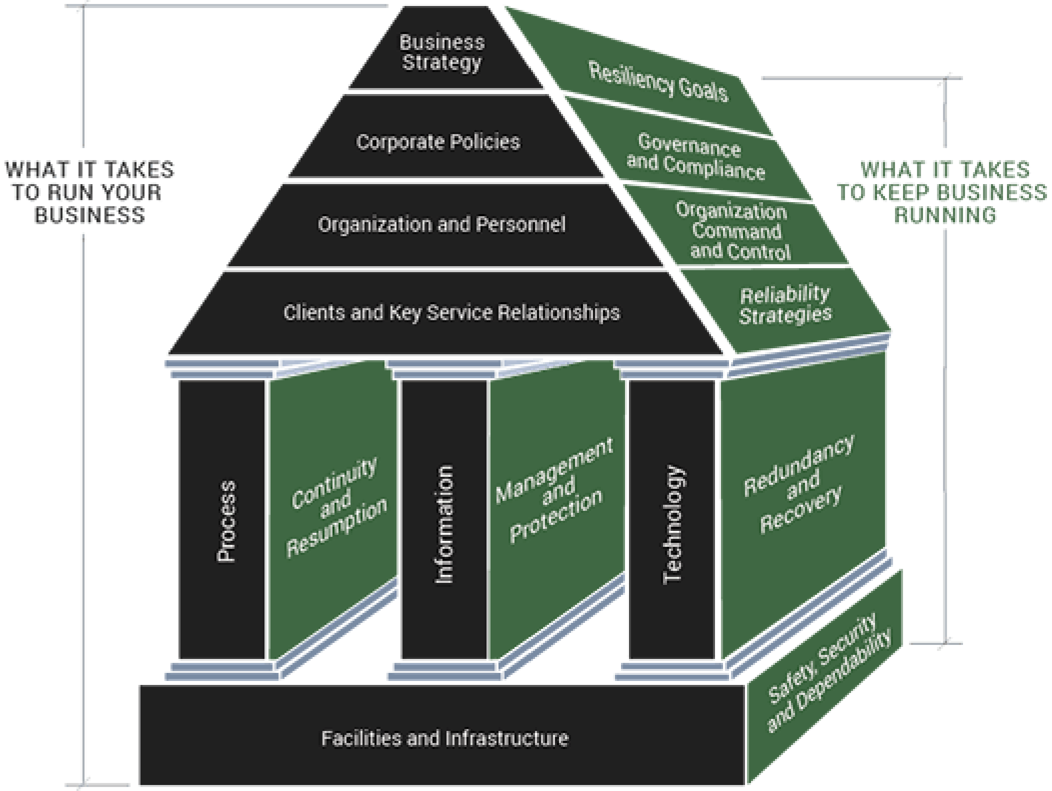
Enterprise Resiliency Blueprint

Overview

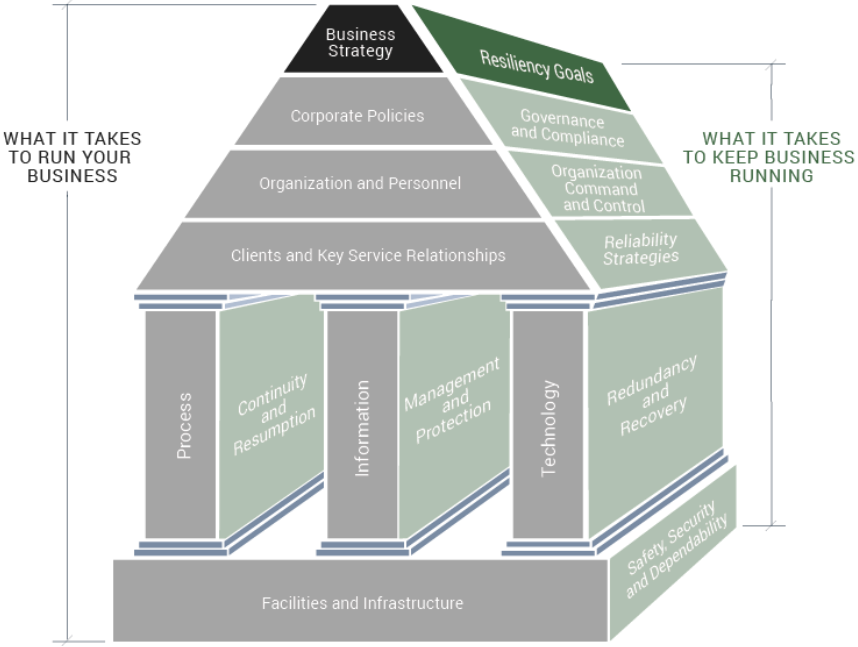
Enterprise Resiliency is the ability of an organization to be flexible, adaptive and responsive to impacts of significant events, predicted or unforeseen, and at the same time be fortified against those same risks. An organization's resiliency is dependent upon the effectiveness of the reliability, protection, recovery and continuity strategies in place and routinely practiced. True resiliency is achieved through proactive, comprehensive and carefully coordinated programs that are designed to maintain desired levels of operational effectiveness of essential processes, and the safety and availability of organizational personnel, under all circumstances.

