Integral Security of Organisations as Living Systems

A Systemic Approach to GRC

Author's Name: Rafael Rodríguez de Cora

Managing Director: Computer Aided Logistics (CALS)

Madrid, Spain

November 14th, 2016

E-mail: rrcora@calogistics.com

Registro General de la Propiedad Intelectual
Nº de Asiento Registral 16/2017/2675
5 de mayo 2017
Fecha de efectos: 15/11/2016

CONTENTS: PAGE

I. INTRODUCTION

Despite actual threats and real attacks, organisations still don't have proper and integrated defence mechanisms under growing threats. Organisations currently deal separately with various concepts related to the different types of Safety/Security and continue to maintain 'different types' of security which are scattered and managed by different departments, with heterogeneous and uncoordinated methodologies and responses to incidents or attacks, in disperse ways and with no coordination. They are not prepared to respond to cyberthreats and they approach Security (Safety or Security) in an isolated way.

Our aim in this document is to propose a different approach to integrate the concepts of Security and Safety and to **think of the organisation as an integrated living system**, with life cycles and objectives of its own.

This means establishing a **Framework for Integral Security** based on the defence mechanisms of living systems, which have been developing strategies and mechanisms for defence, attack and survival during millions of years, including the development of immune systems.

We have used some of the concepts from **General Systems Theory**, which is the interdisciplinary study of Systems in general, with the goal of elucidating principles that can be applied to all types of systems at all nesting levels in all fields of research. Systems Theory can be considered a specialization of systems thinking with an emphasis on generality useful across a broad range of systems.

A central topic of systems theory is self-regulating systems, which are found in nature, including the physiological systems of our body, in local and global ecosystems, and in climate—including human learning processes and ethical values.

These concepts will be explained with more detail afterwards, and have already been presented in the following dates and conferences:

- February 2012 – PESI – Work Group Integral Security: Concept of Integral Security as the Immune System of the Organisations
- April / May 2013 – PESI – GT Security Project. Possible European Project
- October 2014 – 9th International Congress of European Union for Systemics. Valencia.
- October 2016 – PESI – Bilbao Congress S^2R about "The Future Safety & Security Research in Europe" – European Forum.

I.1. - Fragmented Security

When surfing the Internet searching for 'Integral Security', one finds nearly 12,3 millions of references (as of September 2016), but these relate to different types of security, with no concept of integration: Physical Security, Logical Security, Perimeter Protection, Personnel Security, Information Security, Environmental Security, Industrial Security, Public and Private Security, Occupational Safety, Industrial Safety, Security Alarms and Protection Systems, Surveillance and Protection Services, Cybersecurity, Emergency Services, Law Enforcement, Health and Safety at Work, Security Awareness, Corporate Security, Process Security, Critical Infrastructures, and so forth.

Integral Security is still not a concept which is implemented in organisations and in Society. Some recent trends talk about the convergence of Physical Security and Logical Security as a solution for Integrated Security, including Cybersecurity and Critical Infrastructures, which are now hot issues.

Other recent trends mention the convergence IT / OT as a solution, for a connected enterprise.
But this is not enough. A general characteristic of Integral Security and implementing Risk Management Systems is complexity, and organisations are today more vulnerable than ever to growing external and internal threats, without a holistic approach.

Organisations are also in continuous change, with more strict laws, and having to interact with different types of environments locally and internationally. This is correct in general terms but generates constraints in the organisations and allow more "liberty of actions" to cybercrime.

Some statistics show that now a days, 90% of commerce is done by ship and in cyberspace, which takes us to an additional concept of having to act also in **multiple spaces** (land, sea, air, space and cyberspace).

I.2. - New Systemic approach

If we think of an organisation as an integrated living system, which has to survive and protect itself to fulfil objectives, it means that we have to establish and identify the different organic subsystems and its objectives. Survival means that the organisation itself and each organic subsystem are in a permanent conflict between internal and external forces that help or hinder its growth, sustainability and fulfilment of the objectives.

This way of thinking will help in designing a framework for a better understanding of risks and controls and how they should be identified and managed. Organisations have to interact with the environment and with other systems and as General Systems Theory tells us, they are never in isolation, so we also have to think about an **Integrated Ecosystem**, with **systemic concepts** so it can have centralized treatments and responses for the different types of attacks, a coherent risk management and control implementation, and an awareness plan to stress the fact that security is everybody's responsibility and that it is a world-wide problem, so organisations have to be prepared adequately and should act accordingly.

Furthermore, if the attack is too strong and their resilience is broken, organisations by themselves cannot guarantee their own defence. They have to rely upon other organisations of higher level that can provide protection, such as police and fire departments, civil services, legal protection, national and international organisations, etc. This has important consequences as well, since organisations have to **Comply** with the Environment in order that organisations of higher level can help them, if needed be.

As the military say, just with a defensive attitude you cannot win a war. The arms race now takes place in cyberspace. So we do have to focus on an integrated and global approach to Security in all spaces.

We know **100% of security is not possible**, so maybe we should be talking also about different levels of protection. Security is like Health: We only remember it when we have lost it.

I.3. - Threat Horizon

There are many organisations world-wide, such as the Information Security Forum (ISF) [1] that are concerned about the Threat landscape for organisations. For instance, to assist ISF Members, the annual ISF ***Threat Horizon*** report takes a two-year perspective of major threats, describing potential implications and providing recommendations to organisations.

The ISF uses the PLEST methodology to indicate that threats come from different environments:

Figure 1. ISF PLEST Methodology

- **Political**: Regional instabilities, as in the Middle East, Increasing terrorist attacks world-wide. Energy problems, etc.
- **Legal:** Increased laws and regulations. Difficulty of Compliance. New laws for Information Security and increased problems for inadequate management of information security and data breaches, etc.
- **Economic:** More business and applications in Internet. Growing organized crime. Business Continuity. Climate change. Physical catastrophic events.
- **Socio-cultural:** Work at home vs. Work at office. Teleworkers. Different working hours across the organisation.
- **Technological:** Digital convergence of media. More capacity and new plug-and-play devices. New technological architectures. Cloud computing.

Another international organisation, The World Economic Forum is also concerned about the Global Risk Landscape and states that the world is, insufficiently prepared for an increasingly interdependence and complex risk environment.

In its WEF Global Risks Report 2016 edition, presents a report on 29 global risks which are divided into five categories: ***economic, environmental, geopolitical, societal and technological***. [2]

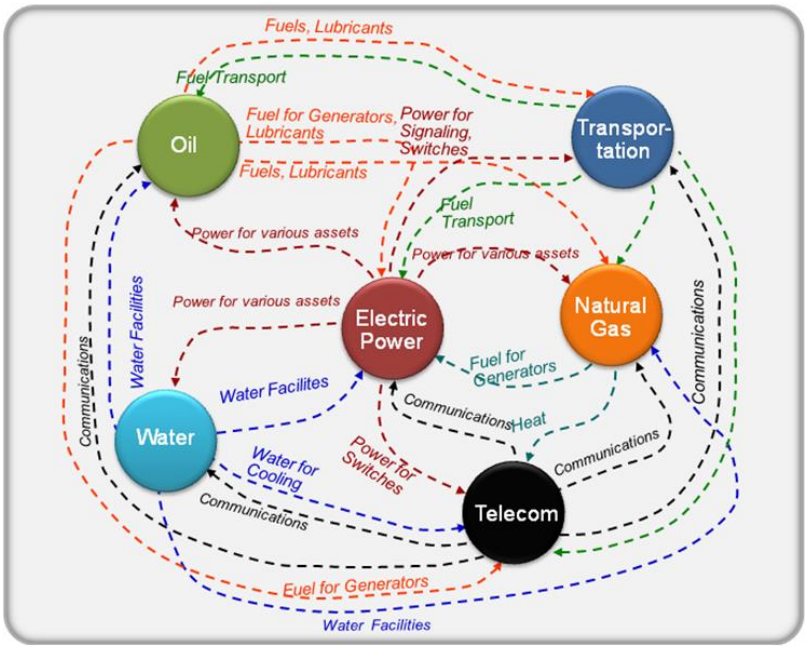
These two organisations give us a clue where threats might be coming from, and can help us design a framework, to define sources of attacks worldwide.

I.4. - American Blackout:

Research studies have estimated what would be the implications of a 10-day power grid outage caused by a cyberattack. There is even a film about it [3], and one of the reasons why Governments worldwide are taking measures to protect their infrastructures

These cascade effects could happen:

- Electrical power fails
- Communications systems fail
- Transportation systems stop
- Basic supplies start to lack
- No water can go up above 6th floor
- Overcharge of emergency services
- Problems with public health systems
- Wastes not collected generate contamination
- Lack of confidence of the population. (Disturbances, riots, fights for survival, etc.)
- Dangerous and difficult times. Law infringement.
- Preparation for the worst. Number of victims raises.
- Defence of the Nation. Army has to take over.
- Electrical energy comes back. Takes time to pick up the pieces and go back to initial situation.



Ten days without Electric Energy. Progressive Impacts

II. SYSTEMS AND MODELS

Systemic concepts and systemic approaches obviously have to do with systems, and systems have to be understood by means of models. We are surrounded by Systems of different types which might be more or less complex, and we try to understand them and interact with them. In most cases and depending on the complexity of the system, for any work or complex project, we have to work with MODELS.

Models can help us manipulate or understand the complexity of the original system by means of reducing the variables and information of the original system.

By definition the model is a partial view of the system that has been designed for a specific objective, so it should never be taken as the real system.

We are dealing with Complex Systems every day. Complex Systems are always found in the fields of Economics, Physics, Sociology, Biology, Psychology and other disciplines [4].

II.1. - General Systems Theory and Cybernetics

In 1954 The Society for General Systems Research (SGSR) was organized and some years later the Viennese biologist, Ludwig von Bertalanffy (1968) developed his *General Systems Theory* [5] to explain some of the main aspects of systems.

A system according to von Bertalanffy is a set of components with attributes that interact dynamically with each other forming a whole.

The main purposes of the General Systems Theory, according to von Bertalanffy are the following:

- *There is a general tendency towards an integration in the various natural and social sciences.*
- *Such an integration can be explained by means of a General Systems Theory*
- *Such a theory can be an important means to explain other theories in non-physical fields of science.*

Depending on the point of view or level, a specific component might be a system or subsystem itself, or part of another one. A system might be a pair of scissors, a home, an automobile, a human being, a cell, a family, an organisation, a city, a universe, etc.

Therefore, systems might be also classified as ***Living*** or ***Non-living*** systems. *Non-living* systems include some systems created by man (Artificial) such as computer systems, an aircraft, production machines, etc., and others created by nature, such as forests, solar systems, galaxies, and so on. *Living* systems then include plants, animals, people, human organisations, communities, nations and the world. *Living Systems* are also grouped together with a certain interdependence forming ***Ecosystems.***

In any case, one of the most important concept of a System is that the "whole" is greater than the sum of its isolated parts (holistic approach).

It is also generally accepted by the laws of physics that the natural tendency in nature is to move towards disorder (entropy). That is, there is a natural tendency in systems to collapse to an internal disorder.

When this takes place in systems created by humans (organisations), we try to establish the lost order to accomplish objectives by means of work, controls, procedures, energy, etc. (negentropy). General Systems Theory relates the concepts of information, entropy and negentropy.

To maintain order in a system and in compliance with its objectives it is required that it has internal communication channels, for feedback and correction mechanisms. Maybe we should also talk here about memories and "experience".

This is also linked with the science of Cybernetics, which takes care of control and feedback mechanisms if objectives fail to be accomplished. Norbert Weiner in its "Cybernetics" [6] studied systems with the central notion of feedback. In following years many other concepts and notions about systems were developed, such as the Turing machine, Behavioural Theory, Graph and Networks Theories, Set Theory, Information Theory (Shannon and Weaver), Game Theory (von Neumann and Morgenstern), and so on.
Cybernetics is oriented to find laws about auto-regulation, feedback, information, communication, etc., in human beings, other organisms, and machines. **These concepts should also be applied to organisations**.

Another final concept related to the above for Living Complex Systems is the level of autonomous decisions that the system can take (autopoiesis). In general the more complex a system is, the more autonomous it can be. They are able to produce and reproduce the conditions of its own existence, so they are capable of maintaining its own **finality** or stable purpose internally despite the frequent pressures for disruption from the environment. This is what is known sometimes as **"free will"**.

More recently further studies have also developed new ideas and applications applying System thinking to specific complex problems, such as Systems Dynamics, which studies behaviour and modelling of complex systems [7].

II.2. - Adaptive Complex Systems

For the purpose of this document we will adopt the definition from the book **"The Quark and The Jaguar"** by Murray Gell-Mann about Adaptive Complex Systems [8]: "*An Adaptive Complex System is a system that acquires information (from its environment and from its own system), identifies regularities and* ***condenses*** *them into a* ***"schema"*** *or* ***model****, and acts on the environment according to such model"*.

Living Systems start with a **"genetic" determinism** that defines how they have been designed or created, with what scope (limitations) and for what purpose (known or unknown).

Then the "genetics", which is just a "**program**" (possibilities), has to develop and interact within its natural, artificial and virtual environments to be able to maintain structures, manage resources and distribute products and services, which are of a **probabilistic** nature.

