the workstation is equipped with an antivirus application;
- **barrier No. 23**: the security policy is the only barrier on the workstation that can limit a virus attack on the workstation (e.g. principle of least privilege, or updating policy);
- **barrier No. 24**: the server is equipped with an antivirus application;

### Figure 11: Inductive approach

![Diagram showing the inductive approach with barriers and events]

**Deductive approach**

This approach works back from the asset to be protected, focussing on confidential information, such as the users' personal data that is used within the teleservice context.

- **barrier No. 31**: checking access rights should prevent unauthorised access to the data server;
- **barrier No. 32**: the workstation is provided with a personal firewall that is configured to only accept message type input and output flows;
- **barrier No. 33**: the workstation is equipped with antivirus detection software that also scans messages in attachments.
- **barrier No. 34**: the personal firewall is configured to only allow authorised output flows.

![Diagram](image)

**Figure 12: deductive approach**

By combining the two approaches it can be seen that certain barriers are particularly exposed insofar as they are found in several scenarios and according to both approaches. This observation contradicts the principle of independence: destroying the barrier would simultaneously remove the first and the last lines of defence and must thus lead to a strengthening of these key points.
**Figure 13: Combination of approaches**

### Conclusion

It can thus be seen that protection against destructive viruses contained in e-mails is very weak: the effective barriers are the workstation and server antivirus tools as well as the security policy for the two items of equipment. It is therefore particularly important to block the virus on the workstation and prevent it from spreading to the server.

Consequently, the study reveals the need to "harden" the workstation by:

- applying a strict policy of checking privileges;
- adding a second anti-virus having a different type of construction to protect the first;
- forcing the signature of outgoing messages;
- raising the awareness of personnel.

Hence the solution shown in figure 14 is adopted for the interface with the user or, more generally, with the Internet.
6.2.2.3 Security incident ranking

Based on the analysis of these three risk scenarios, and in particular their impact on the teleservice system, and combining it with the ranking of feared events (table 6), allows these scenarios to be situated on the severity scale (see table 7).

<table>
<thead>
<tr>
<th>Severity</th>
<th>Malicious code (Availability)</th>
<th>Counterfeit message (Integrity)</th>
<th>Trojan horse (Confidentiality)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 – Unacceptable</td>
<td>Server unavailable</td>
<td></td>
<td>Release of data</td>
</tr>
<tr>
<td>4 – Very Serious</td>
<td>Internet computer unavailable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 – Serious</td>
<td>Malicious code on an Internet computer</td>
<td>Counterfeit request</td>
<td>Server access attempt detected</td>
</tr>
<tr>
<td>2 - Moderate</td>
<td>Malicious code detected by the antivirus application on the Internet computer</td>
<td>Detection of counterfeit request by signature</td>
<td>Trojan horse detected by the antivirus application on the Internet computer</td>
</tr>
<tr>
<td>1 - Low</td>
<td>Intrusion attempt repelled by the firewall</td>
<td>Counterfeit attachment or unknown sender detected</td>
<td>Intrusion attempt repelled by the firewall</td>
</tr>
</tbody>
</table>

Table 7: Predicted incident rankings

The different lines of defence that can now be identified for the critical asset (i.e. the server hosting the teleservice system) with respect to the identified threat are thus as follows:
the firewall of the workstation;
- the workstation itself (electronic signature, antivirus protection and defence policy);
- the protection of the server itself (management of attributes, antivirus protection and defence policy).

<table>
<thead>
<tr>
<th>Line</th>
<th>Malicious code (Availability)</th>
<th>Counterfeit message (Integrity)</th>
<th>Trojan horse (Confidentiality)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Personal firewall</td>
<td>Check message</td>
<td>Personal firewall</td>
</tr>
<tr>
<td>2</td>
<td>Workstation antivirus</td>
<td>Check electronic signature</td>
<td>Workstation antivirus</td>
</tr>
<tr>
<td>3</td>
<td>Workstation security policy</td>
<td></td>
<td>Electronic signature</td>
</tr>
<tr>
<td>4</td>
<td>Server antivirus</td>
<td></td>
<td>Check server access rights</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Table of lines of defence

6.2.3 Step three: develop the defence policy

The purpose of this step is to develop the global defence policy. The previous study served to define the general architecture of the system and must be completed by defining the global security policy, the procedures to be applied, as well as planning responses. The main theme of this step is therefore the problem of security implementation.

There is little interest in determining the security policy in its entirety for the example given in this document. Only the special features associated with in depth defence are thus covered here:
- the coordination of the lines of defence, in particular regarding the detection of security incidents;
- planning responses to various incidents.

6.2.3.1 Determination of a global, coordinated defence policy:

Once the various barriers have been established, the control points (barrier working/not working) and attack detection points (if required) must be determined. This analysis will also enable the "correct" indicators to be selected in step 5 of the method.

