Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Human Resource Management (HRM)

Richard A. Caralli
Julia H. Allen
David W. White
Lisa R. Young
Nader Mehravari
Pamela D. Curtis

February 2016

CERT Program

http://www.cert.org/resilience/

Carnegie Mellon

This material is based upon work funded and supported by various entities under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0003234

HUMAN RESOURCE MANAGEMENT

Enterprise

Purpose

The purpose of Human Resource Management is to manage the employment lifecycle and performance of staff in a manner that contributes to the organization's ability to manage operational resilience.

Introductory Notes

The way that an organization hires, manages, and terminates staff can have a significant effect on the organization's operational resilience. The Human Resource Management process area seeks to address the management of staff in a way that minimizes operational risk and contributes to the organization's ability to manage operational resilience.

In Human Resource Management, the organization consciously approaches the acquisition of staff as an activity that can improve operational resilience by ensuring the acquisition of necessary skill sets and the avoidance of introducing operational risk that results from poor hiring decisions. Staff are acquired with a view toward their contributions to meeting the organization's mission with an understanding and acceptance of their role in sustaining operational resilience. This helps staff to begin acculturation to the organization's philosophy on operational resilience as they become part of the organization.

The management of staff performance is a means by which the organization can enforce (and reinforce) its philosophy of operational resilience. In Human Resource Management, the organization reinforces the connection between staff and operational resilience by using the performance management program as a way to acculturate staff to their resilience roles and responsibilities. Job descriptions include these roles and responsibilities, which are enforced by the organization by their inclusion in annual goal setting. The organization specifically establishes acceptable performance behaviors and measures compliance with these behaviors on a regular basis as part of the performance management cycle. As a result, the organization inculcates a resilience-aware and -ready culture that is essential for supporting the resilience process and the organizational mission.

Human Resource Management also seeks to ensure that the organization's human resources do not pose additional operational risk to the organization when their employment is voluntarily or involuntarily severed. Changes in employment can have significant effects on operational resilience by potentially disrupting the contributions of staff to the productive capacity of services. In addition, because staff typically have other organizational assets in their possession, when they vacate their positions, the repossession of these assets by the organization may be critical to operational resilience, particularly if sensitive information assets or technology assets are not returned. Finally, involuntary separations may be disruptive—they can affect services and the morale and motivation of remaining staff. Thus, the organization must act in a way that minimizes the impact of involuntary terminations and limits unpredictable effects on productive capacity.

The Human Resource Management competency covers the employment life cycle—hiring, performance management, and termination. It has four specific goals addressing the

identification of skill requirements, the acquisition of appropriate staff, the management of staff performance in supporting operational resilience, and the termination of staff in a manner that minimizes organizational impact.

As people are a ubiquitous resource in an organization, there are many aspects of human resources that affect operational resilience. *People Management is focused on the availability of people to the services that they support. The management of people through their employment life cycle and the effect on operational resilience are addressed in the Human Resource Management competency. Finally, promoting awareness of the organization's efforts and providing training to resilience staff for their roles in managing operational resilience are addressed in the Organizational Training and Awareness competency.*

Related Process Areas

The training of staff to meet resilience requirements, needs, and gaps is established and managed in the Organizational Training and Awareness process area.

Determining funding needs for providing human resources to the operational resilience management system is addressed in the Financial Resource Management process area.

The management of operational risks through their life cycle is addressed in the Risk Management process area.

The specific activities involved in cross-training and succession planning as a means for improving and sustaining resilience are addressed in the People Management process area.

The management of intellectual property and knowledge as high-value organizational information assets is addressed in the Knowledge and Information Management process area.

Managing access to organizational assets on a recurring basis is addressed in the Access Management process area.

Summary of Specific Goals and Practices

Goals	Practices
HRM:SG1 Establish Resource Needs	HRM:SG1.SP1 Establish Baseline Competencies
	HRM:SG1.SP2 Inventory Skills and Identify Gaps
	HRM:SG1.SP3 Address Skill Deficiencies
HRM:SG2 Manage Staff Acquisition	HRM:SG2.SP1 Verify Suitability of Candidate Staff
	HRM:SG2.SP2 Establish Terms and Conditions of Employment
HRM:SG3 Manage Staff Performance	HRM:SG3.SP1 Establish Resilience as a Job Responsibility
	HRM:SG3.SP2 Establish Resilience Performance Goals and Objectives
	HRM:SG3.SP3 Measure and Assess Performance
	HRM:SG3.SP4 Establish Disciplinary Process
HRM:SG4 Manage Changes to Employment Status	HRM:SG4.SP1 Manage Impact of Position Changes
	HRM:SG4.SP2 Manage Access to Assets
	HRM:SG4.SP3 Manage Involuntary Terminations

Specific Practices by Goal

HRM:SG1 Establish Resource Needs

The resource needs to staff the activities and tasks of the organization's resilience program and plan are identified and satisfied.

