

# Data Management & Organizational Resilience

**Managing the data waterfall to create a common operating picture and achieve organizational resilience, and how the use of commercial-off-the-shelf software can facilitate the rapid attainment of organizational resilience**

## TABLE OF CONTENTS

Introduction .....	2
Project Overview .....	3
The Business Case for Organizational Resilience Management and the Chief Security Officer .....	4
Path Ahead .....	5
Commitment .....	7
Definition and Analysis .....	9
Planning .....	12
Implementation and Operation .....	14
The Result .....	15
The Chief Security Officer's Relationship to Organizational Resilience Management .....	16
The Cost of Not Being Resilient .....	19
How Do You Make Data Intelligent? .....	20
Solutions For The Next Generation Security Operation .....	22
Getting Started and Moving Forward .....	24
OR <sup>3</sup> M Overview .....	25

OR<sup>3</sup>M™

12011 NE 1<sup>st</sup> St.  
Suite 308  
Bellevue, WA  
98008

[www.OR3M.com](http://www.OR3M.com)  
[info@OR3M.com](mailto:info@OR3M.com)

OR<sup>3</sup>M's mission is to create an information management platform that will meet the needs of our clients including small to medium sized businesses as well as large-scale corporate environments.

## INTRODUCTION

The security industry has experienced significant growth in the past ten years. In our opinion this growth can be attributed to several factors including global instability, significant advances in information technology, and the efforts of professional organizations such as ASIS International, The Security Executive Council, the Security Industry Association (SIA) and numerous others, to create standards, guidelines, and best practices in the larger domain of the Security Industry.

The introduction of standards which address best practices for Chief Security Officers (CSO) and Organizational Resilience Management (ORM), have provided a capstone to our industry and provide us solid processes, allowing practitioners to make the business case and demonstrate value for the security function while identifying and treating enterprise risk.

One of the critical elements of making the business case and achieving organizational resilience is the ability to capture, organize, manage & communicate, and collate information. The old adage of *"You cannot manage what you cannot measure,"* holds true here.

We need information to establish a baseline for measurement and planning. Additionally, later on, we need information so we can measure our findings against that baseline.

This white paper intends to make the case for managing the data waterfall by creating a common operating picture and showing its correlation to Organizational Resilience Management and Enterprise Risk Management.

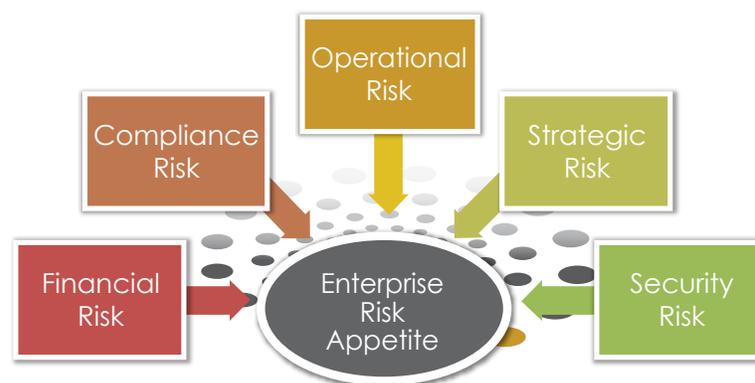


Figure 1: Enterprise Risk Appetite

## PROJECT OVERVIEW

As security leaders mature and advance our knowledge and practices into the realm of Organizational Resilience Management (ORM), they quickly come to the conclusion that in order to implement and measure a successful ORM program, you need information. Quality information is what enables good decision making. Many enterprises have the information but it is largely unusable. In many cases, it is in bits and pieces, in disparate reports, files, evaluations, and assessments. Additionally, we have a new data stream with information being provided through the integration of information technology based physical security systems. The data produced by integrated physical security systems, is significantly capturing this information and presenting it in a usable format, providing analytics and value far beyond the device itself.

Even the U.S. Department of Homeland Security (DHS) is struggling with this issue. In 2001, DHS mandated risk, threat, and vulnerability assessments to be conducted on all water utilities that served a population over 150,000. The methodology which was chosen for this was **Risk Assessment Methodologies for Water Utilities**, which is the product of Sandia National Laboratories. Since 2001, engineering firms, private enterprise, federal government, and many not-for-profit organizations have been creating and marketing their own risk assessment tools, each creating different information and a different repository.

In addition, we have added eighteen additional sectors which require baseline and annual or biannual assessments based on criticality. Now, DHS has thousands of assessments all using different methodologies. Making sense out of the data is difficult. In other words, the data has been collected, but in its current formats, is unusable for any kind of decision making, trend analysis, or other analytical function.

These same issues are also impacting the private sector, especially large enterprise organizations whose operations are influenced by numerous interdependencies and global issues.

The need for comprehensive, detailed, catalogued, and prioritized information is a necessity if Organizational Resilience Management and the Chief Security Officer function are going to be successful.

This paper will attempt to detail these processes and present for consideration, a collaborative tool using commercial-off-the-shelf (COTS) software. By creating a modular COTS architecture, appropriate consoles can be added, providing leaders and decision makers with immediate, factual, and comprehensive data. This data can be used by the CSO and other members of the "C" Suite to achieve enterprise resiliency and thereby minimize enterprise risk.

## Background

Back in the 1950's, W. Edwards Deming provided us a number of principles of management which hold true today. These principles are at the core of Organizational Resilience Management and serve as the foundation for the Chief Security Officer function:

- Continuous improvement requires the collection of good data. Without accurate data, how can anyone tell if things are getting better or worse?

- Create constancy of purpose towards improvement of product and service, with the aim to become competitive, stay in business, and to provide jobs.
- Adopt the new philosophy. We are in a new economic age. Western management must awaken to the challenge, must learn their responsibilities, and take on leadership for change.
- Break down barriers between departments. People in research, design, sales, and production must work as a team, to foresee problems of production that may be encountered with the product or service.
- Put everybody in the company to work to accomplish the transformation. The transformation is everybody's job.
- Use of visible figures only for management, with little or no consideration of figures that are unknown or unknowable
- Make visible the excessive costs of liability (Management, 1998)
- These principles hold true in 2014. The first of these is most important to this paper: "Continuous improvement requires that good data be collected. Without accurate data, how can anyone tell if things are getting better or worse?"

## THE BUSINESS CASE FOR ORGANIZATIONAL RESILIENCE MANAGEMENT AND THE CHIEF SECURITY OFFICER

We have been involved in several case studies which attribute preparedness and resilience to the successful survival of an enterprise. All organizations and especially large enterprise organizations are subject to the same man-made (crime and terrorism), natural (earthquake and flood), or technical (chemical release) disasters. All you have to do is watch the evening news to understand many organizations have suffered great losses as a result of terrorism, military action, natural disaster, or technological disaster. The rebel actions in Libya and the recent Fukushima Disaster come to mind as events that had wide reaching impacts on the global economy and supply chain.

Worldwide organizations who do not prepare for these types of catastrophic events, will suffer significant loss of life, property, and resources, or may cease to exist altogether.