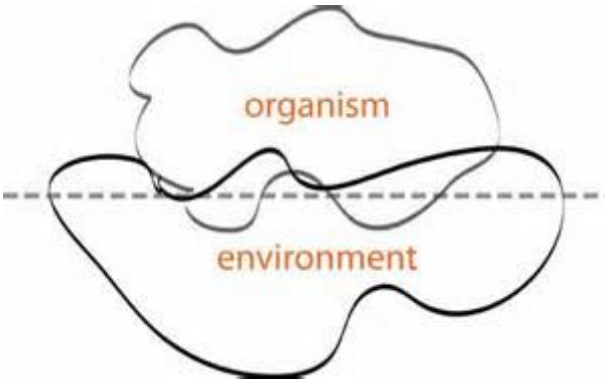


Figure 2. Interactions between organisms and environment

To develop this "program" interacting with the environment and restricted by the "genetic" limitations, the Adaptive Complex System has to cope with an **uncertain future** (capabilities), through **decision-taking** mechanisms often without all the pertinent information, to reach objectives, according to its logical and physical possibilities and limitations.
This important concept that Adaptive Complex Systems have to **make decisions** in order to fulfil a purpose or objectives, is one of the more fundamental ones, for living systems.

The main initial purpose or objective of living systems is staying alive (**preserving its own life**) and reproducing themselves, so life goes on after the specific living system disappears. The other purpose is to **comply with its objectives** (whether they are conscious of them or not).

In some other more developed Adaptive Complex Systems such as humans, another type of system emerges: ***Virtual*** systems. From the earlier phases of evolution man has been confronted by an unknown and threatening Universe and had to make ***"virtual models"*** to survive, creating concepts ideas and explanations about the forces of nature that a limited brain could not cope with.

Over time this has developed into ideas and ideologies that have also acted on the environment for better or for worse. Furthermore, now we know by experiments that ideas depress or stimulate the organism. Ideas interfere with the autonomic functions of the body and are also projected into the social world. Ideologies may be conceived as complex virtual systems, which mobilize individuals and groups toward more or less rational and intelligent actions.

From these ideas or virtual models, a set of values, ethics and rules had to be developed to ***"comply"*** with the system itself internally, and with the environment externally.

However one of the problems with this type of systems is that they are rigid and do not frequently adapt themselves to new knowledge, to changes in the system itself or in the environment, or to circumstances, because they are linked to emotions. (In the organisations this means "culture").

This implies that many models stay the same over time without evolving, when the environment or circumstances change. This lack of flexibility frequently is the cause of failure of organisations to fulfil objectives.

Maria Blasco, researcher and Director of the CNIO (Spanish National Centre for Oncological Research), says that our health depends on Genetics about 20% and on 80% of the habits of living we have [9]. This could also be very well applied to organisations.

Another very interesting book edited by a famous US Psychiatrist, Dr. Peter Titleman, talks about the Bowen Family Systems Theory, which uses emotional triangles as a powerful model for systems thinking applied to solve complex emotional interactions in families. [10]. These concepts could also be applied to solve complex behavioural interactions in organisations and in society.

II.3. - Subsystems. Biological Systems

Adaptive Complex Systems have subsystems and functions to interact with the environment and to comply with objectives, communications, security and safety, and other functions.

As we have said in the introduction, Nature and specially biology through evolution, and accidentally, have been experimenting during millions of years to reach solutions for survival and have arrived to the most competitive options for security and risk management.

We think that by "copying" nature, its defence and attack mechanisms when under threats, and its immune system, we can have hints as how to design an integral risk management and security system for organisations, better adapted to the circumstances, and maybe without accidental results.

Just as a reminder, a System or Subsystem in the human body means a collective functional unit composed of different organs in total coordination with each other.

Organs cannot work in isolation because there are needs and functions of each organ that cannot be satisfied by the same organ independently.

So all organs in the human body need the support of the other organs to be able to comply with their functions and therefore make an organic system. This means that they must work in an **integrated and complementary manner**.

These concepts of **integration and collaboration** are very important and will be developed further for the application of integrated security in the organisations. [11]

Example of dependencies of organs one from each other, in a system:

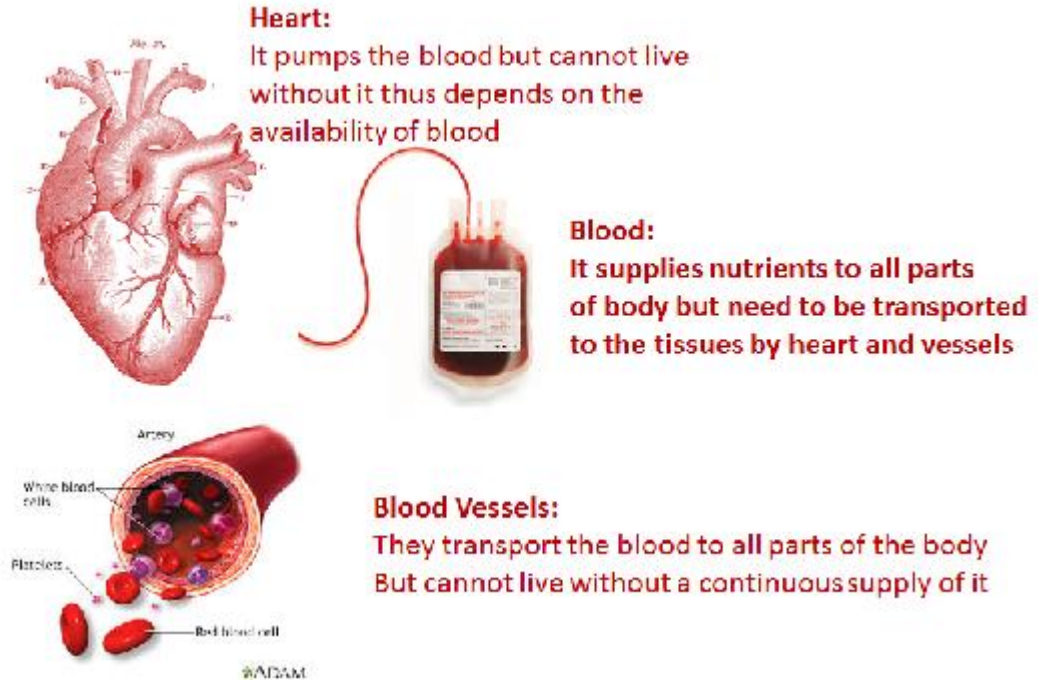


Figure 3. Organ dependencies

The human body has **different subsystems**, specialized in different functions, which require support and collaboration from the other systems for life support and for complying with objectives.

If any of the Systems is damaged the human body is turned unstable and this instability can cause illness or even death (The functions, or the system itself will disappear).

The instability caused by the damage of one system cannot be stabilized by any other system because each one has specific functions.

This might give us some further clues as to how to apply these functions to the organisations, as Living Systems [12]:

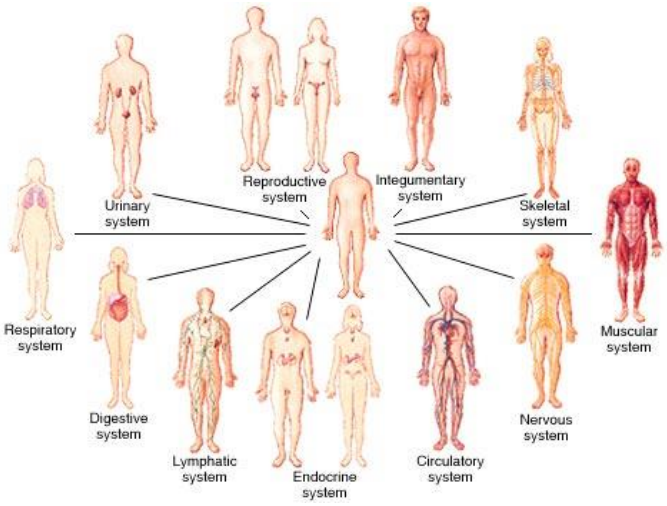


Figure 4. Subsystems of the Human Body

- Skeletal System: Support and Structures (bones), a hard framework around which the entire system is built together with associated cartilages. Almost all the hard parts of human body are components of human skeletal system. Joints are very important because they make the hard and rigid skeleton allow different types of movements at different locations. If the skeleton were without joints, no movement would have taken place and the significance of human body; no more than a stone. So even in this most rigid system there has to be some flexibilities.
- Muscular System: Is the system that provides motor power for all movements of body parts. Muscles have the ability to contract actively to provide the force for movements of body parts. Muscular system is an important system of human body because without it, life will completely stop. Muscles produce not only those movements that are under the control of our will and that we can see and feel, but also those movements that are responsible for activities like breathing, digestion of food, pumping of blood etc. (Locomotive System / Displacements of the system in the environment).

- Circulatory System: Circulatory System means the system of heart and blood vessels of human body, which is also known as Cardiovascular System. The blood flow is necessary for the existence of life. Perfectly functioning cardiovascular system is so important for human body, that if it stops for a minute, rapid death will occur. Logistics and Distribution functions. Materials are exchanged between blood and body tissues. Provides nutrients to body parts and removes excretory products from body parts. Protects body against infection. Distribution of heat. Also acts as a control mechanism.
- Digestive System: Is the food processing system of the human body. The overall process of digestion and absorption of food occurs here. Resources and Energy Capturing and Solid Waste Management. Filters and eliminates toxic inputs. Works with other organs such as the liver and pancreas. So not only acts as manager of energy and resources, but also as **protection and elimination of toxic elements** from the outside or produced by inside production.
- Urinary System: Urinary system is also known as excretory system of human body, for production, storage and elimination of urine. Filter for elimination of toxic agents. Formation and elimination of urine is important for human body because urine contains nitrogenous wastes of the body that must be eliminated to maintain homeostasis. Nitrogenous wastes are formed by metabolic activities in the cells. These nitrogenous wastes along with excess of salts and water are combined in the kidneys to form urine, which is subsequently disposed of. Urinary system is important for keeping the internal environment of the body clean. Urinary system maintains proper homeostasis of water, salts and nitrogenous wastes. Liquid Waste Management. Osmoregulation. Acid-Base balance.
- Nervous System: Central Communications and Coordination System. Command and Control System. Has to have senses and sensors to collect information from the environment and from inside the system. Voluntary and Involuntary responses. Information Receivers and Transmitters. Nervous system is the chief controlling and coordinating system of the body. It controls and regulates all voluntary and involuntary activities of human body.

  There are three characteristic properties of nervous system of human body: Sensitivity, Conductivity and Responsiveness. Motivation, Learning and Memory mechanisms also have a very important function here.

The human brain has three levels for preserving **health and security systems** which also impact on preservation of security and responses:

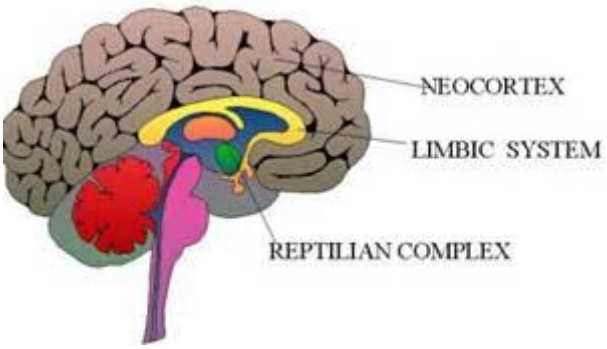


Figure 5. Brain Functions

- **Reptile**: (Thalamus and Hypothalamus) Basic Brain - Governs basic instincts, such as hunger, thirst, sexuality. Defence of the territory. Regulates the involuntary physiological functions of the body. Does not think or feel emotions. Manages risk and survival in a very elementary binary way: **fight or flight**. Goes into action when the rest of the organism needs it. Responsible for ***automatic decisions about security***. Guardian of life since we find in it the basic senses for survival and defence/attack mechanisms. **The first agent to detect threats and dangers**. Allows for rapid and elementary responses that do not require complicated emotional or intellectual processing.
- **Limbic**: On top of above the reptile brain, we have the limbic brain. It stores our emotions and memories. Daily needs for happiness, or feelings of sadness and other basic motivations. Sentimental development. The limbic system is associated with the capabilities of feelings and wishes, care of others, protection, and long-term memory. The investigation of this area seems to support the notion that all information that enters the system is supervised and controlled by the limbic system, which constitutes a vital function for survival. It can also be considered as the affective brain that energizes ***behaviours to fulfil objectives***.

- **Neocortex**: On top of above the other two brains and constitutes the rational brain. Allows us to have a ***conscience and to control emotions***. Capable of cognitive capacity, having functions such as memorization, concentration, auto-reflexion, problem resolution, **ability to choose an appropriate behaviour**. Conscientious part of the system, not only at a physical level but also at an emotional level.

- Reproductive System: Male/female organs that are part of the overall reproductive process of living systems to produce offspring (a new system or subsystem). For the survival of life, reproduction is a necessary process because otherwise no new life will be formed and old life will disappear, after finishing its life cycle. Every individual has a limited life span and no living system can survive forever. Mutations or adaptations to new circumstances in the environment take place here. It can also be thought as a security mechanism for the future and part of the evolutionary cycle.
- Lymphatic System: Is the drainage system of the human body and accessory to the venous system and other systems. In addition to its drainage function the lymphatic system is also an effective defence mechanism of the body. First line of defence of the body during antigenic emergencies. Removal of particulate matter. Filter and Purification against harmful agents. Maintains a reserve of blood for emergencies. Protects the body against any infectious agent that enters the blood. Works as a security agent against all incoming agents from alimentary canal and respiratory tracks. Generation of immune responses.
- Endocrine System: System of glands in the body for regulatory functions. Each of these glands secretes one or more different hormones in the blood for different functions. Hormones are segregated by the endocrine system to regulate functions such as growth, mood, development, metabolism, etc. The control of body functions by the endocrine system is called chemical coordination and is a ***long-term control system***.

  Some of the glands and organs involved are the Pituitary Gland, Pancreas, Gonads, Liver and Kidneys. Parallels with the nervous system in control of body activities. Each hormone has a specific control function.