Skilled people are absolutely essential to successfully managing operational resilience and meeting the objectives of the organization's resilience program. This is particularly true for staff who are actively engaged in all aspects of resilience work—performing security duties, supporting business continuity activities, and managing IT operations—because these skill sets are typically in short supply.

In order to determine what skills the organization must possess to meet its resilience needs, baseline competencies must be established relative to the resilience program and plan to ensure the entire range of necessary skills is identified. Against this baseline, the organization must determine what skills it currently possesses in its pool of available human resources and identify skill gaps that not only can affect its ability to manage operational resilience but can pose additional risk to the organization in meeting its strategic objectives.

In establishing resource needs, the organization determines its baseline competencies, takes an inventory of its current skill sets (based on available resources), identifies gaps and related risks, and develops and implements a strategy for closing these gaps and reducing risk to an acceptable level.

The specific practices in this goal are intended for application to positions that have resilience as their primary responsibility. However, these practices can apply universally to all positions in the organization, particularly vital positions.

HRM:SG1.SP1 Establish Baseline Competencies

The staffing and skill needs relative to the operational resilience management system are established.

The baseline competencies represent the staffing and skill set needs relative to carrying out the organization's resilience program and plan. These staffing and skill set needs may be concentrated in resilience staff (i.e., with staff members whose traditional positions are in the fields of security or business continuity) and may also be found in positions in the operational and business units of the organization where resilience tasks are often performed.

Baseline competencies can be gathered through detailed examination of the organization's resilience program and plan, as well as through review of job descriptions that the organization has developed for resilience positions. In the event that the organization has not developed job descriptions, gathering baseline competencies may be more difficult and may require an inventory of resilience positions from which a foundation for developing more extensive baselines can be created. The baseline competencies should be based on what the organization needs, not what it currently has in terms of staff and skills. By determining what the organization needs, the appropriate target for a sufficient level of staffing and skills is established.

An organization may want to expand this activity to include vital positions in the organization. In this way, the organization establishes a baseline for the skills necessary to meet organizational goals and strategic objectives. If gaps in these skills exist, the risk that strategic objectives will not be achieved is increased, and the operational resilience of associated services is impacted.

Because skilled labor is a significant component of the costs of providing resilience services, the establishment of baseline competencies can aid the organization in determining and validating funding needs for the operational resilience management system. *(Determining funding needs is performed in FRM:SG2.SP1 in the Financial Resource Management competency.)*

Typical work products

1. Baseline competencies
2. Job descriptions

Subpractices

1. Establish and document baseline competencies necessary to meet the needs of the organization's operational resilience management system.

   Baseline competencies may be as detailed as the organization needs to describe its required skill sets. This may involve many layers of information, including

   - role (security administrator, network administrator, CIO, etc.)
   - position (CIO, senior security analyst, network engineer, etc.)
   - skills (Java programming, Oracle DBA, etc.)
   - certifications (CISSP, MSCE, etc.)
   - aptitudes and job requirements (able to work long hours, travel, or be on call)

2. Create or update job descriptions to reflect baseline competencies.

   Baseline competencies should be reflected in job descriptions to ensure that the needs of the organization are translated into skilled positions. In some cases, existing job descriptions may be a means for collecting baseline competencies, but there may be cases where job descriptions do not exist even though there are documented skill needs for the operational resilience management program.

HRM:SG1.SP2 Inventory Skills and Identify Gaps

The current skill set for operational resilience management is inventoried and gaps in necessary skills are identified.

A skills inventory is a means for identifying and documenting the current skill set of the organization's human resources. This inventory provides a snapshot of the organization's current capabilities and can be used to diagnose resource shortages and gaps based on the organization's needs as represented in the baseline competencies.

A skills inventory is not a job inventory; it does not represent the positions that the organization currently has deployed on its organization chart. Instead, a skills inventory captures the skills and aptitudes of the current pool of human resources regardless of their job position or roles and

responsibilities. The skills inventory provides a collective view of the organization's capabilities, which in some cases may be more extensive than the positions currently employed by the organization. For example, there may be staff members who speak more than one language but are not using that skill in their current positions.

Taking a skills inventory gives the organization a true picture of its current competencies from which critical analysis and review of needs can be performed. It may also reveal that staff members have skills that are needed by the organization that were not previously known.

Typically, a skills inventory is self-reported—that is, skills are reported by staff to the organization—which means that the organization may have to do some validation of these skill sets.