There is a significant benefit to embracing the concept of Organizational Resilience Management and creating what is generally referred to as an Organization Resilience Plan. Organizational Resilience Management is a standard which was jointly created by ASIS International ([www.asisonline.org](http://www.asisonline.org)) and the American National Standards Institute (ANSI). ([www.ansi.org](http://www.ansi.org))

The title of the standard is **ANSI/ASIS SPC.1-2009** "*Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use,*" ([webstore.ansi.org/RecordDetail.aspx?sku=ASIS+SPC.1-2009](http://webstore.ansi.org/RecordDetail.aspx?sku=ASIS+SPC.1-2009)). This standard has been selected for inclusion in the **Voluntary Private Sector**

**Preparedness Accreditation and Certification Program (PS-Prep)**, a voluntary program designed to improve private sector resilience and preparedness in an all hazards environment, (International, 2009) . This standard was closely followed by the **ASIS Maturity Model for the Phased Implementation of the Organizational Resilience Management System (2012)** - [www.abdi-secure-ecommerce.com/asis/ps-1127-37-1993.aspx](http://www.abdi-secure-ecommerce.com/asis/ps-1127-37-1993.aspx). (ASIS International, 2012)

Organizational Resilience Management (ORM) allows an organization to anticipate events which may impact its operations. Specifically, the process emphasizes resilience, which is the adaptive capacity of an organization in a complex and changing environment including the protection of its critical assets.

Applying an organizational resilience standard allows the organization to more readily prepare for, respond to, and mitigate all manner of disruptive events, which if unmanaged could escalate into an emergency, crisis, or disaster.

*Generally a plan of this type enables an organization to:*

- Develop a prevention, preparedness, response, continuity, and recovery policy
- Establish objectives, procedures, and processes to achieve policy commitments
- Assure competency, awareness, and training
- Set metrics to measure performance and demonstrate success
- Take action needed to improve performance
- Demonstrate conformity of the system to established standards
- Establish and apply a process for continual improvement

This contribution intends to define this process for the reader and serve as a roadmap for process improvement in a difficult world. The end result is a resilient and adaptive organization capable of executing its worldwide mission during all contingencies.

## PATH AHEAD

*Here are some basics the plan should cover:*

### Leadership

Clearly defined roles, easy access to initiative leaders, and measurable top-management commitment are required to institute a project like this. Without leadership and commitment, the process is doomed to fail from the start.

## Reporting & Communication

Resilient organizations maintain accessible and user-friendly communication practices that encourage participation across the organization and reporting tools that provide insights into the nature of incidents, threats, and vulnerabilities. Furthermore, effective communication accounts for and spans across special circumstances (i.e. Crisis Communication & Emergency Notification) and multiple 'publics' (employees, vendors, customers, community, etc.),

## Assessment & Review

From Business Impact Assessments (BIA) to risk, threat, and vulnerability assessments and security surveys, successful programs identify and address real-life risks and vulnerabilities, while constantly adjusting to changing conditions.

## Standards, Policies & Procedures

Dusty three-ring binders are no longer an acceptable legal or ethical defense. In the world, there is a clear duty (and opportunity) to inform, educate, and train all of your employees.

## Training & Education

Practice, practice, practice! Again, any organization today has ample opportunity to engage, educate, and test of all its members with zero-to-low cost interactive training content ranging from new employee orientation to hazardous materials handling procedures. As one crisis after the next continues to prove – those who practice, prevail.

## Specialized Resources

Each vertical initiative may need specialized technology and teams - from specialized web sites capable of acting as a management tool, to cross-platform emergency notification applications, and a capable well trained crisis management team. The extent by which these applications are effectively integrated, understood, and utilized by all involved in the initiative life-cycle, is a key measure of their value when the emergency occurs. It is a known fact that emergencies by their nature are expensive. The more we can mitigate the impact of an emergency by compressing the amount of time it takes to progress from onset to recovery, the more we can minimize the impact on the enterprise to its personnel, facilities, and financial resources.



Figure 2: A detailed standard for this process is attached at Appendix "A" Organizational Resilience ASIS SPC. 1-2009 (International, 2009) Let's consider each of the above areas and consider what each area means to the enterprise.

## COMMITMENT Management

An endeavor of this nature needs to have firm leadership from the top of the organizational structure. There should be one person with absolute decision making authority who is a member of the Enterprise Leadership Team, that is directly responsible for this process and keeps the Enterprise Leadership team informed. In many organizations, this position is known as a Chief Security Officer. This is a position on the institutional leadership team similar in stature to a Chief Executive Officer or Chief Operations Officer. For more information on the CSO position, please refer to the ASIS International Standard ASIS Chief Security Officer (CSO) An Organizational Model, 2013 Edition ASIS Commission on Standards and Guidelines. ASIS International. (ASIS International Chief Security Officer (CSO) Organizational Standard, 2013 Edition, 2013)

The ASIS Chief Security Officer (CSO) Organizational American National Standard is a model for organizations to use when developing a leadership function responsible for providing comprehensive, integrated risk strategies to help protect an organization from security threats. Designated as Chief Security Officer (CSO), this role may be viewed as a stand-alone position or one that has been incorporated within an organizations existing leadership team. The CSO Organizational Standard details the CSO reporting relationship, key responsibilities and accountabilities, core competencies, experience, education and compensation, and provides a model position description. (ASIS International Chief Security Officer (CSO) Organizational Standard, 2013 Edition, 2013)

The CSO should be a full partner in the governance infrastructure of the organization. If a comprehensive assessment of any areas of risk supports the need for a function specific security role, the assignment of high accountability better insures an integrated security strategy, with less duplication of effort and stronger fiscal management.

A core responsibility for effective program and policy development is the management of positive working relationships among stakeholder and client groups. Front-line accountability for protecting the organization should reside with the leader of each operating unit, with the appropriate organization's security function providing the risk assessment, policy, and supporting infrastructure to those leaders.

The senior security executive should be recognized as the organization's authority on security/risk related matters. Expertise across all domains is not expected, however it is paramount that the individual leverage competencies, experiences, and advanced working knowledge of contemporary security/risk management, practices, protocols and applications. An effective model is a hybrid one that takes into consideration the senior security executive's combined leadership talent, business acumen (i.e., background in business or a governance function), and subject matter expertise. Leadership of a multi-faceted security program requires generalist knowledge, including a relevant background at a senior level within a business, governance function, or some element of the security mission. These attributes and skills or a combination thereof should be given strong consideration in the selection of the senior security executive. Ultimately, the individual's resourcefulness, credentials, and credibility within the organization, and the vision to craft an integrated, multi-faceted risk mitigation strategy, depends on the individual's ability to understand, value, and articulate the varied risks and threats facing an organization in the context of organizational impact (ASIS International Chief Security Officer (CSO) Organizational Standard, 2013 Edition, 2013).