- Respiratory System: System of respiratory passages, lungs and respiratory muscles of the human body. Exchange of gases and energies between the system and the environment. In the process of exchange of gases, human body gains oxygen and gets rid of carbon dioxide. Air filter for elimination of toxic agents, such as lungs. Elimination of carbon dioxide. Oxygenation of blood. Acts as a control mechanism. Respiratory system is extremely important for human body because the process of respiration cannot be stropped even for a few seconds. If the process of respiration stops even for a minute or two, the condition will become serious and will ultimately end in death.
- Integumentary System- Membrane: This is the organic system that protects the system from damage and defines the limits of system's physical identity. It differentiates the system from the environment and at the same time acts as a filter.

  In the human body consists of skin, hair, nails, sweat glands, etc. It serves as a cushion to protect deeper tissues. It also excretes wastes and regulates body temperature.

  With its different types of sensors it is able to detect pain, sensations, pressure, and temperature.

II.4. - Other related Subsystems

Apart from these subsystems there are other systems that either relate or integrate some of the above, which are also very important in Adaptive Complex Systems, and therefore in organisations.
They are mostly related with the relationship between the system itself and the environment, and are basic for threat assessments and defence functions:

- **Immune System** - Defence and Attack mechanisms against harmful internal and external agents (Safety). Responses to attacks from the environment. Life support systems within acceptable limits for survival in the environment (Security). The immune system is one of the most important systems of the living systems and is composed of many of the functions and organs previously described. Strategies for survival. Natural acquired immunity. It implies filters and key indicators that can indicate a problem. Modern medicine helps us to identify personal risk by checking that key indicators are within range, such as blood pressure, cholesterol, heart rate, sugar in the blood, etc. Organisations also have Key Indicators.

- **Environment**: We should consider the environment (or at least part of it) as a subsystem of the system itself. As was mentioned before, we cannot talk about systems being independent or in isolation. The system will have to be studied in relation with its own subsystems and with its environment (supra-systems). Each variation or change in each part can affect the rest of the parts, the system, and even the environment. The environment of a system consists of all other systems, subsystems and internal and external forces to the system, so that a change in the environment's attributes or actions affects the system and vice versa**.**
  The environment has an impact on the system of reference and the system itself has an impact on the environment. In fact, most of the objectives, responses and actions of the system have to be developed in the environment.
  The part of the environment that really affects the system, and the system can act upon is also called the **Field of Influence** or Space of Influence of the system within the ecosystem: This is the **Outside Perimeter** of the system. Other systems in the ecosystem might have a special relationship with the system of reference, such as competitors, symbiotic, depredators, parasites, and so forth.

These types of relationships will also have an important impact on the survival mechanisms and compliance with the objectives of the system. In fact, a recent article in a Spanish newspaper [13] comments that worldwide studies have confirmed that an equilibrium should be preserved among different species and this is proven by mathematical laws.

After having studied data from 2.260 ecosystems in 1.500 geographical areas, the relationship between depredators and preys is always around ¾. If the ratio is broken, it's bad for both. This could also be applied to organisations, marketplaces, etc. This is one of the reasons why Monopolies and Cartels are harmful.

- **Supply Chain**: Also part of the environment includes all the processes to interchange materials, energies and resources to and from a specific system to other systems, within the field of influence.

  They are also part of the system's security because if they do not function properly, the system might not have adequate provisions of materials and energies, and might not be able to survive. Also if the supply chain is not "healthy" enough, it might contaminate the system**.**

  From what we have said before, and due to the complexity mentioned we should be talking more about **Ecosystems or Supply Networks**, rather than Supply Chains.

III. ORGANISATIONS AS LIVING SYSTEMS

III.1. - Objectives and Life Cycles

We will now try to map the biological systems described before into Organisations and Corporations designed by humans, as Living Systems with specific *objectives* and *life cycles*. The different subsystems and functions involved have also their own objectives and life cycles, which should be well identified.

Taking the basic concepts of General Systems Theory, the biological concepts described before, and general accepted organisational concepts, we can start making a model for an organisation as a living system, starting from these important facts:

- Organisations have to be constructed with an **idea** in mind (Plans, Objectives, Design, etc.) normally by another organisation or system of a higher level. Its processes or functions have to fulfil its objectives, within the internal and external constrains and in a certain time frame.
- As mentioned before, a complex adaptive system, such as an organisation has **one or many objectives**. Some of the most obvious ones for a Corporation are Quality of Products and Services, and Security.
- Organisations have **owners and stakeholders**, which could be external persons in the organisation, or other external organisations, which have needs and to which the organisation has to report. Normally these owners and or stakeholders define the **objectives** of the organisation. There are also other stakeholders that could be affected if the objectives are not fulfilled, such as the persons that work in the organisation, clients, suppliers, etc.

- Organisations therefore, have three **main basic functions:** Governance, Internal Resource Management (life support mechanisms), and use of Operational Units in the Field (Objectives, Missions, etc.).

Figure 6. Main Basic Functions

- This idea is also taken from military operations, which have experience dealing with threats, risks, and utilization of operational units, with the following priorities in the field:
  - To preserve life (internal survival systems, resilience).
  - To move from one place to another (adaptation to the environment).
  - To combat – use of operational units for Missions, Objectives, etc. (defence and attack mechanisms).
- The suggestions from CobIT 5 of ISACA [14], should also be taken into account: Government Processes (Top Management) should be distinct from Management Processes (Resource Management).
- The **life cycle** of the organisation as a whole not only depends on its "biological" nature, but also depends on the life cycle of its resources, processes and outputs, and of the specific circumstances of the environment.

CobIT 5 also suggests the following life cycle for an organisation:

- Plan
- Design
- Build / Acquire / Create / Implement
- Use / Operate
- Evaluate / Monitor
- Update / Dispose

This can give us a good idea how to design the life cycle of an organisation and of the processes in it.

III.2. - Processes. Functions.

Each of the subsystems or functions of a living system (or an organisation) are based on **processes**. These are the basic functional components of the system to comply with its objectives, which being sustainable organs of the functions involved, might be under threats and put at risk. Each **Process** has a series of **Activities** and:

- It is a **horizontal function** concept. For an organisation this might include "purchasing", "sales", "production of goods" "services", etc. Has a beginning and an end. This is in itself an important concept since many functions in the organisations are still vertical, with no organic interactions between other functions or departments. This fact creates information and coordination problems that should be avoided.
- Has to have an **owner**, for accountability, which can be a person in the organisation, or another process of a higher level.
- Has to have **resources** assigned so it can fulfil its objectives. (Persons, Materials, Budgets, Information)
- Has **threats**, and certain **associated risks**, which have to be taken into account and managed, have to be evaluated, and have to be controlled so the process can have a reasonable security and comply with the risk appetite of the organisation. Various other internal departments and other external organisations may be **negatively impacted** if the process goes wrong or is under attack.
- Some processes may be **critical** for the business or for the organisation. If they are at risk, **proper controls** have to be implemented to avoid serious impacts.
- Each process or activity in living systems also has a **life cycle** of its own. This means that has a beginning (is born) complies with objectives, reproduces or transforms itself (optionally) has an end of cycle (operational end) and finally is taken out of the system (dies – transformation – links to other processes).
- Typical life cycles in a process look like the following Figure 7, in order to fulfil the organisation's Vision, Missions, and Objectives:

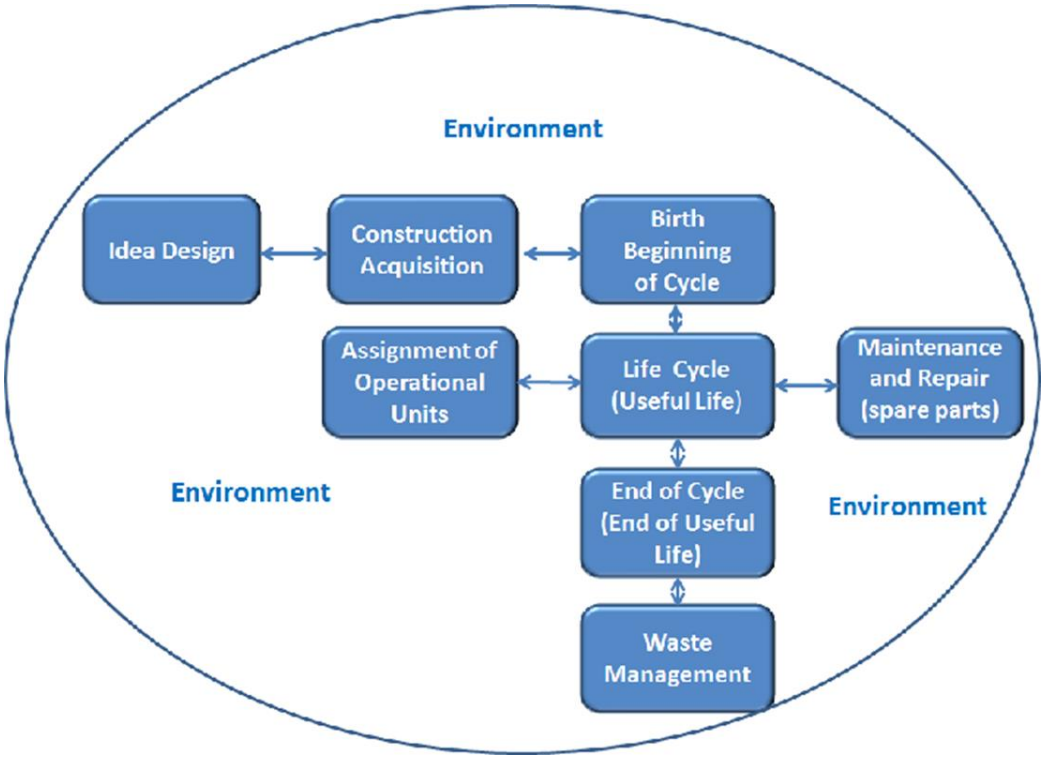


Figure 7. Life Cycles of a Process

- Has a **construction** period of the Process (Build, Acquire, Create, Implement), which implies also appropriate resources and energies.
- Has a **start of life cycle** or process (Process is "born" or generated by another process). This implies creation or acquisition, and selection of resources and energies.
- Has a **useful life** during a period of time. During this period it has to be assigned to **operational units** and may have to go through maintenance periods and repairs. The operational units are the ones that have to comply with action plans, missions and objectives in the field. In military operations they are the combat units (tanks, ships, planes, etc.). In organisations they are the infrastructures or departments to generate products and services that go to the environment. During this life cycle some other functions take place such as learning processes, **evaluation and monitor activities**, etc., to improve efficiency.
- Can also **reproduce** itself (Reproduction or other transformations of the process-optional). Upgrades. Reconstructions. Main overhauls.

- Has an **end of cycle**. Removal /End of operational cycle or useful life. Has filled its purpose or objectives, but not “dead” yet.
- Has an **end of process** or recycling. After death disposal. Waste Management (virtual trails still present, which might be a risk or harmful to other systems).

III.3. - Model of an Organisation as a Living System.

So with all the above concepts in mind we are now ready to define the living functions for an organisation, as an analogy of those from the human body. As Living Systems organisations will have similar functions as those of a human body, which in some cases we have grouped together. We also have to remember that the frequent steps that take place, regarding an organisation, are the following: ***Vision -> Missions -> Objectives -> Processes -> Activities***

Therefore, we propose the following model for an organisation, as a Living System:

- **Structures: -** Decision making Entities – Areas, Divisions, Departments, Assets, etc. (Organisational Structures), Facilities, Buildings, Machinery, Infrastructures, etc.) – (**Skeletal System**)
- **Governance. Control Mechanisms**. Elements for strategic definitions, such as Vision, Missions, Corporate Values and Culture, Ethics. Planning and Establishment of Strategic, Tactical and Operational Objectives. Has four basic functions:
    - **Command and Control System. -** Evaluations, Decision Making, Supervision. This concept is also associated with **risk management and control to maintain objectives in place** by means of feedback mechanisms. It seems that we could also talk about the three functions of the brain to organisations, mapping the functions of the brain to those in organisations: (**Brain**) – ***Command and Control, Internal Audits, Quality Management.***

- **Basic Governance Functions**. Responsible for automatic decisions about security. Basic sensors for defence/attack mechanisms. First line of defence to detect threats and dangers. Rapid and elementary responses by means of sensors. A practical example might be the Real-Time Cybersecurity Risk Management System proposed by Simon Marvell [15]. Part of Risk Management function. **(Reptile Brain) – Real Time Operations - *Departments Management, Individuals***
- **Supervision and Control of Information**. Part of Risk Management function. Experiences. Long-term Memories (Learning memories, Experience, Incident Management). Revision and improvement. Metrics and Indicators. Balance Scorecard. Behaviours to fulfil objectives. **(Limbic Brain) - Vice-Presidents of Areas – *Middle Management***
- **Higher Governance Functions**. Stakeholders needs. Policies, Roles, Responsibilities. Supervision of Objectives. Motivations, Balance for Corporate Responsibility. Evolution. Compliance. **(Neocortex) – Board of Directors - *Top Management. External Relationships***

- **Information and Communication Systems -** Command, Communications, Control, Intelligence – C3I. In an organisation we should take into account that it is not only for the inside the system but also in the outside (sensors and intelligence in the environment, etc.) **(Nervous System) – *Inside and outside communication systems. Networks. Marketing. Prospective.***

- **Resource and Waste Management: -** Management of **Inputs** to fulfil objectives by having proper and assigned key resources in the appropriate quantities, to sustain life and the life cycle itself. In general terms the resources of an organisation are the following: (Energies, Materials, Persons, and Finances). In some other studies, Information and Communication systems are also taken as internal resources but we have preferred to upgrade this concept to an organic function of Governance, since we think is more important now, specially taking new Cyber concepts into account. (**Basic Internal Life Support Systems**)

  Some of the human subsystems mentioned before, that could come under this organic function are the following:

  - Exchange of energies between the organisation and the environment. Filter for elimination of toxic agents, with internal risk management and control functions. (Respiratory System)
  - Internal Supply Chain for Logistics and Distribution of energies and resources, with internal risk management and control functions. (Circulatory System)
  - Process for elaborating useful products for the organisation, from resource management, Solid waste management, Filter for elimination of toxic agents, with internal risk management functions. (Digestive System)
  - Filter for elimination of toxic agents, with internal risk management and control functions. Waste Management. (Urinary System)
  - Waste Management and internal Risk Management. (Lymphatic System)
  - Regulatory Functions, Filters, Balance, Long-term Control System. (Endocrine System)

- **Boundaries or Perimeters**. Organisations, as any other living system, have boundaries or perimeters that separates them physically from the environment and preserves its identity. Nowadays some researchers talk about the "***extended enterprise***" since with Internet there are no such clear boundaries. However the boundaries act as a protection and filter, and depending of the circumstances can make the system (the organisation) be re-opened or closed. In organisations we can think of this concept as walls, firewalls, etc., which are also subject to threats and risks.