The diagrams below, the Enterprise Resiliency Blueprint, illustrates the high-level elements that guide risk and resiliency management planning. Eagle Rock's **ERA*360 methodology** for Enterprise Resiliency Assessments covers each of the elements of the blueprint. Execution of the methodology results in a detailed examination and report on an organization's operational resiliency. Click on the Blueprint tiles on the right to view the elements of the enterprise and their corresponding resiliency investments.


WHAT IT TAKES TO RUN YOUR BUSINESS
Business Strategy
Corporate Policies
Organization and Personnel
Clients and Key Service Relationships
Process
Information
Technology
Facilities and Infrastructure
Resiliency Goals
Governance and Compliance
Organization Command and Control
Reliability Strategies
Continuity and Resumption
Management and Protection
Redundancy and Recovery
Safety, Security and Dependability
WHAT IT TAKES TO KEEP BUSINESS RUNNING

Sectional Breakdown of the Resiliency Blueprint

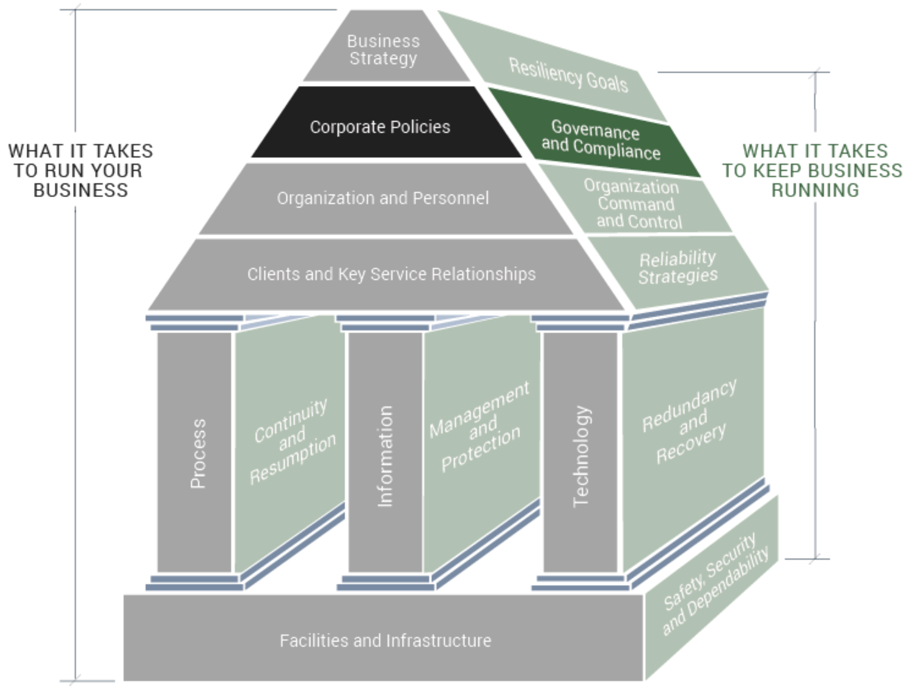
Business Strategy / Resiliency Goals


Business Strategy
Resiliency Goals
WHAT IT TAKES TO RUN YOUR BUSINESS
Corporate Policies
Governance and Compliance
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Organization and Personnel
Organization Command and Control
Clients and Key Service Relationships
Reliability Strategies
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Safety, Security and Dependability
Facilities and Infrastructure

A cornerstone in the implementation of a Business Strategy is the setting of goals for resiliency of the business itself. These Resiliency Goals must be in lockstep with the business strategy. Likewise, the elements of the resiliency model must be aligned with the implementation and execution at all levels of the business strategy throughout the enterprise.