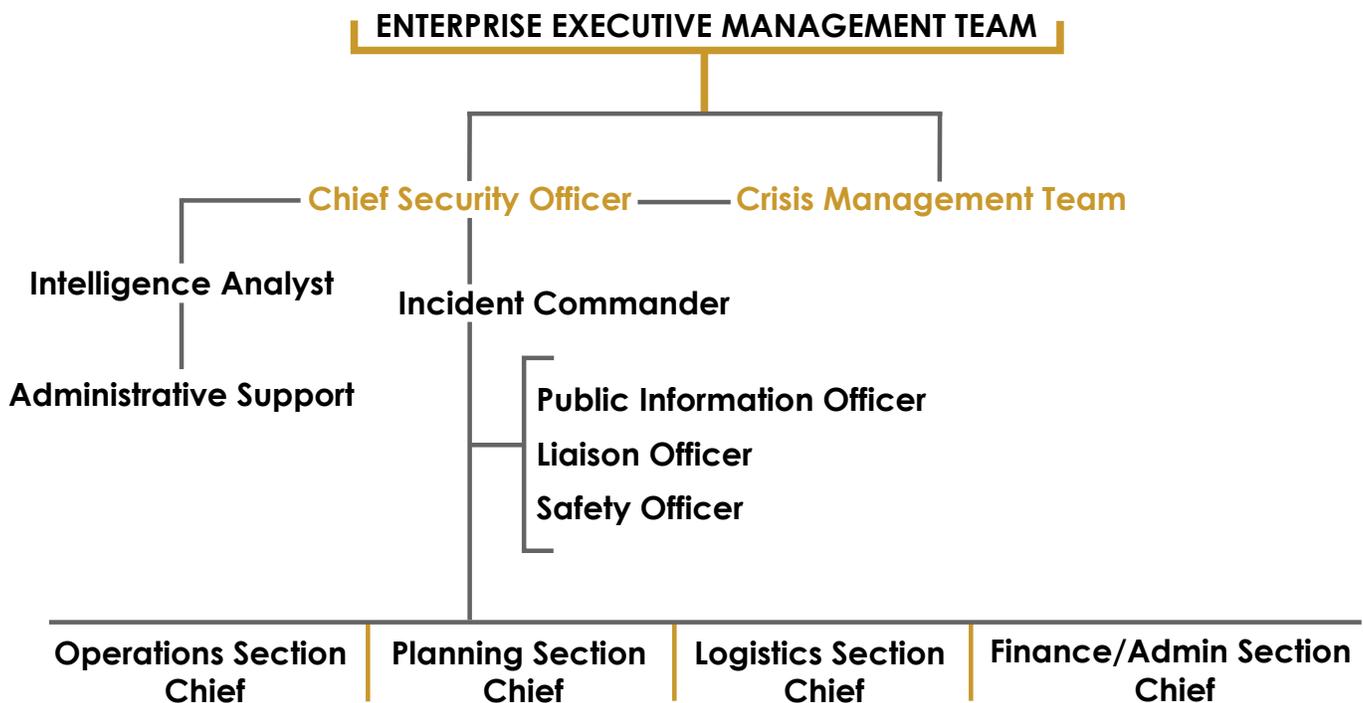
## Resources

Sufficient resources in the form of time commitment, funding, and facilities is required for successful implementation of this process.

## Leadership Roles and Responsibilities

Please see the below graphic which describes the various leadership roles and positions.

Figure 3: This diagram is Incident Command System (ICS) based and demonstrates several critical relationships. The first, is the relationship between the executive management team and chief security officer, as well as the Chief Security Officer's relationship with the Crisis Management Team and Incident Management team.



On a daily basis, the Chief Security Officer manages the security function including intelligence analysts and administrative support personnel to meet the day-to-day needs for operational planning, preparation, and training. This immediate staff changes from organization to organization and can include threat specialists, physical security specialists, investigators, trainers and others depending on the organizational security mission. During very critical situations, the Crisis Management Team would form with the Chief Security Officer who in a lead capacity, would further supervise an incident command team comprised of an operation section, planning section, logistics section, and finance & administrative section. The incident command team is structured in the same fashion as city, county, state agencies, and the federal government, who utilize incident command as outlined by the National Incident Management System and the National Response Framework.

Using the Incident Command System provides the added benefit of being eligible for Department of Homeland Security grant funding. Additionally, it allows the Enterprise team to seamlessly integrate with city, state, and federal emergency management partners. The incident command system has also been adopted by many foreign countries.

The incident management team can be scaled according to the size of the incident. Multiple responsibilities could be contained in one or two people for a small incident or expanded to numerous others in the case of a large incident. The National Incident Management System (NIMS) and the National Response Framework (NRF) documents are available online at [www.fema.gov/emergency/nims/](http://www.fema.gov/emergency/nims/) and [www.fema.gov/emergency/nrf/](http://www.fema.gov/emergency/nrf/).

Additionally FEMA provides free accredited training to any citizen of the United States online at [training.fema.gov/IS/](http://training.fema.gov/IS/)

## DEFINITION AND ANALYSIS

### Scope

In defining the scope of the project, we want to define the boundaries of the organization that will be included in the scope. This could be the whole organization or one or more of its constituent parts. While establishing the requirements for management, it also considers the organization's goals, mission (internal and external), obligations, and legal responsibilities. Furthermore, the enterprise will want to consider critical operational objectives, assets, functions, services, and products. Additionally, we want to determine risk scenarios based on both potential internal and external events that could adversely affect the critical operations and functions of the organization within the context of their potential impact.

### Objectives

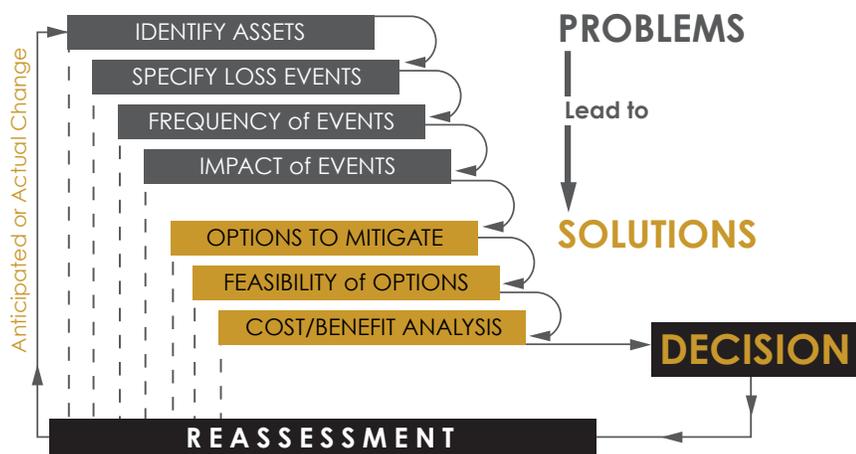
The objectives of the process are a commitment to the protection of human, environmental, and physical assets through anticipating and preparing for potential adverse events coupled with business and operational continuity.

### Risk, Threat, and Vulnerability Assessment

A comprehensive, all hazard, qualitative risk threat and vulnerability assessment should be conducted to determine potential threat scenarios, where risk is a measure of the potential damage to or loss of an asset based on the probability of an undesirable occurrence. A risk assessment is the process of analyzing threats to and vulnerabilities of a facility, determining the potential for losses, and identifying cost corrective measures and residual risk. Vulnerability is an exploitable security weakness or deficiency at a facility. A multi-dimensional assessment process measures an asset's protection against the threats it is most likely to face, while in support of the mission the asset delivers.