  Some of the human subsystems that could come under this organic function are the following:

  - Integumentary System- Membranes: In the human body it consists of skin, hair, nails, sweat glands, etc. It serves as a cushion to protect deeper tissues. It also excretes wastes and regulates body temperature.

Relations between System, Membrane and Environment:

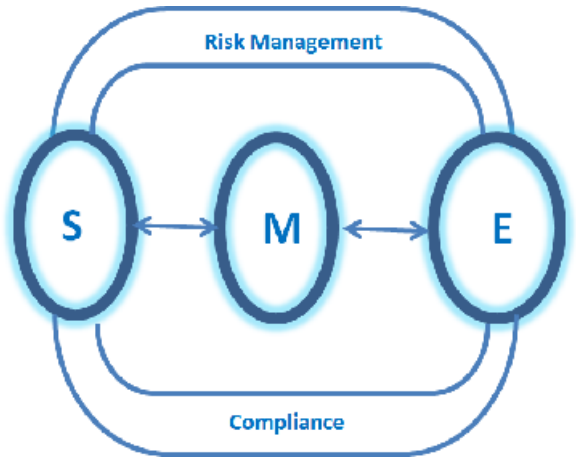


Figure 8. System, Membrane and Environment

S: System **M**: Membrane **E**: Environment

Filters, Membrane: Without them Systems could not survive. Protection Mechanisms. Metrics.

- **Production Processes (Organic Functions)**. The organisation elaborates these inputs by means of its subsystems or functions (**processes**), generating other products and services (**outputs**). These products and services will be inputs for other systems or subsystems inside or outside, creating recursive cycles. Production and Management of products and services. Some of the human subsystems that could come under this function are the following:
    - Internal Organic Production and Management of Products and Services.
- **Field of Influence (Environment).** Every organisation will also have its own field of influence, environment or Ecosystem, such as markets, accessibility to resources, intelligence, external life support systems, etc., which can be thought of as the external boundaries of the organisation. We can have five different spaces where defensive and offensive actions can take place, and where security should get implemented: ***Land, Sea, Air, Space and Cyberspace*.** These spheres or theatres of operations must be taken into account when assessing Threats, Risks, Controls and Actions. Living systems previously had land, sea and air only as environments. With modern technological advances human beings and organisations now have additional environments to cope with risks and controls in order to survive, such as outer space and cyberspace. Most countries consider these two new spheres as economic, social and even war theatres. Cyberspace forces different approaches for defence because of its world-wide aspects, instantaneous and catastrophic effects (as we have seen in the introduction), and disruption of the brain and nervous system.

To look at the same concept from a different point of view we could say that over time different spheres have developed to sustain life:

- Geosphere
- Biosphere
- Atmosphere
- Stratosphere
- Infosphere (Internet)
- Cognosphere (still to be developed)

- **Operations (Objectives, Missions, Plans)**. Fulfilment of objectives in the Field of Influence. Delivery of Products and Services in the field of action, Military Operations, etc.

  Some of the human subsystems that could come under this organic function are the following:

  - Operational Units. Use of operational units. Products and Services. Combat Units, Objectives, Missions, Action Plans.
  - Muscular System (Transport systems, Displacements in the environment of the system)
  - Reproductive System. (Spin-offs, Mutations, Mergers, Acquisitions, Franchises, etc.)
  - Supply Chain **External Supply Chains**, being a subset and part of the ecosystem related to interchange of energies and resources. Delivery of products and services**.** These supply chains can be of different types:
    - Physical Networks (Transportation networks, Utilities, etc.)
    - Logical Networks (Information and Communication, Social Networks, etc.)
    - Mental Networks (Education, Culture, Awareness)
- **Risk Management, Control & Compliance. (Integral Security).** As we have seen, the human body has many specific organs and subsystems related to this function. In organisations we seldom see a specific function for this. No wonder they are at risk without proper defences. Risk Management and Compliance, although independent go hand by hand (along with Governance), so we think these two functions should interact with each other and be given a specific and important rank in the organisations, as a **vital function**.

There are two main human subsystems that could come under this organic function of risk and control management, although sometimes the difference might not be clear:

  - **Immune System.** Basic internal Defence and Attack mechanisms and functions **within the system**. Mostly build inside the organisation for automatic life support.

In fact, there are some companies that are recently now already talking about this concept, such as: **Darktrace:** *"We are at the dawn of a new era in cyber defence, and the Enterprise Immune System is leading the way through it".* The "Enterprise Immune System" concept of Darktrace offers solutions to defend organisations against cyberattacks by means of using probability theory applications, to simulate behaviour and adaptation to changing environments. October 5th 2016 – CCI Congress. Darktrace presents the Enterprise Immune System in Spain. [16].

And **IBM** which is also starting to talk lately about immune systems for organisations, and cognitive security approach as well. Change from the Digital Enterprise to the Cognitive Enterprise. IBM Security Summit: Establish Security as an Immune System. [17]. IBM Business Connect: Welcome to the Cognitive Era. Cognitive Solutions for Complex Problems. IBM Watson [18].

- **Governance. Decision taking.** Basic defence and attack mechanisms and functions in the system to deal with threats and risks in the environment, and decision-taking mechanisms, after proper evaluations. (Limbic and Neocortex functions)

III.4. – Organisational Charts

Organisational charts must also adequately reflect the concepts above with a new systemic approach. They always have tended to be hierarchical and static, by departments.
Some "security functions", depend from different Security VPs, such as Information Security, Physical Security, Business Continuity, etc.

We propose a different approach by adapting the organisational chart to the organic functions we have described before.

This will give a more dynamic chart for responses and compliance with objectives and to manage risks, with leaner decision taking mechanisms. In some countries there are already organisations that have a Security VP (with no surname), and other 'securities', such as Business Continuity, Information Security, Safety, etc. reporting to them, but still without the concept of "integral".

Organisation as an organic or Cybernetic System with more detail and taking the environment into account:

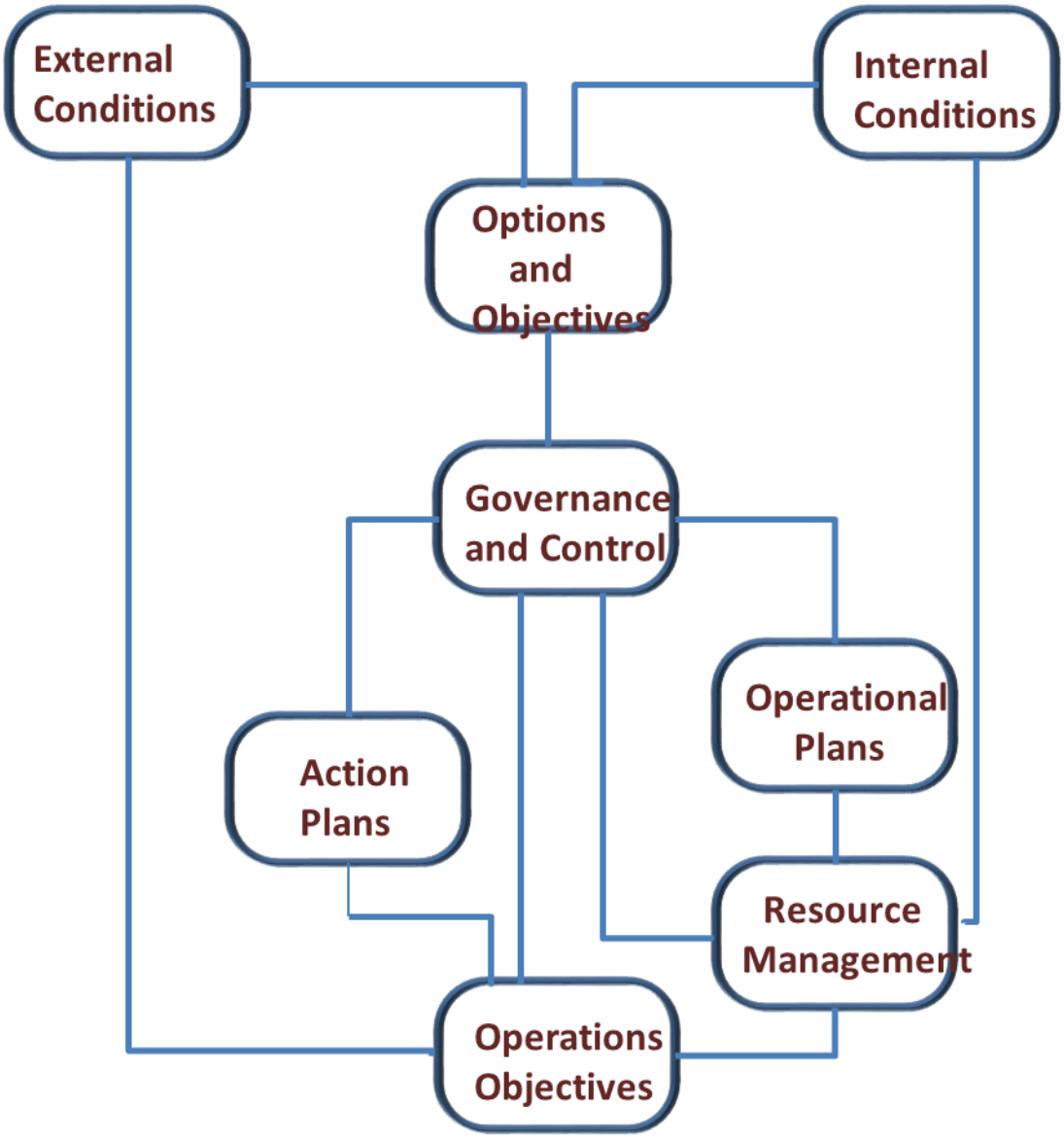


Figure 9. Cybernetic Functions

External Conditions (Environment): (Clients, Suppliers, Other organisations, etc.)

Internal Conditions (Genetics). Organisational Structure (Decision making entities – Areas, Divisions, Departments, etc.). Upper and Lower bounds for health and resilience.

Options and Objectives: Top Management. Stakeholders needs.

Governance & Control: Management (Evaluate, Direct, Monitor, Control of Administrative Processes, Establishment and Supervision of Metrics. Information Cycle)

Action Plans

Operational Plans

Resource Management – Metabolism - (Plan, Build, Operate, Execute, Monitor)

- Inputs (Resources, Energies and other means). People, Skills, Competencies
- Processes (Processing Production of Products and Services, Infrastructures, Organisation for Transformation-Structures)
- Outputs (Operations and Execution) Material and intellectual products)

Operations: Use of operational units, Compliance with Objectives

So taking into account these cybernetic functions and the model of an organisation as a living system, we propose the following organisational chart for a systemic organisation:

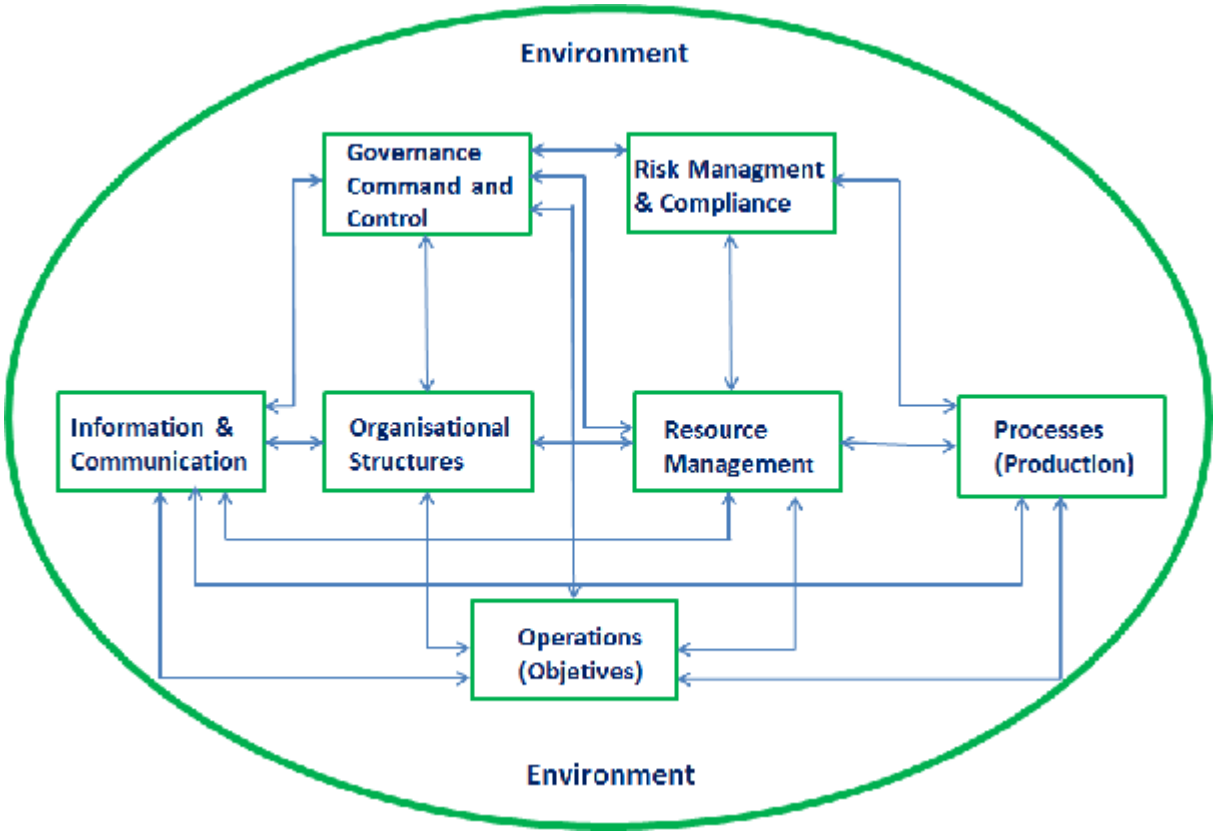


Figure 10. Organisation Chart for a Systemic Organisation

This figure above actually is not much different than for any reasonably well governed company today.