The skills inventory is compared to the organization's baseline competencies in an attempt to identify skills that the organization does not possess. The resulting skill gap provides insight into the skill needs of the organization. These skills may be keeping the organization from performing adequately in managing operational resilience and may result in additional risk to the organization. When the skills inventory is expanded beyond resilience positions, skill gaps may indicate areas of risk that result in potentially diminished operational resilience.

Typical work products

1. Skills inventory
2. Identified skill gaps

Subpractices

1. Develop a skills inventory, particularly relative to resilience skills.

   The skills inventory should contain at a minimum relevant skills, certifications, and aptitudes that staff members currently possess. The organization should concentrate on resilience skills; however, if the organization intends to use the inventory for other process improvement purposes, it may expand the inventory to other skills for vital positions.

   The skills inventory is typically taken by survey. However, this requires that the organization structure the survey in a way that will yield specific skills information. For example, rather than asking whether staff members have skills in programming languages, the organization may want to ask if they have skills in Java or other specific languages that are relevant. In addition, the organization may need to validate the skills survey. Certifications, as well as aptitude testing, may be ways to validate that the staff member possesses the required skills.

2. Compare baseline competencies to the current skills inventory.
3. Identify skill gaps and deficiencies.

   Skill gaps and deficiencies expose the areas where the organization does not have the expertise, aptitude, skill, or experience to meet current needs. These gaps can result in risks to the organization in that significant resilience activities may not be performed appropriately or may not be performed at all.

4. Develop processes for keeping the skills inventory current and for performing regular comparison to baseline competencies.

   As operational complexity changes, so do the organization's needs and the skill sets available to meet these needs. Keeping the skills inventory current allows the organization to perform frequent comparisons so that gaps can be identified before they result in risk to the organization.

HRM:SG1.SP3 Address Skill Deficiencies

Gaps in skills necessary to meet operational resilience management needs are addressed.

Deficiencies in skills may impede the organization's ability to adequately manage operational resilience. These deficiencies pose risk to the organization that must be addressed.

Addressing these deficiencies comes at a cost to the organization. However, through identification, the organization has an opportunity to perform analysis on these gaps (i.e., determining the risk versus reward of closing the gaps based on the relative cost) and make sound decisions about how to address them. An organization can address skill deficiencies in a number of ways:

- Existing staff may be trained to acquire new skills.
- New staff may be hired to acquire the necessary skills.
- The skills may be acquired by outsourcing the work that requires them.
- Jobs may be restructured to take advantage of newly identified skills that were not previously known by the organization.

Skill gaps may require the organization to recast existing positions and create new positions with higher level skill requirements. These positions may have to be "priced," and in some cases, existing staff members may have to be promoted (based upon proper training) into these jobs.

If the skill deficiencies pose risks to the organization, these risks should be referred to the organization's risk management process for analysis and resolution, particularly if the organization does not intend to address the existing gaps.

The management of operational risks through their life cycle is addressed in the Risk Management process area.

Training may be required to fill gaps in skills. *(Processes for providing training to resilience staff are addressed in the Organizational Training and Awareness process area.)*

Typical work products

1. Strategy for obtaining needed skills
2. Training plans
3. Job requisitions
4. Outsourcing agreements
5. Identification of related risks that must be addressed

Subpractices

1. Develop a strategy for addressing skill gaps.

   The organization should develop a strategy for addressing skill gaps based on the comparison process. The strategy should seek to fill the skill gaps at the lowest possible cost to the organization. Each skill gap should have a documented disposition for how the organization intends to obtain the necessary skills or a determination that the organization does not intend to address the skill gap.

   For those gaps that the organization consciously does not intend to close, resultant risks should be identified and referred to the risk management process.

2. Update job descriptions to incorporate missing skills as necessary.

   Job descriptions should be updated if missing skills have been identified and should be included as part of existing positions. This will provide a basis from which job restructuring can be performed and may result in new or updated job descriptions.

3. Develop job requisitions for unfilled positions.

   For positions that must be hired to acquire skills, the organization should develop appropriate job descriptions and document job requisitions as necessary.

   For skills that can be acquired through outsourcing, the organization should develop proposals that document the skill requirements.

4. Develop training plans for skills that can be obtained by existing staff.

   The development of training plans is addressed in the Organizational Training and Awareness process area.

5. Refer resulting risks to the risk management process for disposition.

HRM:SG2 Manage Staff Acquisition

The acquisition of staff to meet operational needs is performed with consideration of the organization's resilience objectives.

The processes that the organization uses to acquire staff can result in exposing the organization to additional operational risk. The organization must verify that candidate staff have the appropriate skills, credentials, and background to ensure that their employment will not adversely affect operational capacity and resilience. In addition, the organization must institute contractual instruments that protect the organization's interests before, during, and after staff are employed by the organization. Proactively, these actions reduce the potential that staff acquisition will result in additional operational risks and provide a foundation from which newly acquired staff can support and contribute to the organization's efforts to manage operational resilience.