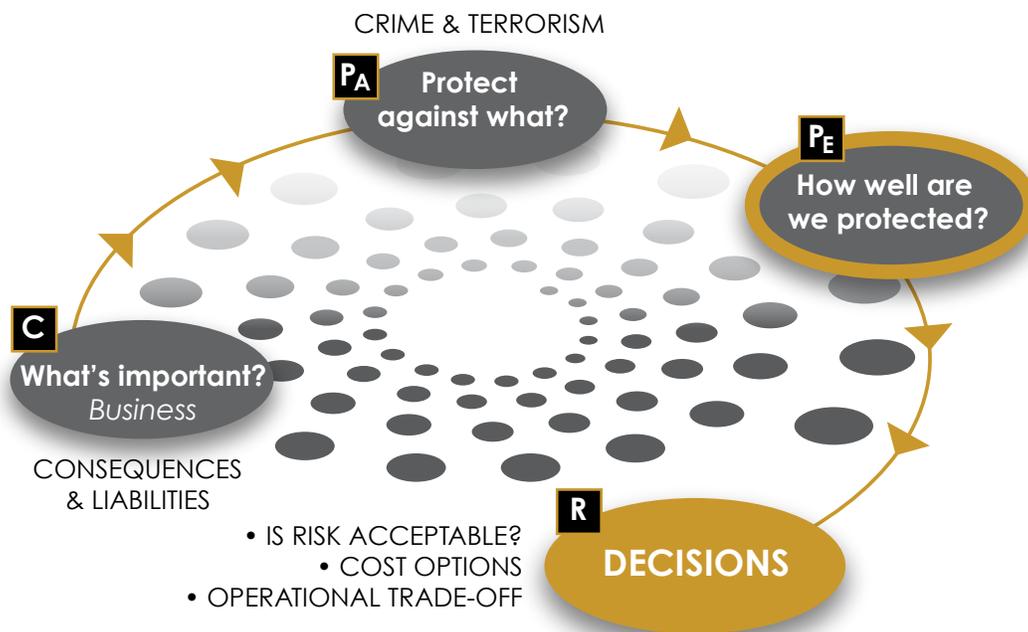
## General Risk Assessment Process

Figure 4: Garcia 2001



## Quantitative Application of a Process

Figure 5: Garcia 2001



## Business Impact Analysis

This Business Impact analysis will identify Enterprise's most crucial systems and processes and the effect an outage would have on the organization. The greater the potential impact, the more money you should spend to restore a system or process quickly. For instance, a stock trading company may decide to pay for completely redundant IT systems that would allow it to immediately start processing trades at another location. On the other hand, a manufacturing company may decide that it can wait 24 hours to resume shipping. A BIA will help companies set a restoration sequence to determine which parts of the business should be restored first.

*Here are some basics the plan should cover:*

- Develop and practice a contingency plan that includes a succession plan for your CEO.
- Train backup employees to perform emergency tasks. The employees you count on to lead in an emergency will not always be available.
- Determine offsite crisis meeting places and crisis communication plans for top executives.
- Practice crisis communication with employees, customers, and the outside world.
- Invest in an alternate means of communication in case the phone networks go down.
- Make sure that all employees, as well as executives, are involved in the exercises so that they get practice in responding to an emergency.
- Make business continuity exercises realistic enough to tap into employees' emotions so that you can see how they'll react when the situation gets stressful.
- Form partnerships with local emergency response groups: firefighters, police and EMTs, to establish a good working relationship. Let them become familiar with your sites.
- Evaluate your performance during each test, and work toward constant improvement. Continuity exercises should reveal weaknesses.
- Test your continuity plan regularly to reveal and accommodate changes. Technology, personnel, and facilities are in a constant state of flux at any company.

As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence.

## PLANNING

### What do these plans include?

All Business Continuity and Disaster Recovery plans need to encompass how employees will communicate, where they will go, and how they will keep doing their jobs. The details can vary greatly, depending on the size and scope of a company and the way it does business. For some businesses, issues such as supply chain logistics are most crucial and are the focus on the plan. For others, information technology may play a more pivotal role, and the BC/DR plan may have more of a focus on systems recovery. For example, the plan at one global manufacturing company would restore critical mainframes with vital data at a backup site within four to six days of a disruptive event, obtain a mobile PBX unit with 3,000 telephones within two days, recover the company's 1,000-plus LANs in order of business need, and set up a temporary call center for 100 agents at a nearby training facility.

But the critical point is that neither element can be ignored, and physical, IT, and human resources plans cannot be developed in isolation from each other. In this regard, BC/DR has much in common with security convergence. At its heart, BC/DR is about constant communication. Business leaders and IT leaders should work together to determine what kind of plan is necessary and which systems and business units are most crucial to the company. Together, they should decide which people are responsible for declaring a disruptive event and mitigating its effects. Most importantly, the plan should establish a process for locating and communicating with employees after such an event. In a catastrophic event (Hurricane Katrina being a relatively recent example), the plan will also need to take into account that many of those employees will have more pressing concerns than getting back to work. (Editor Eric Slater [dslater@cox.net](mailto:dslater@cox.net))

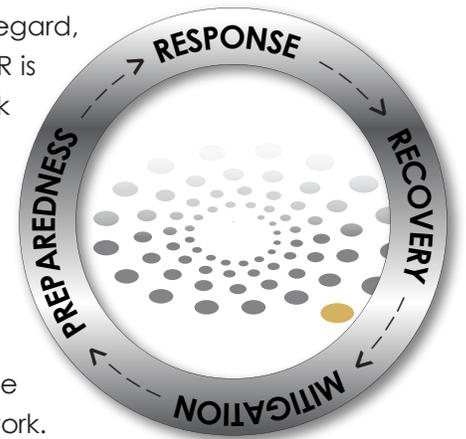


Figure 6: Response, Recovery, Mitigation, Preparedness

### Standards and Policies

Standards and Policies should be developed, written, periodically reviewed, and evaluated in a collaborative environment to insure all aspects of the business function are addressed.

### Awareness, prevention, mitigation, response, and recovery

In the context of planning it is important to address the full life cycle of possible events

**Awareness** is simply being aware of potential incidents which can impact the functions of the Enterprise. These can be known events which are planned for in advance or developing situations which are impacted by world events.

**Mitigation** efforts attempt to prevent hazards from developing into disasters altogether, or to reduce the effects of disasters when they occur. The mitigation phase differs from the other phases because it focuses on long-term measures for reducing or eliminating risk.

A precursor activity to the mitigation, is the identification of risks. This is accomplished during the process of Risk, Threat, and Vulnerability Assessment. In essence, the higher the risk, the more urgent that the hazard specific vulnerabilities are, targeted by mitigation and preparedness efforts. However, if there is no vulnerability, there will be no risk, e.g. an earthquake occurring in a desert where nobody lives.

**Preparedness:** In the preparedness phase, we develop plans of action for when the disaster or serious incident strikes. Common preparedness measures include:

- Communication plans with easily understandable terminology and methods.
- Proper maintenance and training of emergency services, including mass human resources such as community emergency response teams.
- Development and exercise of emergency population warning methods combined with emergency shelters and evacuation plans.
- Stockpiling, inventory, and maintain disaster supplies and equipment.
- Develop organizations of trained volunteers. (Professional emergency workers are rapidly overwhelmed in mass emergencies; trained, organized, responsible volunteers are extremely valuable.

Another aspect of preparedness is casualty prediction, the study of how many deaths or injuries to expect for a given kind of event. This gives planners an idea of what resources need to be in place to respond to a particular kind of event.

The planning phase should be flexible and all encompassing - carefully recognizing the risks and exposures of their respective regions and employing unconventional and atypical means of support. Mutual aide agreements between supporting agencies should be identified early in planning stages and practiced with regularity.

**Response:** This phase includes the mobilization of the necessary emergency services and first responders in the disaster area. This is likely to include a first wave of core emergency services.

A well-rehearsed emergency plan developed as part of the preparedness phase enables efficient coordination of rescue. Organizational response to any significant disaster – natural, man-made, or technical, is based on existing emergency management organizational systems and processes.

**Recovery:** The aim of the recovery phase is to restore the affected area to its previous state. It differs from the response phase in its focus; recovery efforts are concerned with issues and decisions that must be made after immediate needs are addressed. Recovery efforts are primarily concerned with actions that involve rebuilding destroyed property, re-employment, and the repair of other essential infrastructure. An important aspect of effective recovery efforts is taking advantage of a 'window of opportunity' for the implementation of mitigation measures that might otherwise be unpopular.