However it tries to reflect the fact that the functions of the organisation should not be hierarchical, but in a network relationship between functions (all interlinked with the rest). The organisation has gone from vertical departments with no coordination to process management with some coordination. Now it has to go towards organic and integrated functions with full coordination via internal networks.

Apart from this fact of functions in a network, we have added explicitly the most important function of Risk Management and Compliance (**the immune system**) as a vital one for survival, and of course with implications on the rest of the functions.

Also the Information and Communication function as the internal nervous system linked with the rest of functions.

To manage these kind of organisations new managers should be trained with a systems thinking approach.

III.5. - Change Management and Values

During their entire life cycle organisations have to cope with internal and external changes in order to survive. Governance Management has to provoke and manage change, taking into account that information is a fundamental resource, that it can act as an agent for change, and that it has a strategic importance.

This is one of the reasons why we have also suggested Information & Communication to be explicitly a separate vital function in the Organisation Chart above. Information Society brings with it new ethics for organisations and a change of values. This not only implies a new mentality of client service, but also different relationships with employees - and often even with the competition.

Ethical values and compliance should be other items in the Balance Sheet. Modern corporations now take into account its "Corporate Social Responsibility (**CSR**)", and what society demands from them.

Change should always be considered within the context of a cycle. In almost every kind of natural, biological and social system, we have the concept of cycle.

Organisations also have cycles. Change occurs constantly in these areas, which some are linked to the PLEST Methodology of ISF, already discussed:

A. *Political*
B. *Legal and Regulatory*
C. *Economic changes*
D. *Social and Cultural changes*
E. *Technological changes*
F. *Organizational changes*
G. *Changes of attitudes of the persons involved*

If change is not properly managed internal and external forces might end up destroying the system. Change is presented as a complementary concept of cycle, yet it has to be planned for and requires proper methodologies. In human organisations this is very much linked to the most important concept of **"values"**.

The value system of an individual, of a specific organisation, or of a given group or society is determinant when:

- Objectives are fixed or defined
- Plans and strategies are set
- Risks are evaluated and controls are implemented.

From our point of view there are two fundamental types of values for an organisation:

A) Absolute Values: One type that are defined by Francisco Parra Luna [19] in his article "An Axiological Systems Theory": Some Basic Hypotheses", from year 2001, and which we could define as **"absolute".** In this article it was argued that *"Social systems, from global societies to small organisations, are made up of human beings."* (And therefore have some basic needs and values to satisfy them). *"As a result of this variety human needs must be divided into two groups: universal and specific. The former are common to all humans living in a society (health, **security**, justice, etc.); the latter are culture-, group, tribe- or country-specific (dress, adornments, language, religion, folklore, etc.)"*

These **basic needs** and **cultural needs** are normally consequence of the objectives. Cultural needs is a value system that is shared by the organisation. Symbols are also important, such as slogans, rituals, flags, fashions, etc.).

Deviations from the established values corresponding to the basic needs will be a threat to the individual organisation.

Deviations from the established values corresponding to the cultural needs will be a threat to the society. (To other systems or organisations in the environment).

Life is a consequence of an equilibrium between needs, values, environment and objectives. Organisations will have to comply with objectives satisfying their needs within the values established by the organisation itself and the ones imposed by the environment (laws, regulations, etc.)

A general outline of the **"absolute or universal values"** proposed by Francisco Parra Luna – PRV (Reference Pattern of Values), *modified slightly by the author*, and applied to an organisation, could be the following:

- ***Beliefs:*** *(Basic need to believe in something, whether is an ideology, a religion, a culture, belonging to a group, objectives, missions, etc.) –* ***(Introduced by the author)***.
- **Health:** (Basic need for life maintenance and survival. Physical and Mental equilibrium. Resilience after attacks. Immune system)
- **Material wealth. Material Sustainability:** (Basic material needs. Acquisition of energies and materials. Supply Chain).
- **Internal Security:** (Basic need to protect the organisation internally against internal or external threats and contingencies).
- **External Security:** (Basic need to protect the organisation externally against internal or external threats and contingencies. Usually with the help of other Systems such as security agents, police, Health Service organisations, Civil Protection, etc.).
- **Knowledge:** (Basic need for Education, Training, knowledge and control of the environment, Culture, Experience, etc.)
- **Freedom:** (Basic need and liberty for movement, action and decision making, to comply with objectives within the constraints of the organisation itself and of the environment). Liberty of one system stops when it clashes with the liberty of other systems, and conflict will emerge.
- **Justice:** (Basic need for laws and regulations to distribute wealth, control of threats, equity, etc.).
- **Prestige:** (Basic need for esteem from others, corporate image, trust, etc.)
- **Environmental conservation:** (Basic need for equilibrium with environment, compliance with laws of nature)
- **Quality of activities:** (Basic need for the activities generated to be useful and not harmful internally and externally, Good Corporate Governance, Certification organisations, Laws and Regulations, Quality Assurance)

Threats and attacks nowadays orient themselves to do harm to some or all of these values to Persons, Organisations and Society.

B) Relative Values: Other type of values that come in place for compliance with objectives are the ones we call **"relative values"**, since they are dependant of time and of the life cycle of the organisation. They are "Dominant and Emergent" values:

There is always a struggle between "**dominant values"** (the ones that try to keep the system stable: ***no change***) and "**emergent values"** (the ones that try to make the system unstable: ***generate change***).

These are neither "good" nor "bad", and this is why we call them relative. These values will depend on the moment of the organisation's life cycle and of the circumstances of the environment.

Good Governance and proper Controls will have to allow for the **correct balance** between these two types of values, in relation to the specific place and time in the life cycle of the organisation and especially according to the **Objectives**. For instance, some new 21st century values are emerging from the old values of the19th and 20th centuries, as shown in the table below.

Organisations should align with them for better adaptation for the future.

If not, they might be putting themselves at risk.

Values according to Objectives	
Dominant Values (20st Century) ***Classical Organisation***	***Emergent Values (21st Century)*** ***Systemic Organisation***
Only one Objective (maximum benefit, gain political elections at short term)	Multiple and complementary objectives
Rigid Objectives	Change in Objectives when are finished or when situation changes
Work & Capital	Information & Energy
Information has to be Managed	Management relies on Information
Work in the Office	Work at Home
Maximum growth	Limits of growth. Integrated Development
Hierarchies. Chain of command long and slow	Networks. Autonomous decisions. Delegation of functions
Vertical Departments. Specialized and isolated units	Transversal Processes. Polyvalent units interdisciplinary and interrelated Organic Functions
Slow reorganisation	Fast reorganisation for specific missions or tasks. (Task forces)
Centralization. Decisions from above	Delegation. Autonomous Decisions
To know how	How to know
To make, to have, to posses	To know, to be, to create, to share
Capitalism vs. Socialism. Dogmatisms	Integral civilization. Intellectual flexibility

Values according to Objectives	
Dominant Values (20st Century) ***Classical Organisation***	***Emergent Values (21st Century)*** ***Systemic Organisation***
Static. Routines	Dynamic. Movement. Creativity
Contamination	Environmental Protection
The bigger the better (Dinosaurs did not survive)	Small and medium size (Mice survived)
Problem of jobless	Concept of work
Manual Labour	Think-tank
Paper work	Internet of Things
High Investments	Passionate groups
Organisations as Rigid Structures	Organisations as Living Systems
Confrontations. Violence to resolve conflicts	Negotiations. Intelligence to resolve conflicts
Corporation = Financial Benefits only	Corporation = Other additional Benefits. Service to Society

TABLE I. SOME EXAMPLES OF RELATIVE VALUES

IV. GRC MODELS

IV.1. - GRC Concept

We have already been talking about Governance, Risks and Compliance. **"GRC"** concept (Governance, Risk & Compliance). What is this concept?

According to the global non-profit think tank and community OCEG [20], GRC is *"a capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and acting with integrity [COMPLIANCE]."*

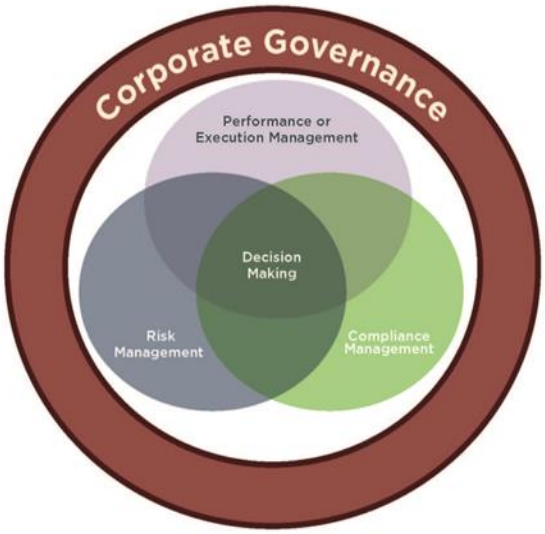


Figure 11. GRC Concept

Governance, Risk Management and Compliance are typically handled in separate parts of the enterprise, and by separate teams of people. This is not bad, since it keeps separation of duties, but there is often a lack of coordination among the various members of the GRC function. These three activities should be very well coordinated.

GRC is a model for upper management and GRC systems allow for the control and supervision by management of these three concepts and their impact on business processes and systems. Through a management dashboard, the integrated management of these concepts is both directly and continually supervised.

Governance deals with proper management and equilibrium between internal and external forces to drive the organisation toward its objectives within its limitations and constraints. Some of these limitations, as we have seen, are the following:

- "Genetic" limitations. (Internal limitations by design. Limited capabilities of internal processes or functional subsystems)
- Environmental limitations. (External factors that work against the organisation. Limited access to external resources)
- Limitations of Information (Uncertainty)

Governance should also promote change and support new implementations and awareness throughout the organisation.

Governance is a set of responsibilities and practices exercised by the board and executive management with the goal of providing **strategic direction,** ensuring that **objectives** are achieved, ascertaining that **risks** are managed appropriately and verifying that the **enterprise's resources** are used responsibly. Governance should also implement Good Practices across the organisation so its behaviour is appropriate, by means of Principles, Policies and Frameworks.

Management, which should be independent from Governance, **deals** with execution of plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO). Its main functions are the adequate *use of resources and energies* and the *assignment of resources to operations and use of units* in the field of operations to fulfil objectives.

Risk deals with assessments of threats and vulnerabilities to the system, which might come from both inside and from outside of the system itself. Governance addresses whether risks should be taken, should be accepted, should be mitigated or avoided, should be shared, or could be displaced to other systems (insurance companies or other systems in the ecosystem). Risks are neither good nor bad. They depend on the life cycle of the system and its objectives, as we have seen. Threats and vulnerabilities depend on time and space (life cycles). Risk Management is about evaluating threats and vulnerabilities to the system and designing appropriate **controls** to minimize impact in relation to the objectives of the system. Statistics, experiences and exogenous factors should be taken into account for evaluations.

Compliance deals with following the general *rules, laws, regulations and limitations imposed by the ecosystem*. Otherwise, the system might be expelled from the ecosystem because it can become a threat itself and a risk for other systems. (i.e.: frauds, criminal offences, environmental offences, threats to integral security of other systems). Some modern organisations suggest that Compliance is more about ethics and not only respecting laws and legislation, so Compliance includes also complying with internal ethics and values. Loss of the ethical component might drive the organisation to extinction. Corruption also acts like a Cancer for organisations and Society. It is believed that in Spain corruption alone costs 1% of its annual GDP (around 150.000 million of euros) [21].

Compliance not only has to do with laws and regulations but also with Culture, Ethics, and Behaviour of individuals.

IV.2. - GRC Concept Extended (Systemic Concept)

Systemic Approach to GRC in Organisations:

If we consider the organisation as a living system there is no doubt that the concepts above are interlinked, making this a dynamic and systemic model.

That is, good or bad management of internal resources and energies will have an impact on the efficiency of the internal conditions and **"health"** of the system in coping with external adversities.

The good or bad **use of operational units** in the market place (battlefield) and proper decision-making (**risk management**) will have an impact on the fulfilment of objectives or even on the survival of the system itself.

The proper understanding of how the system has to comply within the different environments (**compliance** - how much, how, when and where) is also basic for the security and safety of the system. The ecosystem has to manage equilibrium within systems, which the system must follow.

