How to Develop a Vital Records Program Project Plan

According to "Why Records Management?" from Professional Records & Information Services Management International, 90% of businesses are unable to continue beyond two years when their vital records are destroyed. This is why every organization must have a vital records program.

Amy Van Artsdalen, IGP, CRM

The protection of vital records – which ARMA International defines as those that are "fundamental to the functioning of an organization and necessary to the continuance of operations" – could mean the difference between a successful recovery or a devastating loss for an organization. This is why it is incumbent upon information governance (IG) professionals to stress the criticality of protecting vital records, particularly for those in organizations that think a vital records program would be too cumbersome or costly to develop and maintain.

Citing North American Electric Reliability Corporation Critical Infrastructure Protection (CIP) requirements – mandatory for utility companies, which are in a *critical infrastructure sector* that is vital to U.S. security and public safety, but also beneficial for all other types of organizations – may help provide additional justification for establishing a vital records program (see sidebar for more about CIP requirements).

Making the Business Case

In the book *Emergency Management for Records and Information*, Virginia Jones, CRM, FAI, and Darlene Barber, CRM, outline the initial steps of preparing an emergency management plan; selling top management and preparing a proposal, or business case, for the program are at the top of the list.

Thorough development of a business case that stresses the need for continued operations – even the survival of the organization – before, during, and after a crisis or abnormal event is fundamentally important to getting top management's support for developing and implementing a program. Keep in mind that a crisis may not be a natural disaster such as an earthquake, hurricane, fire, or flood; it could be the result of a data breach or ransomware attack, such as the May 2017 WannaCry attack that disabled systems in more than 150 countries.

Key aspects of the business case should include the following:

- An overview outlining the importance of the documents and those they serve
- Project start and end dates
- Projected budget information, including for hardware and software, if needed
- Project objectives, including policies and standards
- A defined strategy to protect vital records
- Data in the form of a vital records inventory
- Methods of protection and locations for remote storage
- A vital records schedule to refresh information so data remains current
- Plan for establishing remote access for electronic records, including the provision of hardware and software to access the information
- Plan for proper backing up, mirroring, or replicating electronic information
- Documented restoration timeframes, including delivery of physical records if needed
- An emergency contact list of employees and vendors, including methods of contact
- Contingency plans for the delegation of authority if the chain of command becomes broken
- Plans to periodically review and test the program

Emergency Management for Records and Information Programs and *Vital Records* (ARMA International 29-2017) provide extensive details on developing these parts of the business case. (Both are available in the ARMA International bookstore.)

Critical Infrastructure Protection Requirements

The Department of Homeland Security has identified 16 sectors that qualify as critical infrastructure sectors, "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." These sectors represent emergency services, transportation, communications, dams, water and wastewater, and energy.

The energy or utility sector must comply with North American Electric Reliability Corporation Critical Infrastructure Protection (CIP) regulations. CIP regulations are quite rigorous and require affected utilities to provide protections that are related to assets and systems such as control centers, backup centers, and energy transmission. CIP standards include those for:

- Security Management Controls
- Personnel & Training
- Electronic Security Perimeters
- Physical Security
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plan for Cyber Systems
- Configuration Change Management and Vulnerability Assessments
- Information Protection

Though not mandated to meet these CIP standards, all other organizations would find that compliance with them would be beneficial to them. These standards are available at *http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.*

Building the Team, Identifying Stakeholders

The protection of vital records is a cross-departmental effort that requires the help of subject matter experts (SMEs) from across the organization. For most organizations with a defined records management program, the best vital records SMEs are records coordinators or champions because they are already familiar with the records of their respective departments. Not only this, they have already developed relationships with their leaders and have key contacts

within the department who can answer questions about any aspect of the department or line of business records.

Records coordinators also can identify important stakeholders and thereby gain support for the program. In large organizations, a single information management or IG professional may have difficulty identifying the team or stakeholders and should seek input from SMEs.