## IMPLEMENTATION AND OPERATION

### Five key principles of Implementation

**Engaged partnership** means that leaders at all levels collaborate to develop shared response goals and align capabilities. This collaboration is designed to prevent any level from being overwhelmed in times of crisis.

**Tiered response** refers to the efficient management of incidents, so that such incidents are handled at the lowest possible level and supported by additional capabilities only when needed.

**Scalable, flexible, and adaptable operational capabilities** are implemented as incidents change in size, scope, and complexity, so that the response to an incident or complex of incidents adapts to meet the requirements under ICS/NIMS management by objectives. The ICS/NIMS resources of various, formally-defined resource types are requested, assigned, and deployed as needed, and then demobilized when available and incident deployment is no longer necessary.

**Unity of effort through unified command** refers to the ICS/NIMS respect for each participating organization's chain of command with an emphasis on seamless coordination across jurisdictions in support of common objectives. This seamless coordination is guided by the 'Plain English' communication protocol between ICS/NIMS command structures and assigned resources to coordinate response operations among multiple jurisdictions that may be joined at an incident complex.

**Readiness to Act:** "It is our collective duty to provide the best response possible. From individuals, households, and communities to local, tribal, state, and federal governments, national response depends on our readiness to act." (Government, 2008)

## THE RESULT

When we look at successfully surviving an event, we have to consider several factors for evaluation. These factors are the type and duration of the event, the organization's risk appetite, and the organizational level of preparedness.

As previously discussed, your event can be man-made, technological, or natural. What is critical here is the magnitude and duration of the event. Simple research will show that the longer it takes to resolve an emergency, the more expensive it becomes. In fact our studies show there is a significant spike in costs when an event lasts beyond seven days. In short, the longer the span of time from onset to recovery, the more costly the event.

We define risk appetite as the amount of risk exposure or potential adverse impact from an event, which an enterprise is willing to or has the capacity to accept. This is generally quantified using measures of loss or measures of consequence. For simplicity purposes, we will use finances as a measure of loss. We measure loss using factors of low, medium, and high. Where a low loss is something that is budgeted for, a medium loss requires a reallocation of funds, and a high loss is a catastrophic failure where an enterprise cannot continue to exist without outside assistance. This point where catastrophic failure occurs, is total value of risk appetite.

*Given the above we have identified three opportunities for enterprise success:*

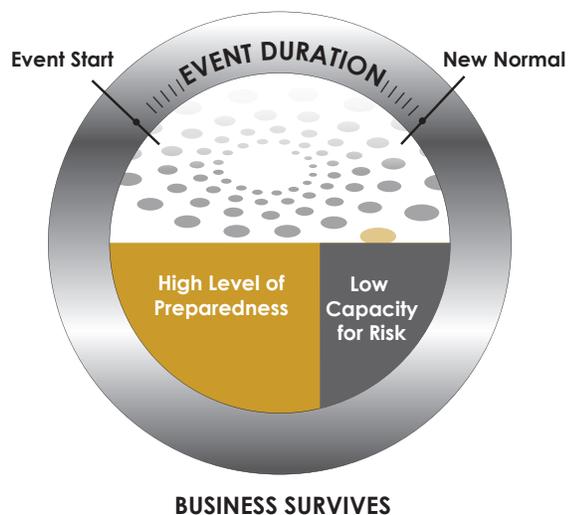


Figure 7: Opportunity #1- High Levels of Preparedness and Low Risk Appetite  
– In this scenario, the enterprise has gone to great lengths to insure it is fully prepared to respond to any risk which impacts the enterprise.

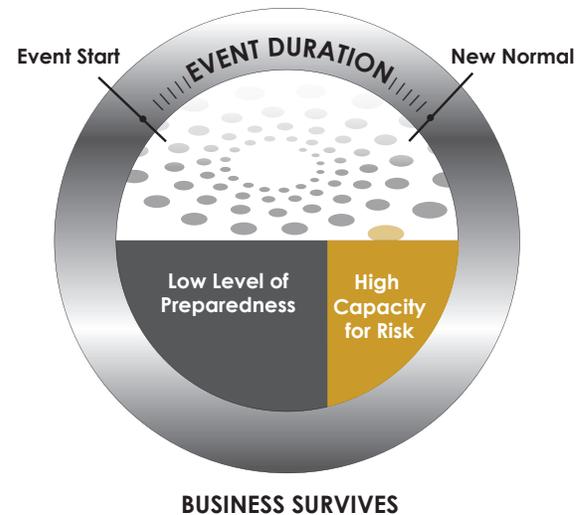


Figure 8: Opportunity #2- Low Levels of Preparedness and High Risk Appetite  
– In this scenario the enterprise has done very little to prepare itself but possesses great wealth and can buy itself out of most events.

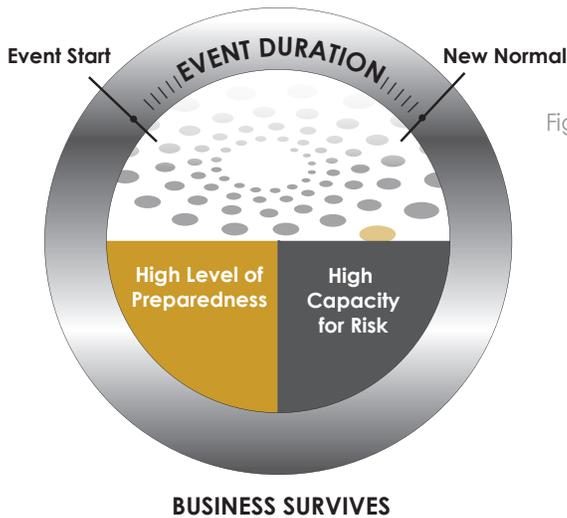


Figure 9: Opportunity #3- High Levels of Preparedness and High Risk Appetite – This is the ideal scenario where an organization has very high levels of preparedness and a high risk appetite. The advantage of this particular scenario is that if the enterprise is highly prepared they can maximize their advantage and even profit when their competitors fail.



Figure 10: Resilience & Risk Management

## THE CHIEF SECURITY OFFICER’S RELATIONSHIP TO ORGANIZATIONAL RESILIENCE MANAGEMENT

As we move forward, it is important to consider Machiavelli, “There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things, because the innovator has for enemies all those who have done well under the old conditions and lukewarm defenders in those who may do well under the new.”

*Change can be dangerous if you are not prepared to lead. And our world is changing.*

So the question becomes: Are you an emissary and leader of change? As a security professional, are you willing to consider new concepts such as Organizational Resilience Management or are you content with supporting the status quo? Do you understand the impact (The Cost of Standing Still) of the Status Quo on your Enterprise? The province of the Security Manager now includes a comprehensive management systems approach for prevention, protection, preparedness, response, mitigation, continuity, and recovery for disruptive incidents resulting in an emergency, crisis, or disaster. The diagram above, Figure 10, demonstrates the relationships of the CSO to other risk functions in the enterprise. These risk related relationships all impact organizational resilience; although in many organizations, the data kept for each of these functions may be disparate. Additionally, data may be stove piped according to discipline. In any case, this generally means that the information is not readily available to the CSO or other members of the C-Suite.



Figure 11: Security Manager – This demonstrates the internal interdependencies that most CSO's must cope with. The job function of the CSO interfaces with all aspects of the enterprise. Some primary examples of this relationship are in the areas of Information Technology, Human Resources, and Operations.