For instance, a specific system has to have a limit of growth. If it breaks those limits it might be *cancerous* to other systems and will have to be eliminated, if considered too dangerous.

In emergencies Compliance is also complementary to other situations where the specific system might need assistance for its survival from other systems in the ecosystem. A system cannot expect help from other systems if it does not comply first.

To conclude, we propose that **Security and Safety** should be addressed as an Integrated Ecosystem in order to obtain centralized processes and responses against different types of threats. This requires consistent risk management processes for an organisation's different levels. With some of the models described before we can start identifying and coping with the different Risks in an organic context of an organisation.

We can summarize the following aspects in general terms, taking into account the biological functions and the different spheres of action defined previously:

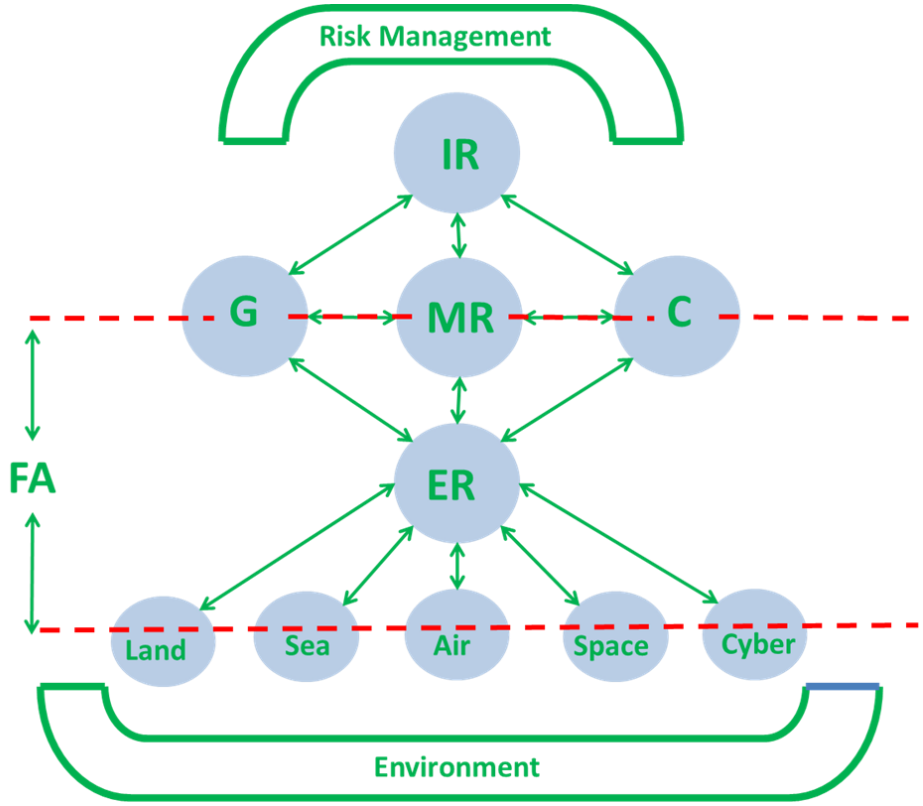


Figure 12. Extended GRC

- **G:** Governance of the System (Information and Communication, Decision taking, Compliance with Objectives, Risk Evaluation and Opportunities)
- **IR:** Internal Risk Management (Immune System, Maintenance of internal vital functions, etc.)
- **MR:** Membrane Risk Management. (Filters, Part of the Immune System. Perimetral Controls, Walls, Firewalls, etc.)
- **ER:** External Risk Management (In different spheres and within limitations in Field of Action, Threats from the different Environments, Security Systems, Residual Risks, Intelligence, etc.)
- **C:** Compliance with Environment (Laws and Regulations, Ethics, Connection and coordination with external Support systems)
- **FA:** Field of Action of the organisation in the different spheres. Extended influence of the system in the environment.

Observations:

1. - Governance, Membrane Risk Management and Compliance have internal and external implications. For instance, Internal Compliance will have to do with internal good practices, ethics and values (health of the organisation itself, certifications, etc.), and External Compliance will have to do with complying with external laws and regulations.

2. - Environment is also divided into Field of Action, where the organisation has some influence, and can take actions and risk management, and outside the Field of Action, where organisations have no influence. Black Swans from the different spheres, will normally come from outside the field of action, but when the Field of Action is analysed for possible threats it could include measures to notice / mitigate Black swans and prevent them from having catastrophic impact.

3. - Threats might have a multiplier effect if they act from the different spheres, so the following combinations has to be taken into account:

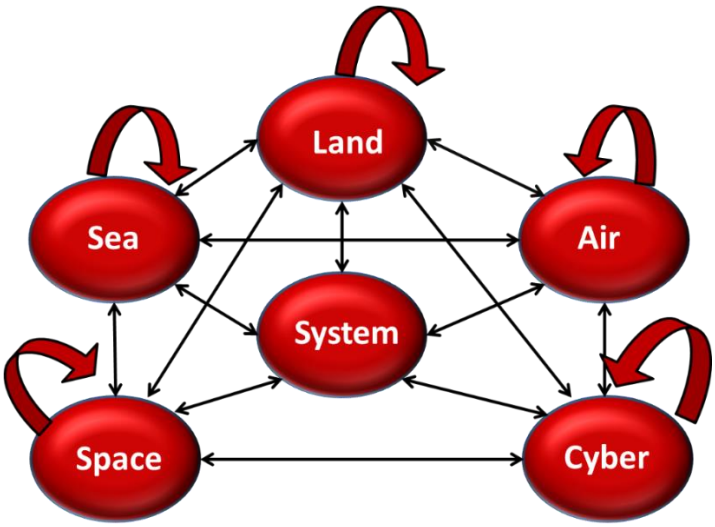


Figure 13. Threats from Spheres

Definition of the level systems you want to protect in the different spheres and across them

Threats within each sphere

Threats across spheres

Therefore we have now with this definition of Extended GRC, the most important concepts of **risks, controls and compliance**, which are basic for survival of the organisations, as living systems.

This is why we have designed the functions of Governance and Risk Management & Compliance as vital functions in the Organisation Chart.

We now know where to place them and where do they come from. This will be developed with further detail later on and in a proposed Taxonomy for Risks and Controls, as a methodology in a separate paper.

IV.3. - Maturity Model

Exposure to risks depends very much on the level of "maturity" of the system.
We propose a Maturity Model for organisations below, to identify in which place of their life cycle they are, in relation to the Risk Management System.

A generic Maturity Model can be useful to study with more details some specific issue, such as Governance, Security, Risk Management, Compliance, etc. It can be the following:

0 – Non Existent:

We cannot find any type of process which is recognizable. The organisation is not even aware that there is a problem, a risk or a threat.

1 – Initial / Ad Hoc:

Exists some evidence that the organisation is able to recognize problems and is aware of some threats and risks, but no formal assessments are made. However there are no standard procedures to deal with the problem and Solutions are ad-hoc, and tend to be applied individually in a case by case basis. Management focus is disorganized.

2 – Repeatable but intuitive:

Procedures have been developed in such a way that similar processes are followed for different persons for same issues, with no coordination. No formal channels for training and communication of standard procedures and responsibility is left in the hands of individuals. Some assessments are done in different departments but with no coordination or same methodologies. High dependence of individual knowledge and, therefore, possibility of errors.

3 – Defined:

Procedures are standard and have been documented and communicated during training. However the individual is left to follow up procedures and is not probable that deviations are detected. The same procedures are not sophisticated but are really the formalization of existent practices.

4 – Managed and Measurable:

It is possible to monitor and measure the compliance of procedures and to take pertinent actions when processes do not appear to function efficiently. Processes are continuously supervised to improve and offer a best practice. Same Methodology for Assessments. Automated tools have limited and fragmented use.

5 – Optimized:

Processes have been adjusted to the level of corresponding to best practice, based on continuous improvement and maturity models compared with other organisations (benchmarking).

Organisation managed as a living system. Integral Security and Extended GRC Concepts applied. IT is used in an integrated manner to automate the work flow and tasks, offering tools to improve quality and efficiency, making the organisation adapt itself to changes and respond quickly under attacks with proper defence mechanisms. (Cyberdefence).

IV.4. – Taxonomy for Risks and Controls

In general terms when we talk about Risks and Control, we have the following concepts and definitions:

Threats exploit Vulnerabilities creating Incidents / Events affecting the Assets of the Organization producing Business Impacts.

Practices and activities are designed to treat related risk (avoid, reduce/mitigate/control, share/transfer). Once we have done this, the organisation can decide the acceptable risk- risk appetite (residual risk).

We have already mentioned that each process or subsystem in an organisation has certain **associated risks**, which need to be managed, evaluated and controlled, to assure that the process is secure within acceptable limits for the process itself, for the organisation and for other external stakeholders.

These Risks will have different impact depending of the specific situation of the life cycle of the process itself and of the life cycle of its resources.

For instance adolescents are most prone to injuries and accidents because of exposure to risks and search for strong emotions. Some adolescents go after situations of risk deliberately searching for higher doses of Adrenalin.

There are currently many organisations and individuals that like to practice "high risk" sports, putting other persons and organisations in danger. We have seen examples in the mountain climbing sector and in the financial sector.

Older people are more prone of having risks due to deterioration, falls, lack of exercise, etc.

Some processes or activities might be **critical for the system** (business) and if they are at risk at a specific time, they can be very harmful and put at risk the rest of the system.

Each process should also have **adequate controls** to mitigate its possible risks in a specific time and place. This is where the concept of effectiveness of controls come into place. If a control does not exist or is inefficient, the organism is itself at risk. If, at the other hand there are excessive controls, is costing too much and the system might not be flexible enough to comply with its objectives.

"Risks measure the distance that separates opportunities from success"

"No Risk, No Glory"

As in all other Living Systems, internal and external agents can have a positive or negative impact in the "health" of the organisation, and need to be identified and managed. We should also consider internal agents that might be "dormant" and can be activated (for good or bad) by changes that might occur externally or internally.
Exposure to Risk depends also of the "maturity" of the system, as we have seen.

Risks by growth should also be taken into account. **Uncontrolled growth** results in a "cancer" for the organisation itself or for the ecosystem. Why do we traditionally insist on 20% annual growth in sales, productivity, products, etc.? Each system has to have a limit of growth imposed by its genetics or by the environment.
Living systems function this way; organisations do not.

This fact frequently leads to lack of ethics by trying to cheat on numbers, corruptions, short-cuts, etc., to comply with unsustainable growth.

We are now in a position to upgrade these typologies of Threats, Risks and Controls with the concepts above and especially with the biological functions and elements of the organisation, as a living system, and according to the organisation's strategy to comply with objectives. Risks that affect an organisation are of many kinds and often depend on the nature of activity or business, although some can be considered generic.

Therefore **Threats, Risks and Controls** should then be identified, classified and managed with different variables and perspectives in mind:

The first classification or distinction we can make for Threats, Risks and Controls, is to focus on which **part of the system, function or area** can be impacted, and is affected. That is, **where** the impact takes place in the organisation, and to which extent:

- **Internal – Inside the Organisation** (Threats, Risks and Controls internal to the Organisation). Impact at specific internal functions affected: Structures, Governance, Resource Management, and Internal Processes. **Controls:** Resilience to internal attacks. Awareness regarding internal behaviours (Health, Habits, etc.). Attitudes. Best Practices. Training. Audits and Certifications (¿is the system functioning well?). **Examples:** Genetic limitations and possibilities of actions; Life cycles (structures and functions becoming old and obsolete). Changes of attitudes of the persons involved in the organisation. Ethical, unethical employees.

  A factor to take into account when assessing the likely impact from the event is to consider which **time of the life cycle** the organisations or processes the incident takes place. (Maturity of the organisation).

- **Membrane – Interaction of the system with the environment - Interfaces (**Threats, Risks and Controls in the Physical Perimeter**).** Impact at the Interfaces between internal and external environment. **Controls:** Resilience at the interfaces. Adequate filters of inputs. **Examples:** Security controls at entrance of organisations. Firewalls.

- **External or Environmental– Outside the Organisation.** (Threats, Risks and Controls coming from the Field of Action). Impact at specific external functions affected: Supply Chain, Operations, and Field of Influence. **Controls:** Resilience to external attacks. Awareness regarding external behaviours and threats from outside. Best Practices. Training. **Examples:** Threats from Nature or natural catastrophes. Antisocial groups. Disruptions in Supply Chain, Black Swans.

Within the outside external or environmental group above, we can make a further distinction by taking into account the **sources of threats**.

The second classification to be made for Threats, Risks and Controls, is to focus on **where the threats might be coming from**.

That is:

Political (favour / disfavour)

Legal and Regulatory. Changes of laws

Economic changes. Difficulty to access to loans, financial restrictions.

Social and Cultural changes. Changes in demand of Products and Services

Technological changes. Changes in competition and markets.

Organizational changes. Local and International. Mergers and acquisitions.

We should also take into account which are the **spheres** or risk factors that are causing the incident (land, sea, air, space, cyber). For instance an organisation might be affected by an earthquake (land), by a toxic cloud (air), or even by solar explosions (space) which are said to provoke disruptions in communications if they are too big. This way we can identify which of the various security departments should be mostly involved in assessing risks and deciding controls.
These classifications are important, because of the treatment to be applied. Normally with external risks the organisation can only defend itself. Internal risks can be managed.

The third classification has to do with **intentionality**. Some research organisations like the ISF [22] have already defined a threat profiling depending on the type:

- Intentional (or Adversarial). When there is value generated for the attacker. Directed attack. Hacking group. Competitors. Organised crime.
- Accidental, Fortuity / Accidents, Incidents. Not intentional.