The human factor must not be underestimated, as rapid detection of incidents often depends on the users, as it is not always possible to automatically and speedily analyse all of the information gathered by the detection systems.
The security policy must take into account:

- configuration of software to allow users to be advised of flaws (if needed, to authorise a flow for just the time necessary e.g. to update the antivirus);
- specific training for users to make them aware of the risks associated with the Internet connection and in particular the viruses contained in e-mail attachments that represent the major risk of this connection as the flow of messages must be allowed;
- full system operational checks (traces, event log, disc space, etc.).
- bulkheading of the various systems, each provided with its own means of protection. The implementation of special IDS type detection systems;
- a security incident reporting system allowing a response (see next section on planning) or at least warning to be issued to the users e.g. in the event that a new virus is detected.

6.2.3.2 Planning

There must be a planned response to anticipated security incidents. In the example studied in this document, the major risk highlighted is the unavailability of the actual teleservice system which may be due to two main causes:

- a hardware or software failure (e.g. operating error) that might affect the server itself or the local network and, to a lesser extent, a chain of communication;
- a security breach of the system by malicious action from without (the case of malicious action from within is not covered here and the case of error has been covered previously).

In the event of a server shutdown due to a hardware failure, the plan defines the various possible repairs:

- booting from the second server using the RAID disks of the first without loss of data in approximately 30 minutes;
- booting from the second server from the disk-to-disk backup with recovery of data from communications and re-entry of other information in half a day;
- booting from the remote backup site using the cassette backup with recovery of data from e-mails (systematic re-routing of mailbox to a back-up mailbox) and re-entry of other information in a day.

Network backup is made possible by redundancy of equipment (two servers and backup network facility).

6.2.4 Step four: Qualification

Qualification involves a qualitative approach (compliance with the principles of in depth defence) and a proof-based approach (response to envelope scenarios and component failure).
6.2.4.1 qualitative approach

Any demonstration of this aspect within the context of the case study would of course be entirely artificial. The principles governing the in depth defence of an information system are therefore simply restated, without performing the demonstration.

<table>
<thead>
<tr>
<th>Title</th>
<th>Nature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensiveness</td>
<td><strong>Defence must be comprehensive, meaning that it must include all aspects of the information system:</strong></td>
</tr>
<tr>
<td></td>
<td>d) organisational aspects;</td>
</tr>
<tr>
<td></td>
<td>e) technical aspects;</td>
</tr>
<tr>
<td></td>
<td>f) implementation aspects.</td>
</tr>
<tr>
<td>Coordination</td>
<td><strong>Defence must be coordinated, meaning that the means implemented act:</strong></td>
</tr>
<tr>
<td></td>
<td>c) on account of a warning and distribution capability;</td>
</tr>
<tr>
<td></td>
<td>d) following correlation of incidents.</td>
</tr>
<tr>
<td>Dynamism</td>
<td><strong>Defence must be dynamic, meaning that the IS has a security policy that identifies:</strong></td>
</tr>
<tr>
<td></td>
<td>d) a response capability;</td>
</tr>
<tr>
<td></td>
<td>e) a plan of actions;</td>
</tr>
<tr>
<td></td>
<td>f) a scale of severity.</td>
</tr>
<tr>
<td>Adequacy</td>
<td><strong>Defence must be adequate, meaning that each (organisational or technical) means of protection must have:</strong></td>
</tr>
<tr>
<td></td>
<td>d) its own means of protection;</td>
</tr>
<tr>
<td></td>
<td>e) a means of detection;</td>
</tr>
<tr>
<td></td>
<td>f) response procedures.</td>
</tr>
<tr>
<td>Completeness</td>
<td><strong>Defence must be complete, meaning that:</strong></td>
</tr>
<tr>
<td></td>
<td>d) the assets are protected according to their criticality;</td>
</tr>
<tr>
<td></td>
<td>e) each must be protected by at least three lines of defence;</td>
</tr>
<tr>
<td></td>
<td>f) feedback is formalised.</td>
</tr>
<tr>
<td>Demonstration</td>
<td><strong>Defence must be demonstrated, meaning that:</strong></td>
</tr>
<tr>
<td></td>
<td>d) defence is qualified;</td>
</tr>
<tr>
<td></td>
<td>e) there is an certification strategy;</td>
</tr>
<tr>
<td></td>
<td>f) certification follows the life cycle of the information system.</td>
</tr>
</tbody>
</table>

6.2.4.2 proof-based approach

The proof-based approach comprises an envelope scenario analysis similar to that performed at stage 2 and a failed component analysis. In the context of the case study, the demonstration will be limited to the analysis of a failed component in one scenario.

We will again consider scenario No. 2 presented previously:

- a malicious code delivered by e-mail is not detected by the antivirus application for whatever reason,
- the barriers that remain are the workstation's security policy,
- as well as the antivirus application on the server which is of a different type to that on the workstation.