The Resiliency Goals affect all facets of the enterprise and are the drivers for all investments in protection, risk mitigation, redundancy, continuity and insurance. They are affected by life safety, regulatory, and short- and long-term viability and other concerns of the enterprise.

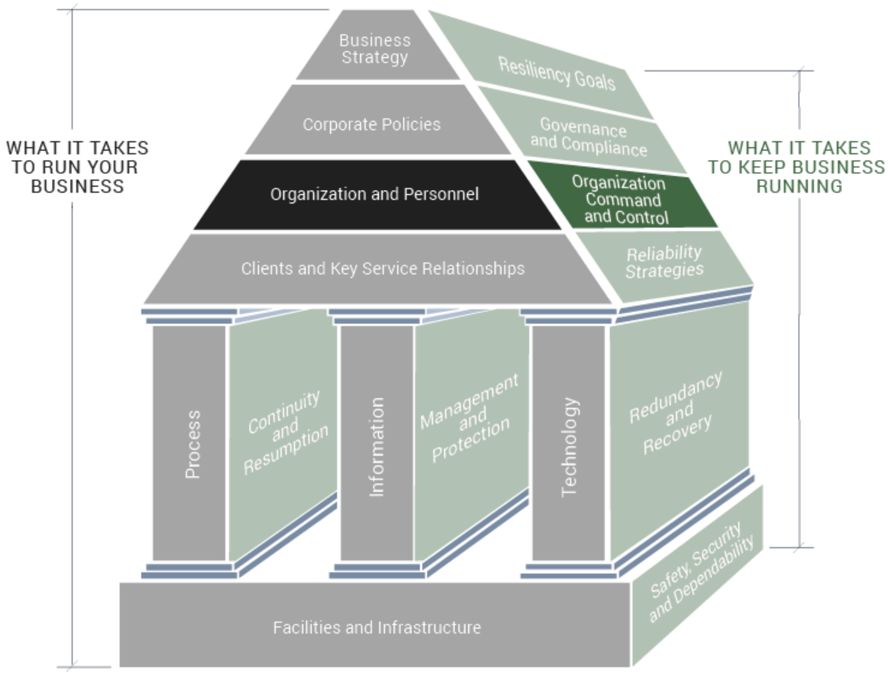
Corporate Policies / Governance and Compliance


WHAT IT TAKES TO RUN YOUR BUSINESS
Business Strategy
Corporate Policies
Organization and Personnel
Clients and Key Service Relationships
Process
Information
Technology
Facilities and Infrastructure
Resiliency Goals
Governance and Compliance
Organization Command and Control
Reliability Strategies
Continuity and Resumption
Management and Protection
Redundancy and Recovery
Safety, Security and Dependability
WHAT IT TAKES TO KEEP BUSINESS RUNNING

Resiliency goals can be analyzed and established in a structured and controlled program, or less formally by practice. Either way, they should be documented and communicated to all key personnel. The organization must be able to plan and measure progress and investments against stated resiliency objectives. The goals must be translated into objectives for safety, service, response and availability commitments of the business. These objectives must align not only with the overall resiliency goals and budgets established, but must also meet all internal and external compliance requirements for the business.

A Governance and Compliance model will translate the corporate goals and policies into manageable metrics and required reporting for the entities within the enterprise. Then, the resiliency program manager will define the organizational elements, quantify the objectives, establish the measurement criteria and set up the operational program elements.