The specific practices in this goal apply universally to all staff who are acquired for positions in the organization. However, for positions that directly support the organization's resilience program and objectives, these practices may be expanded to include specific requirements for credentials and employment agreements. These practices may also apply to staff who are acquired through outsourcing arrangements.

HRM:SG2.SP1 Verify Suitability of Candidate Staff

Candidate staff are evaluated for suitability against position requirements and risks.

Verifying the suitability of candidate staff prior to their employment is a vital risk management activity. Whenever new staff members join an organization, they potentially present risk—they may fail to meet critical requirements for the position, resulting in poor operational performance, or they may pose unacceptable risk based on their prior experience, behavior, or other criteria. Candidates who pose unacceptable risk or who fail to meet certain criteria should be hired with caution and an explicit consideration of potential risks to operational resilience.

Pre-employment verification actions may include interviewing, performing reference checks, or other forms of screening. The actions taken to verify the suitability of candidate staff must be completed consistently, ethically, with an appropriate level of rigor, in accordance with applicable laws or regulations, and in proportion to the risk associated with the position. Data collected on candidate staff should be handled with an appropriate level of confidentiality.

Typical work products

1. Documented verification procedures and guidelines
2. Documented screening criteria
3. Verification data

Subpractices

1. Establish baseline verification criteria that apply to all positions in the organization.

   Baseline verification criteria are developed that apply to all positions in the organization. For very large organizations, there may be multiple baselines, each of which would apply to a large specific segment of the population.

   The baseline verification criteria should reflect the general resilience obligations expected of all staff members in the organization. In addition, the verification criteria must be set in compliance with all applicable privacy, employment, and other laws and regulations, organizational policies, and collective bargaining agreements.

   Baseline verification criteria should include

   - confirmation of identity
   - character references, both professional and personal
   - accuracy of résumé or curriculum vitae, including employment history, academic achievements, and professional qualifications
   - credit checks
   - criminal and/or court record checks
   - specific regulatory screening requirements, such as pre-employment drug testing

   Baseline verification criteria should be documented, included in job descriptions, and maintained in accordance with the organization's human resources policies and practices.

2. Establish job-specific verification criteria that apply to vital positions.

   Baseline requirements are supplemented with additional verification requirements for particular positions and vital staff. For example, the baseline requirements may be more extensive for positions that directly affect the organization's operational resilience (such as security positions and business continuity staff).

   For vital positions, additional attention should be given to ensure that specific requirements (including any additional resilience obligations) are appropriate to the circumstances of the position and that they are sufficient, given the risks associated with the position.

   Specific verification criteria should include

   - security clearances or other federal credentials
   - specific certifications or accreditations required by the position (such as CISSP, CBCP, CISA, and CPA)
   - certain physical requirements
   - citizenship requirements (which may preclude employment in some positions)
   - legal requirements

   The additional verification criteria should be documented, included in job descriptions, and maintained in accordance with the organization's human resources policies and practices.

3. Establish verification program and procedures.

   A program is established and managed for performing the background verification checks on employment candidates. The program should include the design and documentation of procedures and the allocation and authorization of staff to perform the verification screening.

   Verification procedures should address

   - how and when verification checks are to be carried out
   - storage of the data collected during the procedures
   - handling of notifications of screening results, both within the organization and to the candidate
   - whether the candidate should be informed of the screening beforehand
   - compliance with any applicable rules, regulations, organizational policies, laws, collective bargaining agreements, or other requirements
   - variations of the verification process for contract, temporary, or other external entity staff

   Staff who are responsible for the verification procedures should be identified and given the necessary tools, resources, training, and authority to carry out the verification process.

4. Review and revise verification criteria and program as required.

   The verification criteria, program, and procedures should be reviewed and revised on a regular basis or as required to address changes in the resilience requirements for staff.

HRM:SG2.SP2 Establish Terms and Conditions of Employment

Employment agreements appropriate for the position and role are developed and executed.

Many positions in the organization require extraordinary levels of responsibility and trust. While these positions are needed by the organization to meet its strategic objectives, they can also expose the organization to risk, particularly when the staff who occupy these positions leave the organization. For this reason, the organization should establish baseline terms and conditions for all positions and document these terms and conditions in job descriptions.

Situations under which specific terms and conditions should be considered include positions that

- require high levels of trust and authority
- require confidential handling of knowledge and experience (trade secrets and intellectual property) gained during tenure with the organization
- provide access to information that could result in consequences to the organization if disclosed, including information that could result in direct impact on the life, safety, and health of staff and customers
- require privileged access to organizational facilities or organizational systems, networks, and other technical infrastructure components

Terms and conditions must often be enforced through employment agreements or similar constructs, executed before the candidate begins employment. Typically, these agreements include confidentiality and non-disclosure agreements and non-compete agreements, but the organization may have various other constructs at its disposal, so long as enforcement would survive legal challenges.