The fourth classification has to do with the different levels the system has to deal with. The context of Risk and Threats also have to be considered and managed at different levels since all levels are consistently becoming more interconnected and globalized:

- World Level
- Country / State Level / Society Level
- Industrial Sector Level / Specific Industry Level
- Organization Level
- Individual Personal Level (living cell of the organisation, and last – or first - line of defence)

An awareness plan should be implemented so that all members of the organisation understand and recognize that each person is responsible for its security and that of the organisation.

So with these variables and classifications in mind we could apply them in accordance with the different subsystems of the living system, having the following combinations for a general framework for identification and evaluation of risks and controls:

- **Structures** (Risks and Controls to Assets, Organisational Structures, etc.)
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Governance** (Risks and Controls to Objectives, Evaluate, Make Decisions, Supervise)
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Nervous System** (Risks and Controls to Command, Control, and Communications, Intelligence, C3I)
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Resource and Waste Management** (Risks and Controls to Basic Internal Life Support Systems, Life Cycle of Resources).
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Membrane**. (Risks and Controls to Interfaces between internal and external environment).
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?

- **Processes**
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Field of Influence**. (Risks and Controls to Ecosystem. Links to external life support systems, when internal resilience is broken).
    - Part of the system affected (External)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Operations.** (Objectives)
    - Part of the system affected (External)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Immune System**. (Risks and Controls to Basic External Defence and Attack systems)
    - Part of the system affected (Internal)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?
- **Supply Chain** (Risks and Controls to Transport and Distribution systems)
    - Part of the system affected (Internal / External)
    - Where is it coming from? Source of Threat. Spheres
    - Intentionality (Intentional, Accidental, etc.)
    - Level of threat and risk management. Can the system cope with them alone?

If the impact of an incident exceeds the capacity of resilience of the system, depending of the level of the catastrophe the system has to count with external help for survival, such as National Authorities, Emergency Services, etc.

IV.5. – Taxonomy of Responses

Furthermore, under Threats and Risks the following aspects for responses should be taken into account:

- **Prevention**: Training, Awareness, Good Practices, Audits, Monitorization of Environment (Intelligence). Some processes as Quality Management can act as a preventive tool, such as the firm DNV-GL [23], which motto is the following: "To safeguard life, property, and the environment" – Make a Safe and sustainable future.
- **Detection**: Deployment of detection mechanisms such as early alerts, Intelligence, etc.
    - Pre-pare (detection) – (Intelligence procedures, sensors, Metrics (measures of variables, KPI, etc.).
- **Recovery**:
    - Re-pare – (¡They are already inside! We have to take them out! Maintenance and Damage Repair, etc.)
    - Internal: Recovery, Resilience (within certain limits), Minimization of Impact. Business Continuity.
    - External: Support from other local, national or international protection Systems. Threat neutralization, etc.
- **Response / Correction**: Attacks to the attacker, Military Operations? Legal, Judicial, Political and Diplomatic responses, Incident response management, etc.
    - Post-pare (response) – (Preparation and Responses for Emergencies, Deep Defence, and Counterattack) – Can generate a *"Conflict of High Intensity"* (called War, before). War protocols.
    - Crisis Cabinets. Responses to incidents and conflicts in real-time.
    - Level of response and readiness under threats and attacks, such as emergency levels under terrorist attacks or the different levels of readiness and Defence Conditions in the US Armed Forces: (Defcon1, Defcon2 …Defcon5).
    - When exposed to a possible peril (in a plane) the recommendation is to put the oxygen mask first to yourself in the first place, and then help others. In business terms this means that the preservation and control of basic life support systems should be first.

- **Learning**: Keep updated an Incident Data Base. Gather experience to get better and more efficient procedures in prevention and detection mechanisms Intelligence). Follow up and interchange of incident data with other organisations in the environment. Benchmarks.

V. SOFTWARE IMPLEMENTATION OF THE MODEL

V.1. - Software Specifications

We would now need a proper **Software Tool** to implement these concepts of Integral Security and GRC to be able to handle all this organic functionality of the organisation, as a living system, such as structure and functions definition, Extended GRC concepts, Incident Management, Business Continuity, etc.

Design and development of this Software to manage Integral Security can be taken by companies that already have a functional base, which can be upgraded for new functionalities, if necessary, so as not to invent the wheel and generate unnecessary costs.

Some of the general functionalities that we propose for this Software according to the description of an organisation as a living system, are the following:

- Organisational Structures. Definition of areas, assets, etc.
- Business Organic Processes (as in Living Systems)
- Governance & Strategic Risk Management.
- Operational Risk & Assurance Management
- Regulatory & Compliance Management
- Project & Quality Management
- Business Continuity Management
- Health & Safety Risk & Assurance Management
- Environmental Risk & Assurance Management. In the different spaces.
- Information Risk & Assurance Management
- Immune System Management. Incident Management. (Sensors, Filters, Response Mechanisms, follow up Actions, etc.)
- Supply Chain Risk & Assurance Management. Third Party Management

And to have following capabilities:

- Flexible reporting and graphs for management.
- Ability to model complex systems with multiple dependencies.
- Real-time reaction to changes in Threats, Vulnerabilities, Objectives etc.
- Possibility of defining taxonomies for risks and controls. Identification of risks and controls of different types and from different sources.
- Capability to include some of the existent norms and methodologies (ISOs already in place):
    - ❑ ISO 27001/2 Information Security
    - ❑ ISO 22301 Business Continuity
    - ❑ ISO 14001 Environment Management
    - ❑ BS OHSAS Health and Safety
    - ❑ ISO 9001 Quality management
    - ❑ PCI – DSS Compliance
    - ❑ NIST Cyber Security Framework
    - ❑ SCADA
    - ❑ Supply Chain
    - ❑ Etc.
- Capability to act as a nervous centre, producing alerts that are believable and acted upon quickly. Use of Dashboards.

V.2. – Examples with STREAM Tool

Among the multiple GRC solutions in the market we have chosen STREAM from Acuity [24] to implement some examples since we think it is easy to use, and is business oriented.

We have also valued the integration possibilities of treatment of risks for Good Governance, all types of Risks, and Compliance.

Source: Acuity Risk Management

Figure 14. Main Functions of STREAM

Furthermore this tool provides the possibility of integrating Metrics and Events Management, which we think is essential for simulation some of the regulatory and resilience functions that we have mentioned before.

The GRC Model proposed by STREAM, which can be adapted to organisations as Living Systems, is the following:

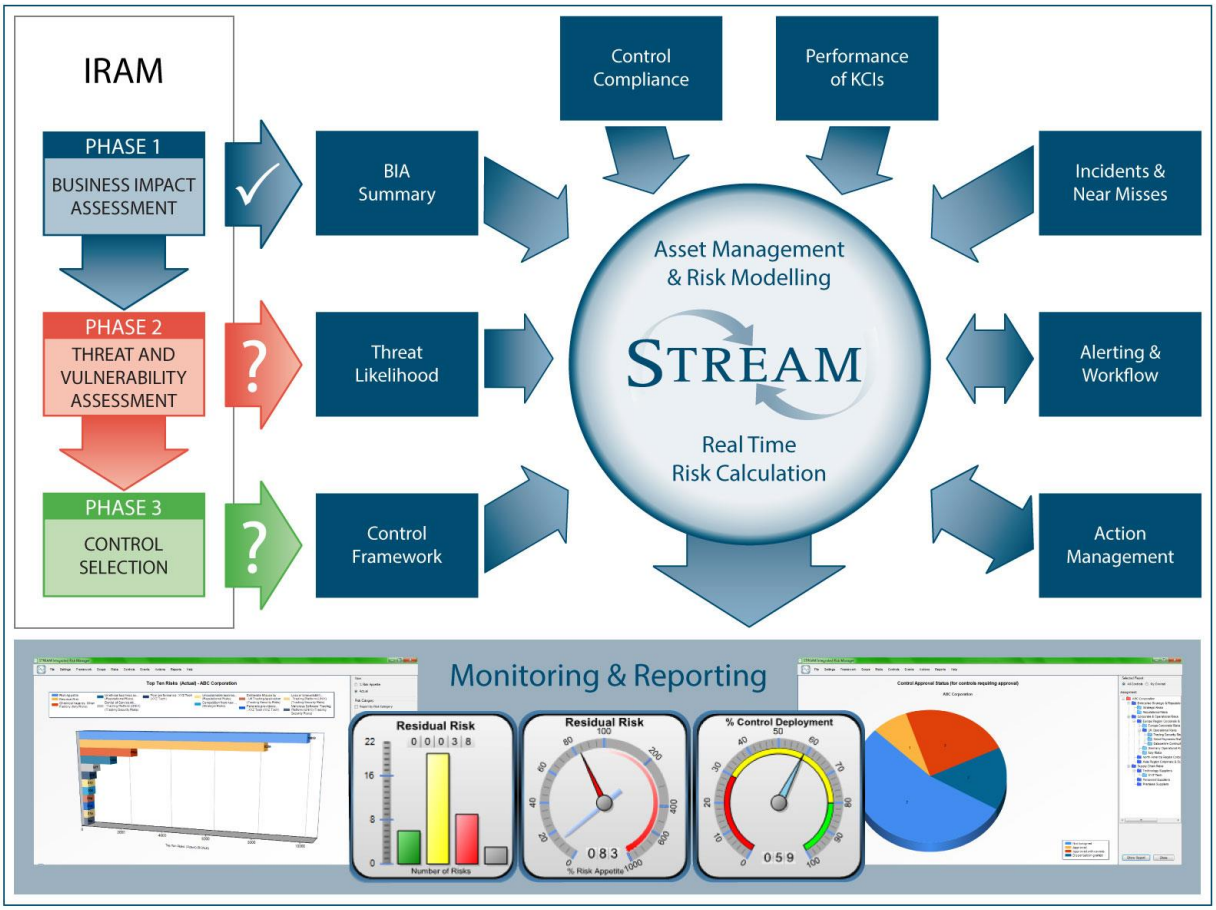


Figure 15. GRC Model of STREAM

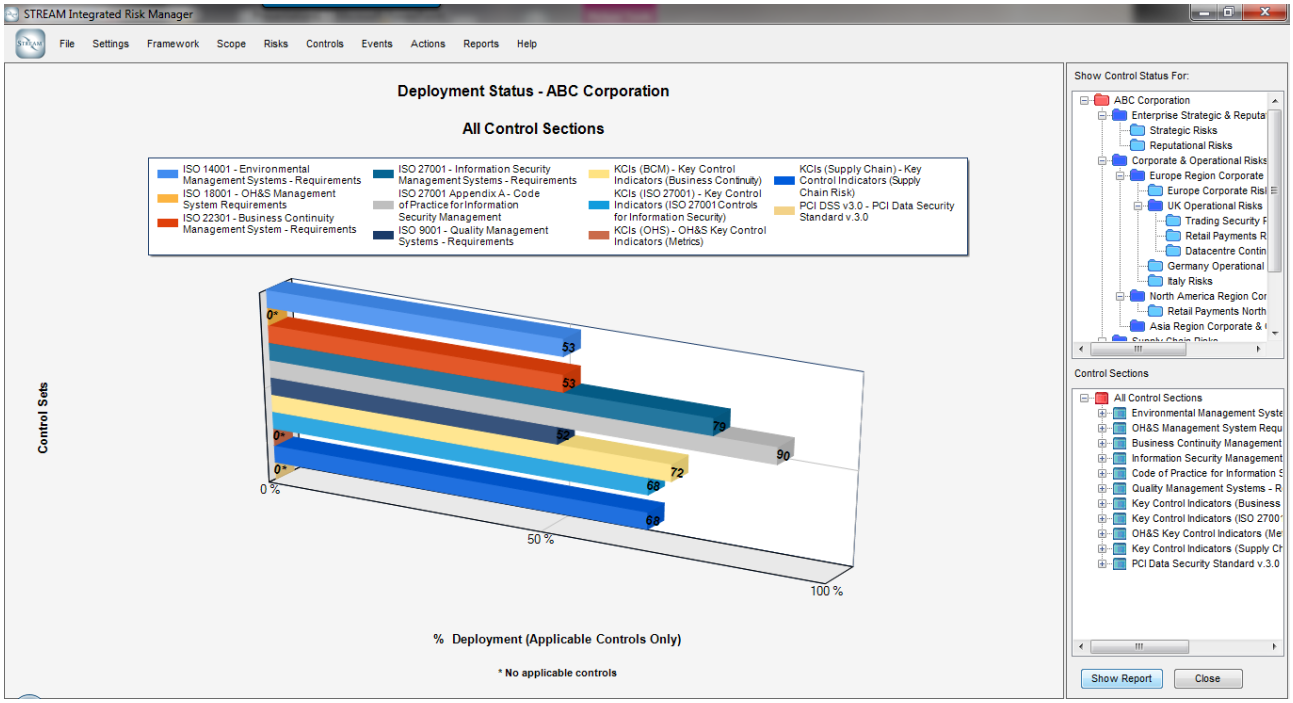


Figure 16. Control Model in context of ISOs

Reports into the overall health of the Living System and its individual components can be extracted on demand.

This can include snapshots of current status or historical views with trend analysis.

Risk-based priorities for treatment can also be identified and actioned.

VI. CONCLUSIONS FOR INTEGRAL SECURITY. NEXT STEPS

We therefore propose as a starting point for future research and developments, a holistic and **systemic approach** to security, safety, and risk & control management.

Since organisations are living systems, using a systemic approach we could adapt some of the solutions that Nature has developed over millions of years to deal with defence and attack functions that protect living systems in an integrated way, such as the immune system among others.

Organisations **should develop the concept of Integral Security as an organic and survival function of a Living System.** This will help define concepts and methodologies and will help to put them into practice with an integrated focus, based on concepts of living systems applied to organisations.