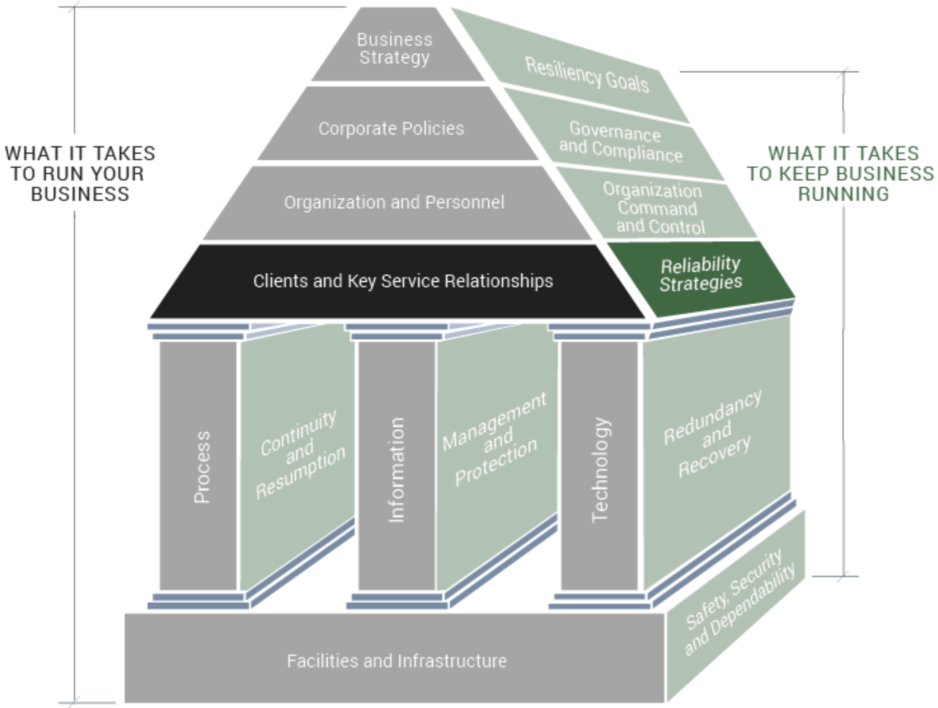
Organization and Personnel / Command and Control


Business Strategy
Resiliency Goals
Corporate Policies
Governance and Compliance
WHAT IT TAKES TO RUN YOUR BUSINESS
Organization and Personnel
Organization Command and Control
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Clients and Key Service Relationships
Reliability Strategies
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Safety, Security and Dependability
Facilities and Infrastructure

The ability to provide timely and visible leadership during a crisis is important to the safety and welfare of the personnel and the long-term viability of the enterprise. Communication with critical information sources, first responders, civil authorities, facilities personnel and utility providers sets the stage for proper assessment of the incident and its impact. Communication with staff members allows the flow of vital information to ensure safety, security and proper response to the crisis. Communication with clients, business partners and stakeholders is key to preserving the reputation and marketability of the enterprise. Communication with key vendors, outside service providers and other third parties is vital to establishing smooth and continued operation of business and the avoidable consequences of a poor response to an unplanned event.

Organizational Command and Control must be achieved quickly at the time of crisis. An emergency communication capability and documented Crisis and Emergency Response Plans are the top priorities required to assure the safety of personnel and future viability of the enterprise during and after an emergency.

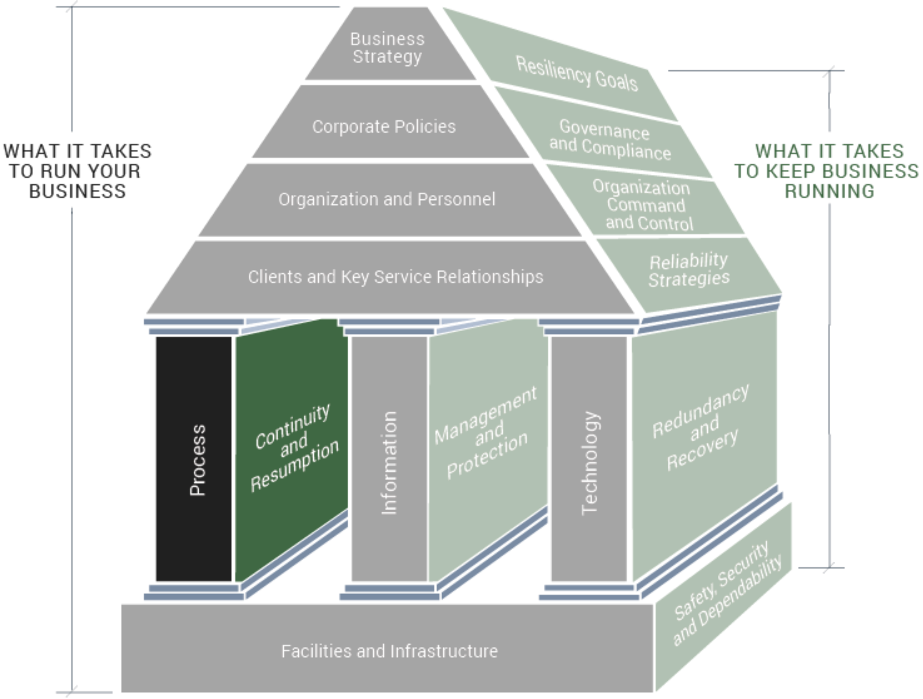
Clients and Key Service Relationships / Reliability Strategies