The management of intellectual property and knowledge as a high-value organizational information asset is addressed in the Knowledge and Information Management process area.

Typical work products

1. Job descriptions
2. Criteria for terms and conditions of employment
3. (Signed) employment agreements

Subpractices

1. Establish baseline terms and conditions of employment that apply to all positions in the organization.

   Baseline terms and conditions of employment are established that apply to all positions in the organization. For very large organizations, there may be multiple baselines, each of which would apply to a large specific segment of the population.

   The baseline terms and conditions of employment should reflect the resilience obligations of the position. In addition, the terms and conditions must be set in

compliance with all applicable laws and regulations, organizational policies, and collective bargaining agreements.

These are areas to consider when establishing the terms and conditions of employment:

- the level of confidentiality and sensitivity of information that the candidate will require in a specific position
- the organization's resilience policies and the organization's right to amend such policies
- the organization's obligation for handling the staff member's personal information
- any legal requirements with which staff are required to comply
- the organization's policies on copyrights, trademarks, patents, and other intellectual property ownership issues
- any obligations to report risks or threats
- codes of ethics or codes of conduct that are required
- conflict of interest or conflict of influence requirements, including notification and disclosure procedures and requirements
- responsibilities that extend beyond the organization's premises or outside of normal working hours
- agreements to changes in duties as a result of or during events
- rights, actions, and procedures that will be followed in the event that the staff member fails to comply with the terms and conditions of employment

Baseline terms and conditions of employment should be documented, associated with job descriptions, and maintained in accordance with the organization's human resources policies and practices.

2. Ensure that terms and conditions are clearly documented in job descriptions.

3. Execute agreements as necessary to enforce employment terms and conditions.

   In conjunction with an offer for employment, candidate staff should be made aware of all terms and conditions of employment in writing. As part of the offer acceptance, candidate staff should be required to execute agreements to indicate their acknowledgment of and agreement to all terms and conditions of employment.

   It is appropriate and necessary for certain terms and conditions, such as non-disclosure requirements, to continue for a defined period of time after employment ends.

HRM:SG3 Manage Staff Performance

The performance of staff to support the organization's resilience program is managed.

The active management of staff helps to ensure their availability, productivity, and contribution to high-value services throughout their employment life cycle. By actively managing staff for resilience, the organization maintains staff awareness of and focus on resilience roles and responsibilities, equips them with the resources, skills, and

abilities to perform resilience functions, and reduces the risk of human actions (erroneous and otherwise) that may cause harm to the organization's resilience.

A primary component of effective performance management is to maintain a continual dialogue between manager and staff member about work performance. Incorporating resilience roles, responsibilities, and functions into the dialogue is an effective way to emphasize the individual's contributions to managing and sustaining the organization's operational resilience. Performance appraisals that emphasize resilience objectives provide a regular checkpoint to document performance against these objectives and to gather data for improvement if necessary.

In this goal, it is assumed that the organization has an established performance management process (or practices) into which resilience measures and controls can be inserted. To establish resilience as a performance management target, the organization must first establish resilience as a job responsibility, establish resilience goals and objectives, measure performance against these objectives, and implement processes to correct behavior when necessary.

HRM:SG3.SP1 Establish Resilience as a Job Responsibility

Resilience obligations for staff are communicated, agreed to, and documented as conditions of employment.

Resilience obligations should be clearly documented in job descriptions so that staff members know their responsibilities and can plan their performance accordingly. The definition of resilience obligations in the job description establishes the foundation for performance management and measurement of the staff member's commitment to helping the organization sustain operational resilience.

When hiring staff, it is also important that resilience obligations be documented as part of the terms and conditions of employment. When employment is offered to a candidate, it should be offered subject to the candidate's understanding of resilience obligations and other terms and conditions of employment. The organization and the candidate should execute contractual agreements to signify agreement and commitment to the terms and conditions of employment.

Typical work products

1. Job descriptions

Subpractices

1. Insert resilience obligations into job descriptions.

   All job descriptions in the organization, particularly those with vital roles, should clearly state the candidate's or staff member's resilience roles, responsibilities, and job tasks.

2. Ensure that job descriptions and resilience requirements are communicated to candidate staff prior to employment.

   Candidate staff should be provided with written job descriptions that document the resilience requirements and obligations for the position.

HRM:SG3.SP2 Establish Resilience Performance Goals and Objectives

Goals and objectives for supporting the organization's resilience program are established as part of the performance management process.