If the security policy were also to fail, there would still be one barrier before the feared event, which is a satisfactory position.
6.2.5 Step five: Evaluation and audit

It appears useful, within the context of this document, to study significant security incidents in order to highlight the dynamic feedback phase.

The following security incidents will be studied:

- a failure of the server network interface card;
- a DAT drive failure.

The failure of a server network interface card is an *unacceptable event* if it is not dealt with within the required time as it might interrupt the availability of the teleservice. While awaiting repair, the incident is circumvented by applying the planned procedure of switching over the network from the main server to the backup server. This procedure results in a stoppage of approximately 30 minutes to swap over the two servers.

A DAT drive failure is a security event that is not allowed for on the event severity scale. It threatens the availability of the remote backup centre, but the security of the main site remains unaffected as there is duplication of information between the two main servers. The means provided for bypassing the event should therefore be analysed and the potential risks evaluated:

- backup is ensured in the form of a Zip disk of sufficient capacity (data is extracted by emptying tables and compressing if necessary to minimise the space required instead of a physical backup of the database as on the DAT drive). There thus remains at least one barrier before access to the backup centre is restricted;
- the potential risk, which is to compromise the availability of the main site, is covered by the lines of defence provided by the redundancy of servers and the backup site. There are three lines of defence against the feared event (server redundancy, backup site and means of circumvention).

A virus contained in an e-mail attachment compromises the request reception system previously modelled, and for which the model highlighted a flaw in the scenario. This paragraph will therefore examine how feedback can be used to enhance the model and the scenarios. There are two aspects to be considered:

- the classification of the event on the severity scale and the corrective measures normally derived from the planning process;
- the study of potential risks and the enhancement of scenarios.
The classification of the event depends firstly on the means of detecting the incident that may have been highlighted at the following control points, classed in order of importance:

- detection by workstation's anti-virus system: this is not an incident, but a normal operation of the anti-virus system;
- detection by the workstation user before the virus has been able to act: this is a moderately serious event according to the modelling of malicious codes (there remains the protection of communication between the workstation and the server, the server's anti-virus system and finally the server's security policy (redundancy) and the backup site;
- detection by the server's anti-virus system: this is a very serious event as the request reception system is inoperative and because there is no other barrier than the security policy to protect the server (including the backup site reduces the level of severity, but this is a degraded availability requirement due to the very low probability of occurrence: its inclusion results from the consideration of residual risks considered to be unacceptable).

This incident highlights the importance of user training and the regular updating of applications. Preference must be given in this context to feedback as well as the implementation of indicators for detecting weak signals which when associated could prevent serious incidents. Hence, the repeated detection over time of user workstations attacked by viruses should constitute a warning for the defence system.

Two principles should be kept in mind when considering how to deal with each new weakness detected:
- Prevent regression;
- Improve if cost-effective.

The other tasks planned for this stage are not specific to in depth defence with the exception of the trend chart section that must incorporate the incident severity scale.
Comment Form

Please send completed forms to the address below:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP, FRANCE
conseil.dcssi@sgdn.pm.gouv.fr

Contributor details
Name and organisation (optional): .................................................................
E-mail address: ..............................................................................................
Date: .............................................................................................................

General remarks about the document
Did the document meet your needs? Yes ☐ No ☐

If you answered Yes:
Do you think the document's content could be improved? Yes ☐ No ☐
If you answered Yes:
What else would you have liked it to include?
..................................................................................................................
..................................................................................................................

Which parts of the document do you think are unhelpful or irrelevant?
..................................................................................................................
..................................................................................................................

Do you think the document's presentation could be improved? Yes ☐ No ☐
If you answered Yes:
What aspect(s) could be improved?
- readability and/or understanding ☐
- presentation and formatting ☐
- other aspects ☐

What improvements would you like to see in this area?
..................................................................................................................
..................................................................................................................

If you answered No:

Please state what area was unsatisfactory and specify what you would have liked to be included:
..................................................................................................................
..................................................................................................................

What other subjects would you like this document to have addressed?
..................................................................................................................

Page 50 of 51
**Specific comments about the document**
You can use the table below to make any detailed comments.

"No." is a "serial number".
"Type" is a two-letter code:
The first letter specifies the category of comment:
- **O** Spelling or grammatical error
- **E** A point that was made requires explanation or clarification
- **I** Incomplete or missing text
- **R** Error

The second letter indicates its seriousness:
- **m** minor
- **M** Major

"Reference" indicates the exact place in the text (paragraph number, line, etc.)
"Content of the remark" is where you should write the comment.
"Proposed solution" is used to submit a proposal for solving the problem described.

<table>
<thead>
<tr>
<th>No.</th>
<th>Type</th>
<th>Reference</th>
<th>Content of the remark</th>
<th>Proposed solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Thank you for your contribution