Information Technology directly interfaces to security through the integration of networked physical security and the use of physical security devices for multiple functions such as card key access systems being utilized for time and attendance.

An example of the interface with Human Resources are background checks, employee investigations, and terminations.

An example for Operations is the security and impact to the enterprise's supply chain.

Interdependency defined: A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.

Critical external interdependencies have significant impact on the enterprise. Identifying and categorizing interdependencies helps the enterprise to understand where it is most vulnerable. Rinaldi, Peerenboom, and Kelly (2001) classified infrastructure interdependencies as being one of four types: physical, cyber, geographic, or logical. (Figure 12)

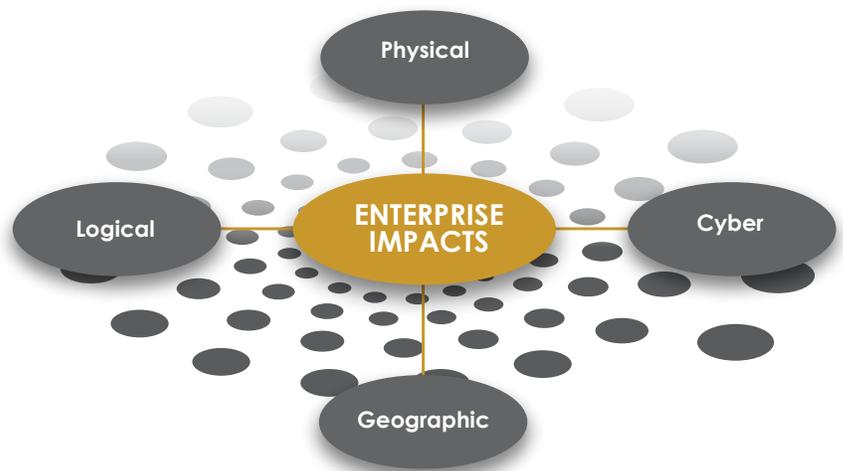


Figure 12: Enterprise Impacts

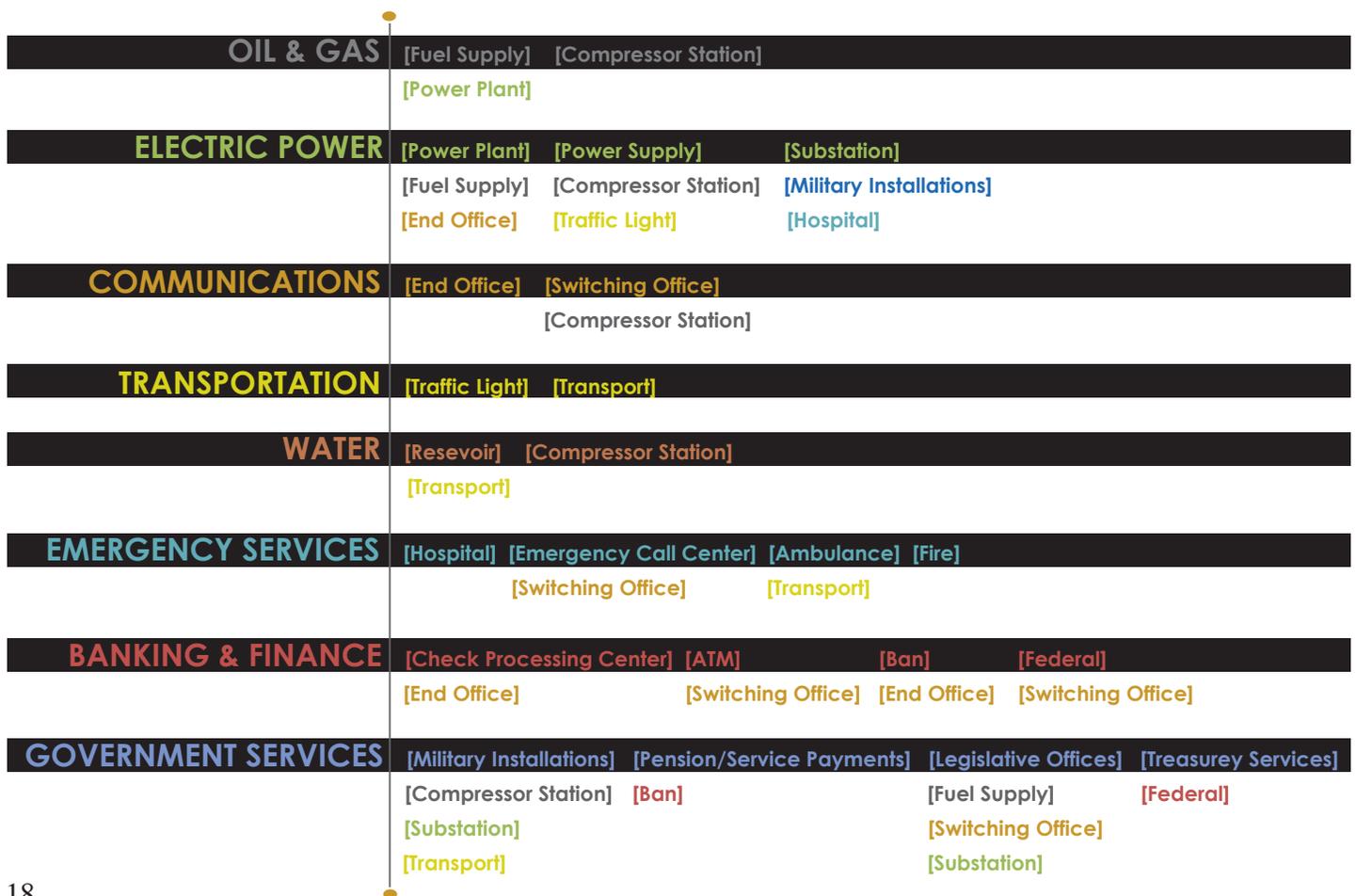
**Physical** – A physical reliance on material flow from one infrastructure to another. Physical interdependencies involve disruptions that physically impact one or more other infrastructures. The risk of failure from normal operating conditions in one infrastructure will be a function of risk in another infrastructure.

**Cyber** – A reliance on information transfer between infrastructure assets. Cyber interdependencies occur when the operation of one infrastructure is dependent on another infrastructure via information or communication links. This is the type of complex system whereby control of a networked system is dependent on the transmission of information.

**Geographic** – A local environmental event affects components across multiple infrastructures due to physical proximity. Geographic interdependencies involve the physical proximity of one infrastructure to another. An event such as an explosion of a gas main in an urban area could create correlated disruptions with other infrastructures such as water and electric services to a community.

**Logical** – A dependency that exists between infrastructures that does not fall into one of the above categories. Logical interdependencies mean that the state of one infrastructure is dependent on another due to some economic or political decision. An example of this is the logical interdependency between the cost of fuel and the number of vehicles using the transportation infrastructure. (Rinaldi, 2001)

Figure 13: Graphic shows a more complex view of critical interdependency employing utilities as an example. It is important to note all the complex multi-levelled inter-relationships. (Rinaldi, 2001)



## THE COST OF NOT BEING RESILIENT

The financial impact of events cannot be overstated. Worldwide, the cost of natural disasters and terrorism exceed the gross domestic product of many countries. When you consider the financial and global supply chain impacts of the recent tsunami in Japan, the costs of terrorism since 2011, the financial impact of the conflicts in Libya, Syria, and Lebanon, or the cost of the recent riots in England and France, you immediately get a sense of the real costs of not being resilient.