WHAT IT TAKES TO RUN YOUR BUSINESS
Business Strategy
Corporate Policies
Organization and Personnel
Clients and Key Service Relationships
Resiliency Goals
Governance and Compliance
Organization Command and Control
Reliability Strategies
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Facilities and Infrastructure
Safety, Security and Dependability

Clients rely on the availability of the personnel and processes of the enterprise in the daily conduct of their own businesses. Likewise, the enterprise relies itself on its key service relationships, aka the Supply Chain, whether internal or outside services providers (OSPs), to fulfill service commitments to its clients and other counterparty relationships (such as governmental agencies, banking, regulatory, etc.). The linkages in the process chain must be re-established when broken, and in proper sequence and timing, to ensure that service reliability continues to meet contractual, regulatory, market reputation, and customer confidence criteria defined by the organization.

Reliability Strategies must be designed to protect against the interruption of the business process or to ensure the rapid re-establishment of the process, if interrupted. The strategies must ensure predictable restoration of services and resumption of business at the proper time, in the proper sequence and to the acceptable levels to meet the business strategy as defined.

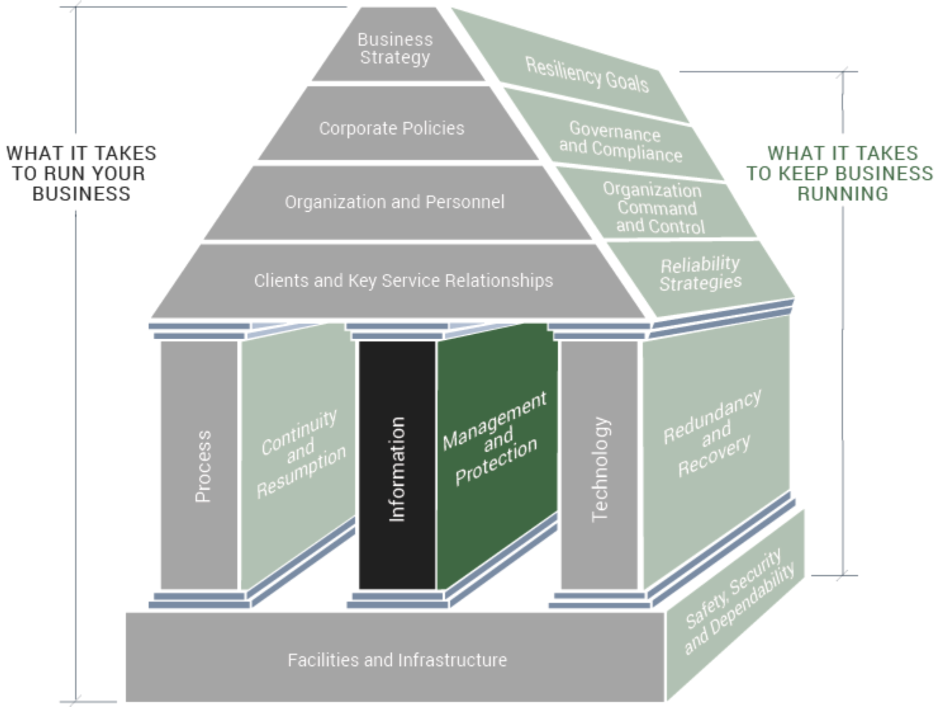
Processes / Continuity and Resumption


WHAT IT TAKES TO RUN YOUR BUSINESS
Business Strategy
Corporate Policies
Organization and Personnel
Clients and Key Service Relationships
Resiliency Goals
Governance and Compliance
Organization Command and Control
Reliability Strategies
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Facilities and Infrastructure
Safety, Security and Dependability