Goals and objectives are a key administrative control for managing the resilience contributions of the organization's staff. Goals and objectives provide time-sensitive focal points and a solid framework for managing the resilience roles, responsibilities, and functions of staff. Additionally, they reinforce the expectation that staff will behave in compliance with organizational resilience policies and avoid actions, activities, and behaviors that expose the organization to risk.

To effectively use goals and objectives to support resilience, the organization should ensure that goals and objectives are established and reviewed on a regular basis, are maintained and updated in writing, and include behavioral and functional targets for resilience. Communicating about and developing resilience goals and objectives in collaboration with staff provide a strong cultural reinforcement of the importance of the organization's resilience posture and practices.

From a practical standpoint, resilience goals and objectives may specifically include security goals, business continuity goals, information (or other asset) protection goals, and other objectives related to appropriate behaviors and activities in support of the organization's resilience posture and program.

The resilience goals and objectives addressed in this specific practice are intended to be applied generally to all relevant staff members in the organization. However, for staff whose job responsibilities are directly focused on managing operational resilience (such as security managers and business continuity planners), a more specific and extensive set of resilience goals and objectives would be developed for performance management purposes.

Typical work products

1. Resilience goals and objectives

Subpractices

1. Review resilience obligations, roles, and responsibilities of the position as the basis for establishing resilience goals and objectives.

   Managers should review the resilience obligations for the position when establishing goals and objectives for a specific person. The relevant resilience requirements of the services and assets under the manager's and the staff member's control should also be established as a basis for direct goals and objectives related to resilience.

   This review provides an opportunity for updating the resilience obligations in job descriptions.

2. Formalize and establish resilience goals and objectives in writing.

Resilience goals and objectives are established in writing on a regular basis as part of the organization's performance management process. These goals and objectives should align with

- the organization's philosophy on operational resilience
- the objectives of the organization's resilience plan and program
- the relevant resilience requirements in the staff member's organizational unit or line of business (for assets and services under the staff member's ownership and control)
- the resilience obligations as documented in the staff member's job description

Resilience goals and objectives should be specific, measurable, relevant, and timely.

Resilience goals and objectives may include specific targets, behaviors, or measures that contribute to the organization's ability to manage operational resilience, such as

- development, implementation, and enforcement of resilience requirements for assets and services under the staff member's control
- compliance with organizational security policies
- adherence to IT best practices or guidelines
- awareness of resilience issues and demonstration of appropriate resilience behaviors
- appropriate handling of sensitive information
- work practices associated with accessing information, technology, and facilities
- maintaining good password hygiene
- maintenance of necessary skills and qualifications
- providing resilience leadership
- demonstrating readiness for resilience events or incidents

3. Ensure that the staff members understand resilience goals and objectives.

HRM:SG3.SP3 Measure and Assess Performance

Performance against goals and objectives is measured, achievements are acknowledged, and corrective actions are identified and communicated.

Measuring performance and providing feedback against established resilience goals and objectives and the organization's resilience policies are important mechanisms for encouraging acceptable behaviors. Performance metrics should be collected throughout a staff member's tenure, and feedback should be provided to the staff member on a regular basis.

Communication about performance should be a regular part of the dialogue between staff members and their managers and should be the focus of regular, documented performance appraisals. Including resilience topics in such dialogues is a means to promote awareness of and encourage resilience contributions.

Data collection and communications about staff members' performance should be performed in compliance with organizational policies, applicable regulations, and applicable collective bargaining agreements.

Typical work products

1. Performance evaluations
2. Recommendations for improvement
3. Revised resilience goals and objectives

Subpractices

1. Measure performance against resilience goals and objectives.

   Data should be collected throughout the goals and objectives period on the performance of staff against resilience goals and objectives. Additionally, any violations of the organization's resilience policies, as well as any exemplary resilience behaviors or accomplishments, should be noted.

2. Conduct performance evaluations.

   Performance feedback should be part of the routine dialogue between managers and staff. Formal performance evaluations should be conducted according to the organization's standard practices and schedule. The evaluations should include feedback on the achievement of resilience goals and objectives, any violations of the organization's resilience policies, any behaviors or actions that expose the organization to risk, and any exemplary behaviors or achievements related to resilience.

   Performance evaluations should be documented in writing.

3. Acknowledge performance achievements as appropriate.

   Private and public acknowledgment of resilience performance achievements can have a powerful effect on creating and reinforcing a culture of resilience.

4. Identify improvement opportunities and take corrective actions as necessary.

   Performance feedback conversations and the performance review in particular are opportunities to design and implement improvement plans or to take corrective actions for staff members as appropriate. Improvement plans are appropriate to address deficiencies in performance as well as to facilitate learning so that additional resilience roles and responsibilities can be assigned.