A recent situation which had presented itself in my own community was the identification of defects in an abutment to the Howard Hanson Dam. The Howard Hansen Dam provides flood control for the Green River Valley in Washington State. This posed a unique threat to our state economy and to the second largest goods and services distribution center on the West Coast, including job sites of more than 112,000 workers and homes of more than 25,000 residents. The valley is home to about 170,000 residents and numerous industrial facilities some of which are the Seattle-Tacoma International Airport and sprawling corporate complexes and distribution centers belonging to companies such as Boeing, Microsoft, Starbucks, and REI. The Dams Sector Exercise Series DSES10 focused on the Green River Valley and all the complexities of the critical interdependencies in that location. As you can imagine, the regional impacts were huge with national economic implications.

With this in mind, it makes it easier to understand that we measure impact on the enterprise by identifying potential measures of loss. For purposes of this paper, a low loss is something that is budgeted for and has no impact on the enterprise, a medium loss requires a reallocation of assets to survive the loss, and a high loss is one that requires outside assistance to survive.

*Some measures of loss that we often consider in evaluating resilience are;*

- Loss of Life
- Loss of Revenue Stream
- Loss of Public Confidence
- Loss of Civil Order
- Loss of Personnel
- Loss of Supply Chain
- Loss of Utility
- Loss of Facilities
- Loss of Finances
- Loss of Communication

Capacity for risk or risk appetite is measured by many things including;

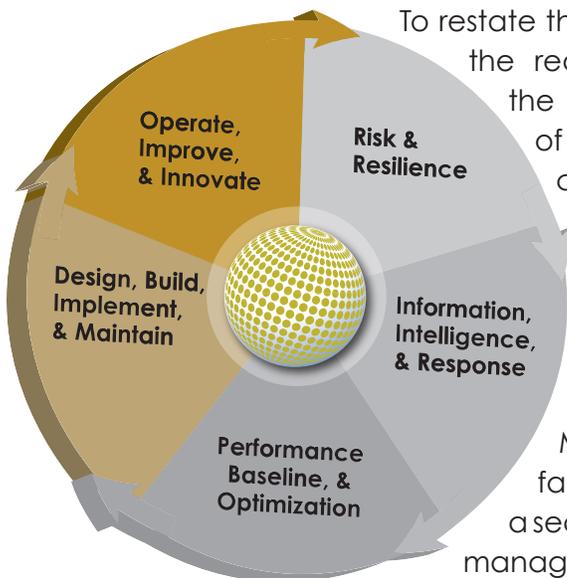
- Financial Resilience
- Supplies on hand
- Resource Availability
- Communication Capability
- Business Intelligence

The challenge is creating a common operating picture which leads to a common planning picture or unity of effort and purpose.

Understanding the above leads the reader to an apparent conclusion, in order to understand the common operating picture, we must have large amounts of information (data) which is easily understood, searchable, quantifiable, measurable, and recoverable.

## HOW DO YOU MAKE DATA INTELLIGENT?

### The Value of Data Management Tools and a Proposed Solution



To restate the above, understanding the cost of NOT being resilient leads the reader to an apparent conclusion, in order to understand the common operating picture we must have large amounts of information (data) which is easily understood, accessible, changeable, searchable, quantifiable, actionable, measurable, usable and recoverable.

There are a suite of products from Microsoft that, in conjunction with physical security devices and software, support all these attributes and more. There are some that you have been using for years, like the Office Suite and Microsoft Exchange email. Combined with SharePoint, these familiar tools become extremely powerful. SharePoint provides a secured, accessible, central collaboration platform for document management and business activities. SharePoint can centralize enterprise data such as calendars, contacts, tasks, and more. It provides

Figure 14: OR<sup>3</sup>M Value Stream

data analysis and manipulation tools and enterprise search, all in a platform that can be easily modified and extended with new features as your business needs change. SharePoint can deliver on a variety of clients from laptops to smart phones. There is an ever expanding variety of 3rd party custom features. Finally, it utilizes other industry forms of communications like RSS feeds, social media connections, visualization, and physical security information management.

OR<sup>3</sup>M and its partners such as General Dynamics Information Technology, Aronson Security Group, and the Security Executive Council, have taken this platform and tool-set to develop capabilities that provide value to your enterprise.



Figure 15: COP, Coord. Response, Cont. Org. Improvement

and compliance standards. They know it influences their organization's effectiveness and resilience as well as their supply chain.

In their enterprise, they have external and internal standards as well as protocols, which address risks, threats, and incidents. Additional information streams are found in deployed physical security devices, software, and databases, and they need an intuitive means to collect, organize, and harmonize this huge influx of data.

What is required is a central repository that unifies and aligns business intelligence with all-hazards risk intelligence. Couple this with industry best practices and processes, and align and harmonize those standards with internal standards. This creates an opportunity to see, manage, measure, and report on the information. These are the drivers and metrics that determine performance and value.

## The Process

OR<sup>3</sup>M services allow for the integration, harmonization, and customization of internal standards. As well, it provides the connector methodology and services that allow for seamless integration of data streaming from the devices, software applications, and databases that drive business and security analytics. Analytics drive business & security intelligence and response.



Figure 16: vSOC ra

OR<sup>3</sup>M has a process and an application that uses a Commercial Off-the-Shelf (COTS) technology platform – SharePoint. The process steps you through the main components of the PDCA process, a standard project management process with a twist. The process begins with OR<sup>3</sup>M's vSOCra™, a detailed all hazard Risk, Threat, and Vulnerability (RTV) assessment tool. Utilizing touch technology and a dashboard-driven user interface, vSOC-RA (Risk Assessment) achieves real time information which can then be leveraged and utilized for security master planning, metrics creation, critical decision making, and defining physical security system network architecture. Gathering this critical information allows us to work with you to develop the appropriate framework for your market, company, and solution.

Your success depends on a thorough understanding of your unique requirements. However, today's business and budgetary requirements depend on a rapid implementation and return on investment (ROI). The OR<sup>3</sup>M process does both by utilizing a network of qualified risk consultants, technology process optimization professionals, and systems integrators, working with shared values and shared processes. A proper review of facilities, personnel, and area crime activity identifies any pre-existing or potential threat as well as the current vulnerability of personnel & physical assets. The finished product should address not only terrorist and criminal threats, but safety, natural disasters, and continuity of operations planning (COOP). Threat Assessment and Vulnerability Studies include a review of all policies and procedures to ensure that your current documentation supports contemporary security standards.

But don't let our process cloud your perception of Time-to-Value. To be specific, the OR<sup>3</sup>M approach ensures that every minute and dollar is focused on the value you are attempting to achieve. We work backwards from the metrics that ultimately fund your operation. We have experience in doing so as well as industry benchmarks that will help guide your future metrics.

## SOLUTIONS FOR THE NEXT GENERATION SECURITY OPERATION

Today, there are a variety of approaches to managing distributed work forces and supply chains. As well, more and more applications are making themselves available through different virtualized environments: from Software-as-a-Service, Infrastructure-as-a-Service and Hybrid services involving private and public clouds.

At OR<sup>3</sup>M, we want to ensure that we are building your solution to fit your current and future needs. By standardizing on Microsoft's SharePoint 2010 and other COTS products that are being built 'cloud-ready,' we are ensuring your future.