The identification and prioritization of critical business processes are essential in establishing a comprehensive business continuity capability. The ability to sustain critical business operations during an unplanned event may require workarounds, alternate workspace or other special solutions. Business processes must be identified, prioritized and mapped to all supporting functional requirements: voice communications, e-mail, fax, workspace requirements, applications, technology, etc. Procedures are also needed to account for operational activity lost due to the event and from the time an incident occurs and the time when the business can resume, which could be hours, days or weeks.

Continuity and Resumption plans document who should go where, how to get there and what to do to restore, resynchronize and resume the processes in a pre-orchestrated, coordinated, and predictable manner. Testing and rehearsing (Table Top or simulated) will minimize crossed signals, confusion, and avoidable loss. All of these requirements and activities are to be documented in Business Continuity Plans, which must be properly maintained and periodically exercised.

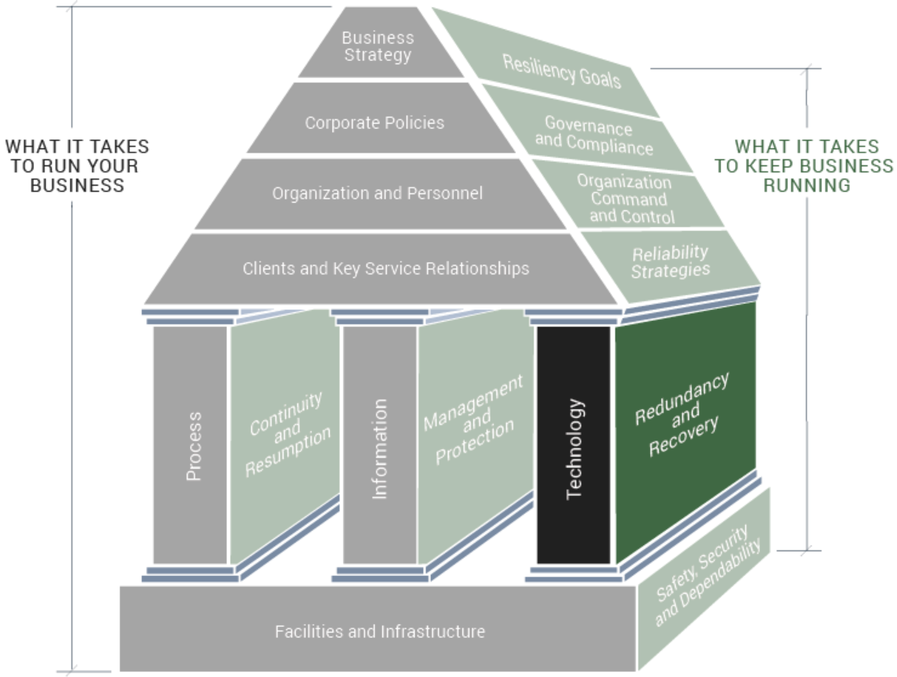
Information / Management and Protection


Business Strategy
Resiliency Goals
Corporate Policies
Governance and Compliance
WHAT IT TAKES TO RUN YOUR BUSINESS
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Organization and Personnel
Organization Command and Control
Clients and Key Service Relationships
Reliability Strategies
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Safety, Security and Dependability
Facilities and Infrastructure

Information in all its forms is a key asset of the enterprise. Lost information is difficult or often impossible to recover. Regulations mandated by legislative bodies, executive orders, the Sarbanes-Oxley Act, FINRA, the FDA, the FFIEC, the OCC, HIPAA, or by contracts impact the retention and availability requirements of data for certain businesses. These regulations, coupled with sound business practices, drive the need to properly safeguard information under normal working conditions, as well as in the event of a disaster.

Management and Protection of information, both hard copy and electronic, through a comprehensive Vital Records program driven by the needs of the business, including regulatory requirements and service level agreements (SLAs), are necessary to ensure availability of business information. Making records and data available when and where needed at time of crisis is paramount to business resiliency.