For this, we propose below a General Model for Integrated Security and a Methodology, to start with:

VI.1. – General Model for Integral Security

If Security and Safety can be considered as an Ecosystem and looked at with systemic concepts in accordance with the General Systems Theory, the various types of threats from outside and inside should be treated in a more consistent and systemic way.

Moreover, the security of organisations should be considered when taking into account the functions of a living system from the following perspectives and in the following levels:

General perspective: We propose the following starting points:

Physical Security + Logical Security = **Corporate Security** **(Security of Infrastructures, Processes, People, Property, etc.)**

Corporate Security + **Personnel awareness** = **Integral Security.**

Integral Security + **Immune Subsystem** (Threat Assessment and Risk Management) = **Defence and Attack Ecosystem.**

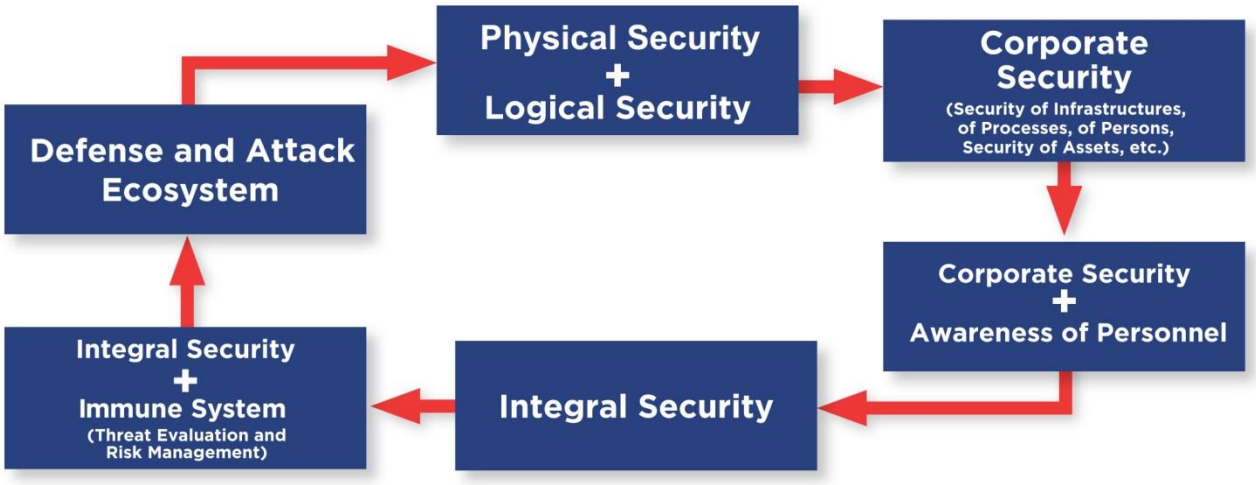


Figure 17. Integral Security

VI.2. – Proposed Methodology

The new paradigms and existent complexity cannot be managed and solved with old and obsolete concepts and methodologies. We can get help from General Systems Theory to help solve complex problems.

Establishment of an Integral Security Policy as a systemic concept should take into account physical, logical and other aspects with regards to internal and external threats, at different levels. Policy should also take into account the three brain levels for the management of responses. (*Reptile, Limbic and Neocortex*).

More orientation to the business. We have to know how to "sell" security to the higher levels of the organisation. Security should not be seen as a problem to the organisation, but as an added value. This is why sometimes we don't have enough support from Top Management.

To develop these new concepts and a practical model of Integral Security for Organisations, based on the organic functions of a living system, the following **suggestions and Methodology** for Best Practices should be considered regarding **Objectives**, **Research Activities** or **Actions** for an implementation project of Integral Security:

- Definition of the living organic subsystems of the organisation according to the vital functions of a Living System. **Internal Conditions** and system management for survival, as an isolated system. For an organisation, four main resources must be considered: Personnel, Material, Financial, and Information. **Evaluation of Internal Threats, Risks, and Controls**. Capability of resilience by design. “Health checks”. Internal Audits. Life cycles and maintenance for each vital resource should be contemplated. Take into account roadmap of the organisation to comply with objectives, since Risks change overtime.
- Definition of the upper and lower limits of each function or subsystem, to define key indicators metrics, and its **resilience**. Resilience is the capacity of a system or subsystem to recover from an impact, stress or harm, and be able to go to the initial state and normal functional operation, as soon as possible. This will also help decide when some subsystem, or the system itself, requires outside help or external support from **security or emergency services**, such as public or private health services, police, firemen, etc. Monitorisation and measurement of key indicators for variables that might be out of range. Preparation and responses to emergencies.
- Definition of the flexibility, conditions and degrees of open-close of the **membrane** of the organisation. **Evaluation of Threats, Risks and Controls at the interfaces**. Links and interchange procedures with systems of lower levels (internal subsystems) and of higher levels (supra-systems of the environment). The solution really comes down to have a good definition and delimitation of the organisation, of its field of influence, and of the interfaces, we have to protect.

- Definition of the Absolute and Relative (Dominant and Emergent) Values at a certain point in time, depending on the life cycle of the organisation. Implies Change Management. This exercise is essential to determine what type of risks and controls should be managed and when to modify assessments. This also implies the kind of training and awareness needed at a certain point in time. Identification of Threats and Risks to the different values.
- Definition of the different Theatres of Operations. **External Conditions** and Management of the Environment (Ecosystem) to comply with Objectives, in the five spaces mentioned (Land, Sea, Air, Space and Cyberspace). **Assessment of External Threats, Risks and Controls** in each of the operational theatres. We could also add an additional one such as **mental space** (personal behaviour and cultural)
- Definition of the decision-taking mechanisms regarding Internal and External Conditions to **Comply with Objectives**. Action Plans, Management of uncertainty and unknowns. **Assessment of future Threats, Risks and Controls**. Prevention functions (Intelligence, Sensors, Measurement of variables), Detection, Inspections, and Responses.
- Implementation of an extended GRC (Analysis and Risk Management System), acting as the Immune System of the Organisation. This should take into account the different threats, risks and controls within each of the organic subsystems described for a living system. The organisation should consider Internal, External and Future Risks and Controls at all levels and spaces. Compliance should take into account aspects and ethical behaviours.

- Assessment and Management of Third-Party Security since the other external organisations can possibly ‘contaminate’ or ‘infect’ our system. (Supply Chain Security). Define strategies for Cloud and in Supply Networks. Securization of consumer devices. The same risk can affect in different ways the assets of each element of the logistic system.
- Associations and interactions with other organisms. External links with the Ecosystem (i.e.: with different security and law enforcement organisations for Compliance and for help in case attacks go beyond the system’s own capabilities for defence). Dependencies from other organisations or external infrastructures, when resilience of the isolated organisation is broken. Sharing of resources with competitors. Collaborative environments. Interchange of Information when incidents happen.
- Understanding that people must be involved and sufficiently trained and aware. Without taking into account the human factor, other measures are useless. Development of **Awareness and Training Plans** as a major factor for Integral Security.
- Development of flexible procedures and contingency plans in order to make organisations more **resilient**. Resilience can be strengthen by means of exercises. Measurement of capabilities for survival even when some systems are not functioning. Occasionally difficult circumstances or traumas enable organisations (and people) to develop resources that have previously been either latent or unknown. Concepts of plans and procedures for Business Continuity, Drills, Simulations, War games, etc. Establishment of Cabinets for Crisis Management to prepare and respond under emergencies.

- Understanding that we are dealing with an international issue. We are all at the forefront: public organisations, private organisations, individuals, society and so forth, and that we must act together.

  Big corporations and organisations operate world-wide. Threats might be the same but risks and controls might be different.

  Relations and cooperation with international organisations in the field of Security can be useful.

  Participation and collaboration in forums, international organisations and international projects on Integral Security is essential to avoid *reinventing the wheel* and to know what is happening "out there".

VII. ACKNOWLEDGMENTS

We would like to give special thanks to the following persons that have helped reviewing the text and concepts:

- Albritton, Anne – Educational Consultant, Facilitator, and Executive Coach
- Córdoba, Vicente – Quality Systems, Process and Risk Management expert
- de Luna, Francisco – Sales Manager Computer Aided Logistics
- de Miguel, María - High School professor. Degree in Biology and Immunology expert.
- Libove, Jay – ISF Security and Compliance Consultant, CISSP, CIPP/US, CIPT, CISM
- Marvell, Simon – Partner, Acuity Risk Management
- Ortega, Manuel – Business Development Computer Aided Logistics
- Parra Luna, Francisco - Catedrático Emérito de Sociología, UCM
- Puebla, Inmaculada - PhD professor at the University Degree and MBA. Expert in Information Technology, Entrepreneurship, Marketing and Sales, and its interface with the Systems Management at board level.
- Wells, Ian – Director HighQuest Solutions

VIII. REFERENCES AND LINKS

References:

[1] Information Security Forum: Threat Horizon 2015 – PLEST Methodology

[2] World Economic Forum: Global Risks 2016 11th Edition

[3] American Blackout: National Power failure because of cyberattack – September 2013

[4] Angel Sanchez Sanchez - Complex Systems: The science of the XXI Century - IMDEA Matemáticas - Universidad Carlos III – 2004

[5] Ludvig von Bertalanffy, 1950, *An Outline of General System Theory*, British Journal for the Philosophy of Science 1, p. 114-129. *General System Theory*, George Braziller, Nueva York, 1968.

[6] Norbert Weiner – Cybernetics 1948 – Wiley, New York

[7] John D. Sterman – MIT Business Dynamics: Systems Thinking and Modeling for a Complex world.– McGraw-Hill 2000

[8] Murray Gell-Mann, "The Quark and the Jaguar" Tusquets Editores, 1995

[9] Maria Blasco: Interview published in "El País" by José María Izquierdo - April 12, 2015

[10] Peter Titleman – Editor: Triangles. Bowen Family Systems Theory Perspectives. – 2008, Haworth Press, Taylor & Francis Group, 270 Madison Avenue. New York, NY 10016

[11] Codynamics: Understanding The Characteristics of Living Systems

[12] Living Systems: https://en.wikipedia.org/wiki/List_of_systems_of_the_human_body

[13] "Matemáticas en la ley de la selva" Article published by Miguel Ángel Criado in "El País" – September 4, 2015

[14] ISACA – CobIT 5 (Framework for governance and management of enterprise IT)

[15] Simon Marvell - Real-time cyber security risk management system – September 2015

[16] Enterprise Immune System - Darktrace (Immune System Technology for cyber security)

[17] IBM Security Summit 2016 – Madrid, September 21st 2016

[18] IBM BusinessConnect 2016 – Madrid, November 11th 2016

[19] Francisco Parra Luna – "An Axiological Systems Theory: Some Basic Hypotheses" – John Wiley & Sons - 2001

[20] OCEG – Open Compliance and Ethics Group

[21] "Acabar con la corrupción: un imperativo económico, no solo ético" Article published by Luis Garicano in "El Pais" – April 19, 2015

[22] Threat Profiling in IRAM2 – ISF Project 2014

[23] DNV-GL: Audit and certification enterprise from Oslo

[24] STREAM: Integrated Governance, Risk Management and Compliance Software and GRC Solutions from Acuity Risk Management.

Other references:

Ackoff and Emery, (1972), *On Purposeful Systems,* Atherton.

Aracil, J. (1978), *Introducción a la dinámica de sistemas,* Alianza Editorial, Madrid.

Beer, S. (1985). *Diagnosing the System for Organisations,* Wiley, New York.

Beer, Stafford *"The Brain of the Firm"* John Wiley, N.Y. 1970

Bunge, M.: *"The concept of a social system",* págs. 210-221 en *International Systems Science Handbook*, Systemic Publications, Madrid, 1993.

Checkland, P. (1981) *Systems Thinking, Systems Practice*. Chichester, England: John Wiley and Sons

Checkland, P. (1986). *Systems Thinking, Systems Practice*, Wiley.

Miller, J. G., (1978), *Living Systems*, McGraw Hill, New York.

Maturana, H. y Varela, F.J.: *Autopoiesis and Cognition*, Prólogo de Sir Stafford Beer, D. Reidel Publishing Co., Dordrecht, Holand, 1980.

J.R. Reguiero Gonzalez, C. Lopez Larrea, S. Gonzalez Rodriguez, E. Martinez Naves: *Inmunología Biologia y patología del sistema inmunitario,* 4ª Edición Revisada (2010) Editorial Medica Panamericana

Rodriguez Delgado, Rafael, *Del Universo al Ser Humano*, McGraw-Hill, 1997

Uexküll, J. von: (2ª ed., 1951), *Ideas para una concepción biológica del mundo*, Biblioteca de ideas del siglo XX, Espasa-Calpe Argentina.

Links:

http://channel.nationalgeographic.com/american-blackout/

http://reports.weforum.org/global-risks-2015/

http://codynamics.net/

https://en.wikipedia.org/wiki/Human_body

http://www.the-human-body.net/systems.html

http://www.organsofthebody.com/

https://www.isaca.org

www.darktrace.com

www.oceg.org

https://www.dnvgl.com/

http://www.acuityrm.com/

http://www.mind-development.eu/systems.html

http://lewisorgtheory.pbworks.com/w/page/16682143/Organisms

http://legoviews.com/2013/04/26/organisations-as-organisms-consciousness-and-wellness/

http://www.ribbonfarm.com/2010/07/13/the-eight-metaphors-of-organization/

http://adaptiveworkforce.blogspot.com.es/2008/01/organizations-are-living-organisms.html

https://www.biodynamics.com/forums/organizations-living-organisms

http://www.cleanlanguage.co.uk/articles/articles/19/1/Metaphors-of-Organisation-part-1/Page1.html

http://www-05.ibm.com/es/securitysummit2016/