   Corrective actions should be taken whenever staff members violate policies or otherwise behave in a manner that creates risk for the organization.

5. Revise goals and objectives as needed.

   Goals and objectives should be revised as a routine part of the performance conversation and in consideration of the organization's operational environment.

HRM:SG3.SP4 Establish Disciplinary Process

A disciplinary process is established for staff who violate resilience policies.

A disciplinary process is an essential administrative control for enforcing organizational resilience policies. Awareness of the disciplinary process provides staff an additional incentive to comply with the organization's resilience policies and ensures fair and appropriate treatment in the event

that wrongdoing is suspected. From the organization's perspective, a formalized disciplinary process provides a preplanned response to suspected resilience infractions that is designed to address all relevant concerns while protecting the organization to the fullest extent possible on all fronts.

The disciplinary process should be formalized and documented. It should ensure fair treatment of staff in compliance with all applicable regulations and agreements, protect the organization's interests, and include a range of acceptable responses that correspond to the seriousness of the infraction.

Investigation of resilience or security breaches is a critical first step of the formalized disciplinary process.

Typical work products

1. Investigation reports
2. Relevant documentation of disciplinary action

Subpractices

1. Establish an investigation process.

   An investigation process should be established to collect and review information (or evidence) whenever a staff member is suspected (or known) to have committed a breach of resilience policies or practices or to have otherwise performed in a manner that creates risk for the organization.

2. Establish a disciplinary process.

   Most organizations have disciplinary processes that address violations of the organization's policies and procedures. However, because violations of resilience policies can result in additional risk to the organization, it is imperative that the disciplinary process specifically address resilience infractions.

   The disciplinary process should provide for graduated response depending on the severity of the infraction as well as the staff member's role in the organization, tenure and level of training, and whether previous offenses have been documented. The process should comply with all relevant legal and regulatory bodies and should make provisions for coordination with public authorities, depending on the severity of the infraction. *(Some infractions may have to be managed through the organization's incident management processes, as described in the Incident Management and Control process area.)*

3. Revise the disciplinary process as needed.

   Revisions to the disciplinary process may be needed in response to changes in organizational policy, regulatory or compliance obligations, collective bargaining agreements, or contracts. It may also be appropriate to revise the process to incorporate lessons learned from experience in executing the process.

HRM:SG4 Manage Changes to Employment Status

Changes in the employment status of staff members in the organization are managed.

There are specific risks that the organization must address relating to changes in the employment status of staff members. For example, when staff *voluntarily* terminate their employment (either to leave the organization or to change positions within the organization), the organization must be able to cover their roles and responsibilities, manage their access to high-value organizational assets, and manage the impact of their departure on the operational environment, including the effects on remaining staff.

When staff leave the organization *involuntarily*, additional risks are presented. In addition to covering the vacated roles and responsibilities, the organization must manage the termination in a way that minimizes operational impact and retains the organization's assets in their intended form and function to the extent possible (information, technology, or facilities are not destroyed, etc.). Assets in the possession of the terminated staff member, particularly information and technology assets, must be collected as well so that the potential effect on services that rely on those assets is minimized.

To manage the effects of employment changes on the organization's operational resilience, the organization must manage the impact of position changes, manage possession of organizational assets, and address the unique challenges and threats posed by involuntary separation and termination.

HRM:SG4.SP1 Manage Impact of Position Changes

Administrative controls are established to sustain functions, obligations, and vital roles upon position changes or terminations.

When a staff member vacates a job (either through job change or voluntary or involuntary termination), one of the primary concerns for the organization is to sustain any resilience functions, obligations, or roles for which the person was responsible. This can be accomplished through reassignment of functions and roles to others and through reinforcement of obligations that persist beyond the period of employment.

Reassignment of resilience roles and functions to others should take place as soon as possible upon termination (or in advance of termination where possible) to ensure sustained coverage for the organization. Whenever possible, resilience roles and functions for the position being vacated should be reviewed with the person leaving to ensure that all such roles and functions are identified for reassignment.

Certain resilience obligations, such as confidentiality of information, trade secrets, and intellectual property, will persist beyond the period of employment for a defined length of time. Any such obligations should have been established upon hiring. When a position is vacated, it is prudent to review the obligations to ensure renewed or continued awareness on the part of the departing staff member.

Typical work products

1. Exit interview notes

2. Plan for sustaining roles and responsibilities
3. Executed confidentiality agreements
4. Executed non-compete agreements

Subpractices

1. Establish and execute an exit interview process.

   An exit interview process should be established. Exit interviews should be held with all persons who voluntarily leave a position, whether they are separating from the organization or taking another position within the organization.