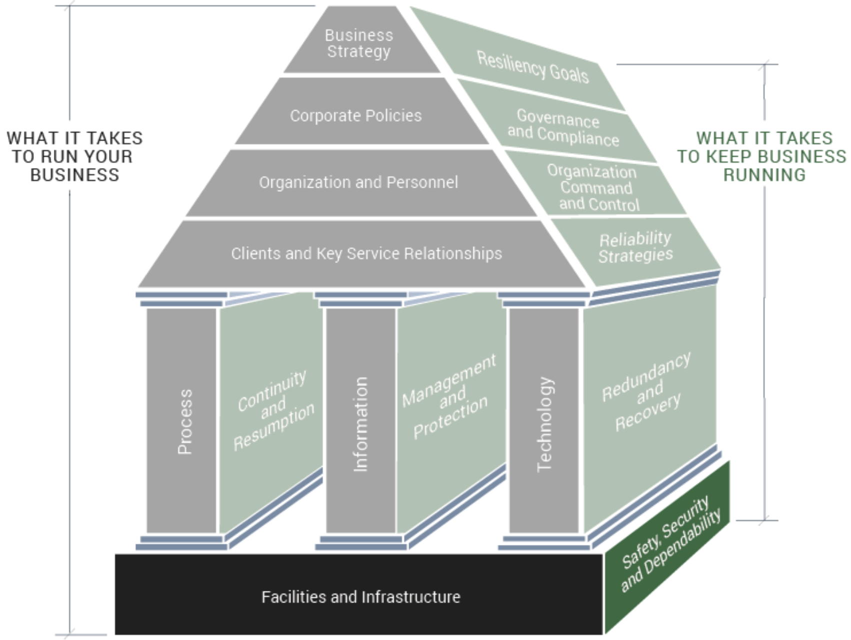
Technology / Redundancy and Recovery


WHAT IT TAKES TO RUN YOUR BUSINESS
Business Strategy
Corporate Policies
Organization and Personnel
Clients and Key Service Relationships
Resiliency Goals
Governance and Compliance
Organization Command and Control
Reliability Strategies
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Facilities and Infrastructure
Safety, Security and Dependability

Many IT departments today are managed as internal or sometimes external service organizations to the business. Typically, there are service level agreements or expectations by which these departments are measured by their users. These services must be provided under normal conditions and during emergency/disaster conditions, as well. Proactive, structured and integrated efforts are required to achieve desired resiliency commitments. Business application priorities driven by Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) will dictate the level of investment to be made in the technology resiliency architecture.

Redundancy and Recovery: IT Disaster Recovery plans should be a combination of service continuity (fail-over) and restoration from disk, tape or network download, accounting for all levels of RTO/RPO specified by the business. The first step of the plan involves the people and tools required to maintain or restore the environment. The next step is the granular implementation "playbook", which details the priority order of steps, anticipated time frames, and inter-dependencies among the processes.

Facilities and Infrastructure / Safety, Security and Dependability


WHAT IT TAKES TO RUN YOUR BUSINESS
Business Strategy
Resiliency Goals
Corporate Policies
Governance and Compliance
Organization and Personnel
Organization Command and Control
WHAT IT TAKES TO KEEP BUSINESS RUNNING
Clients and Key Service Relationships
Reliability Strategies
Process
Continuity and Resumption
Information
Management and Protection
Technology
Redundancy and Recovery
Facilities and Infrastructure
Safety, Security and Dependability

The enterprise that truly wants to be resilient will first mitigate its risks in order to reduce the likelihood of an occurrence. Investments in enhancing or "hardening" facilities to comply with an acceptable percentage of failure or breach probabilities are typical as a starting point. Increased investments in physical, network and software security are often wise investment requirements. Risk can be in the form of man-made risks, natural risks and infrastructure risks. Risk can also come from internal as well as external sources.

Safety, Security and Dependability: Job #1 is ensuring the safety and security of the personnel, and then the security and dependability of the business. The facilities' safety and security procedures are foundational to the establishment of an Emergency Response Plan for the enterprise. The Emergency Response Plan will integrate the emergency needs of all other business aspects, once people and property are secured.