The v-SOC (Virtual Security Operations Center) is designed to leverage and mitigate risk to achieve organizational objectives. The following is a brief summary of general capabilities which form the basis of the v-SOC. These can be customized or enhanced based on your requirements.

*The operations consoles are developed to support the various roles conducted at the center. These include:*

- Duty Office, Supervisor and others
- Time Accounting
- Checklists and Protocols
- Incident Management
- Field Support
- Systems and Logs
- Check In and Out

The field operations are delivered by site and consoles accessed from field locations and applications resident on mobile devices. Features include:

- Time accounting
- State and end of shift checklists
- Protocols for maintenance checks
- Incident reporting
- Route management
- Post orders

We offer the following consoles which can be operated as stand-alone products or integrated to achieve organizational resiliency:

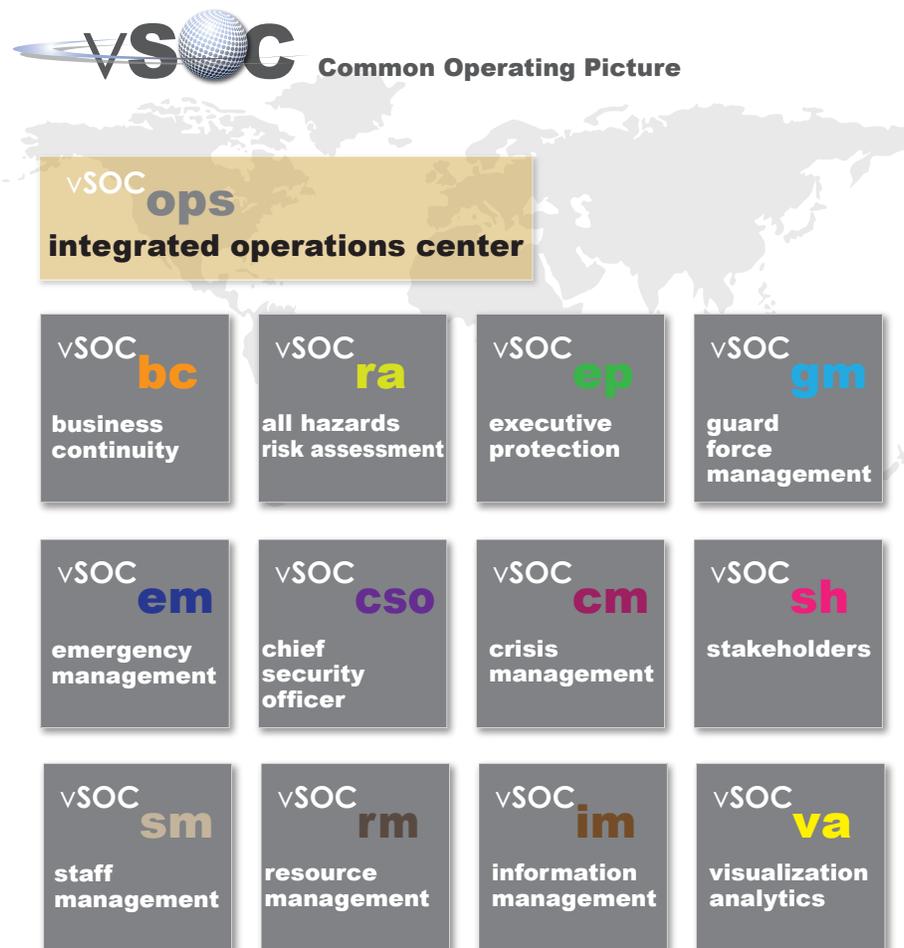


Figure 17: Integrated Operations Center

## Industry Best Practices and Compliance Library

*Examples Include:*

- Critical Infrastructure
  - Utilities
  - Oil and Gas
  - Transportation
- Customization Assessment and Update Service Available

## Institutional Knowledge Repository (IKR)

- Aggregation of organization intelligence and practices gathered during an IRA-PM through a board certified security management professional that has been trained to use our OR<sup>3</sup>M v-SOC Portal

## Business Analytics

- IKR and Business Process (Risk Protocols) are aligned to create a high velocity, leveraged, and targeted response

## Assessment Practices of OR<sup>3</sup>M™

- IRA-PM: Risk, Threat, and Vulnerability Assessment of Critical Infrastructure
- Business Impact Analysis (BIA)

## Planning Practices

- Business Continuity
- Crisis Management
- Emergency Management

## GETTING STARTED AND MOVING FORWARD

As the CSO, this can be easy enough if you start with thoroughly understanding core business concepts as intended by W. Edwards Deming, embrace the concept of Organizational Resilience, and utilize tools like Microsoft SharePoint to assist in collating and manipulating data.



Figure 18 (International, 2009) Understand, this is a continuous process which uses the Plan, Do, Check, Act (PDCA) cycle.

But moreover, leaders need to create a picture or vision for their organization. Paint a picture of success, detail for your colleagues what success looks like, and create metrics to quantify success. More importantly, understand that you cannot eat a whole pie at once but you can enjoy each bite. Keep your eye on long term success and realize that you will be better tomorrow than you were today, and you will be better six months from now than you were last month. To do that, you have to keep your eye on the long term, celebrate your successes, and maintain momentum by communicating, planning, and reaching for the next step.

***The end result is an efficient enterprise capable of confronting adversity anticipated and not anticipated. You will be better managed because the management team is practiced, adaptive, and collaborative.***

Challenges are acceptable when processes are in place to handle any emergency.

## OR<sup>3</sup>M OVERVIEW

OR<sup>3</sup>M is a security information management company. OR<sup>3</sup>M provides products and services that are intended to fulfill the promise of Organizational Resilience Management (ORM). The products reside on a Commercial Off-the-Shelf (COTS) platform: Microsoft SharePoint. The information architecture is a layered approach beginning with the external standards and protocols that undergird every security operation. This creates the context for Total Quality Management and Continuous Compliance™.

### A Story of Risk and Technology

We were started by a certified risk consultant who had a dream of providing his peers with a tool that would help their clients see the power of aggregating the critical information that was collected during and after the assessment process. As well, if that information was available to be integrated and aligned real-time into the physical and logical devices, applications and databases, then the organization would be positioned to achieve continuous compliance and continuous quality improvement. To do that requires a risk and performance dashboard.

## “SECURITY NEEDS A RISK, VALUE, AND PERFORMANCE DASHBOARD”

He then teamed up with an ex-CIO who believed in Commercial Off-the-Shelf (COTS) implementations that were highly customizable with easily adaptable and configurable connectors or integration capabilities.

They worked with a number of pilots and collaborated with their early clients over the course of two years before launching under their new name: OR<sup>3</sup>M. It stands for Organizational Risk Management (ORM) with the power of risk, resilience, and reward (ROI, TQM, CQI, etc.) that is: an alignment of an organization's risk profile with their organization's goals and objectives so that the company is adaptable and resilient in facing the challenges of a global marketplace.

Today, they are moving rapidly to create the first Total Quality Management (TQM) information platform for security and risk professionals. We are working with the industry standards organizations, the certified professional risk consultant community, security integrators, and technology vendors to deliver to end users a new level of visibility to their risk profile and operational performance; a redefinition of the term 'integration.'

**Risk and Technology; Metrics and Performance; Intelligence and Action:** a new approach that will redefine integration between the industry's professional disciplines and well as the products within its security information architecture. When security operations are built intelligence ready, performance ready, and cloud ready, a new level of value will be achieved.

## “INTELLIGENCE-READY, PERFORMANCE-READY, CLOUD-READY”™