Consider conducting a RACI analysis, determining for each project task who is:

- Responsible – the person who performs an activity or the task
- Accountable – the person who is ultimately answerable for the project and has yes/no/veto authority
- Consulted – the person who needs to submit feedback and contribute to the project
- Informed – the person who needs to know of the decision or actions

A RACI analysis is useful for balancing the workload. It ensures that key functions and processes are not overlooked, and it helps those new to the team identify their roles and responsibilities. In addition, it allows work assignments to be distributed among groups and individuals. The RACI may also provide a forum for resolving inter-departmental conflict because roles and responsibilities are documented.

Performing the RACI analysis will permit the project manager to look at the project horizontally and vertically. If there are too many responsible parties, for example, the project manager might ask if it is realistic to have the tasks divided into smaller parts so the workload is evenly divided. Likewise, too many informed parties could suggest there are too many people requiring feedback or involved in the approval process, which may slow the project.

In the *ezine.com* article "How to Do RACI Charting and Analysis: A Practical Guide," Roystan Morgan advises to "be sensible about the level of granularity for the definition of tasks/activities. Take it to a deep enough level that it is meaningful and at a level of that [that] is sensible."

A RACI analysis is useful for balancing the workload. It ensures that key functions and processes are not overlooked, and it helps those new to the team identify their roles and responsibilities. In addition, it allows work assignments to be distributed among groups and individuals.

Identifying Milestones and Deliverables

The program should begin with a project kickoff. For some organizations, this is a big celebratory event, while others may conduct a standard business meeting. Whatever the budget, begin the project with enthusiasm! During the meeting, introduce team members, discuss the initiative, and try to build momentum for the project. Discuss the milestones and how to achieve the goal.

Project milestones may include:

- Performing a risk analysis
- Developing a risk assessment
- Creating a chart that identifies critical functions of the organization
- Conducting a vital records inventory
- Classifying the vital records into emergency operating, disaster recovery, or legal and audit categories
- Developing methods of protection and working with IT to develop backup strategies
- Mitigating the loss of vital records
- Documenting a plan to periodically review and test the program

See *Emergency Management for Records and Information Programs* and *Vital Records* (ARMA International 29-2017) for more details.

Evaluating the Program

Once the program is implemented, involve the business continuity and disaster recovery teams to test whether and how well vital records can be accessed and retrieved. Ask SMEs to identify specific documents for retrieval, and measure success by the number of documents retrieved during testing, using a pass or fail scoring methodology.

The feelings of elation that occur when SMEs have successfully retrieved vital records are wonderful. Personnel understand they have a role in protecting information for themselves, their organizations, and their customers.

After the test, evaluate the successes and failures. Document what worked and what didn't. When failure occurs, turn to the ideals of process improvement rather than finger pointing. After all, the process will be new to most of those involved. Use the lessons learned to improve the program for the next series of tests.

Being Prepared: Better Than Being Lucky

Protecting vital records is one of the most important things IG professionals can accomplish during their careers. Most organizations will not be as lucky as a utility company that was affected by the August 2014 earthquake that struck in Northern California.

The supervisor related that the company was able to restore service

to more than 70,000 utility customers in less than 24 hours because all the important maps and drawings were stored in a large cabinet. So, even though the organization was without power to operate computers or to access network systems, it could still access the maps and other vital information that were stored in a paper format.

The company's ability to respond was impressive, but I asked what would have happened if the building that stored these physical documents had been "red tagged"as too dangerous to enter, making these documents inaccessible. He paused at length. We both knew the answer. E

About the Author: Amy Van Artsdalen, IGP, CRM, is an information management and information governance consultant for Joe Hill Consulting Engineers. She is charged with developing a comprehensive records management migration plan, including evaluating current databases and processes, providing technical support to be consistent with regulatory standards, and assisting with roll-out, data conversion, and training tasks. A certified Information Governance Professional and a Certified Records Manager, Van Artsdalen is working toward a bachelor of science degree in information technology – mobile development, management information systems, general from Capella University and has studied web design and new media at the Academy of Art University. She can be contacted at *mrsjpvan2@yahoo.com*.