   Topics addressed in the exit interview should include

   - any specific resilience roles and functions that are or have been performed by the departing person (This information is useful to confirm the job description and to enable the reassignment of the roles and functions.)
   - review of any obligations that persist beyond the period of employment (or period in the position), such as confidentiality provisions
   - inventory of organizational assets in the possession of the departing person and coordination of their return *(see PM:SG3.SP2)*, including badges, data, and mobile devices
   - elicitation and review of knowledge held by the departing person that may be vital to the organization and that may not be documented or otherwise available to the organization *(The management of knowledge is addressed in the Knowledge and Information Management process area.)*

2. Develop a plan for reassignment of roles and responsibilities.

   To the extent possible, the organization should have developed a plan for the reassignment of roles and responsibilities for vital positions and staff in advance of voluntary or involuntary separation. This plan may include various strategies such as job sharing, outsourcing, cross-training, and succession planning, depending on the importance of the job position and role in the organization. The plan should be able to be executed in advance of a voluntary separation to ensure a smooth transition with minimal impact on resilience or immediately upon involuntary separation. For staff whose roles and responsibilities are directly focused on resilience activities, particularly those who have “superuser” or other privileged or trusted status, these plans are absolutely essential.

   The specific activities involved in cross-training and succession planning as a means for improving and sustaining resilience are addressed in the People Management process area.

3. Reassign resilience roles and functions upon a staff member’s departure from a position.

4. Review and confirm understanding of confidentiality agreements and obtain assurances for compliance.

   For staff in roles that require ongoing considerations of confidentiality and non-compete clauses that extend beyond their current employment, the organization must establish that separated staff understand their responsibilities and agree to be bound by them. Departing staff members should be reminded of their agreements and the terms of the agreements should be reiterated to ensure understanding. The

organization should also clearly explain the potential consequences of violating these agreements.

HRM:SG4.SP2 Manage Access to Assets

Access to and possession of organizational assets relative to position changes is managed.

When staff members vacate their positions, they are typically in possession of important organizational assets—information (usually in the form of organizational procedures, policies and manuals, trade secrets, customer data, and intellectual property) and technology (cell phones, PDAs, personal computers, etc.). These assets can be tangible (such as paper reports) or intangible (such as access to the customer information database). In addition, staff possess organizational credentials—ID cards, access cards, parking passes, etc.—that provide them access to these organizational assets, including facilities where they once worked. Access to these assets, including credentials, must be managed in order to limit potential effects on the organization when staff members vacate their positions. This is particularly true when a staff member's separation is involuntary.

For staff who are in resilience positions or who have privileged or trusted access to assets, managing access to and possession of these assets is extremely important for preventing potential disruptions or effects on operational resilience.

The processes for managing access to organizational assets on a day-to-day basis are addressed in the Access Management process area.

Typical work products

1. Asset inventory checklist
2. Asset inventory sign-off
3. Request for changes to access privileges
4. Verification of access changes

Subpractices

1. Secure the return of all organizational assets, property, and information upon a staff member's departure.

   Procedures should be put in place to ensure that all of the organizational assets, property, and information in the possession of a staff member are returned when the staff member leaves the organization. For staff members who voluntarily separate from the organization, this process should be performed in advance of their separation date. For involuntarily separations, this process should be performed without advance notice immediately upon separation.

   These are examples of organizational assets that should be returned upon departure:

   - software
   - identification badges and access cards

- computing and communications devices and hardware (including personal computers, PDAs, cell phones, mobile email devices, pagers, and job-specific tools and equipment such as meter-reading devices)
- corporate documents (such as policy and procedures manuals, customer lists, and other proprietary documents)
- notes and documents that contain organizational information (trade secrets, intellectual property, customer contracts)
- tools and other equipment
- credit cards
- electronic media
- information, in any form (paper, electronic), including intellectual property

In cases where staff members use their own computing equipment or media or are allowed to purchase corporate equipment in their possession, procedures should be in place to retrieve organizational information and/or software from such equipment and to securely erase corporate information or software from any such media.

In many organizations the return of assets is coordinated as part of the exit review process *(see HRM:SG4.SP1)*.

2. Inventory all organizational assets, property, and information in possession of staff upon position changes, and make necessary adjustments.

3. Discontinue all access to organizational assets upon termination or position changes.

   Access rights to all organizational assets, including facilities, technology, and information, should be discontinued upon termination. *(Access privileges and controls are addressed in the Access Management process area.)*

HRM:SG4.SP3 Manage Involuntary Terminations

Administrative controls and procedures are established to manage the effects of involuntary terminations.

Certain terminations are involuntary—typically related to job performance or a violation of company policy, rules, or regulations. Special controls and procedures must be established to address and manage the potential impacts on the organization in these cases.

When terminations are involuntary, staff may exhibit a range of behaviors from introspection to aggressiveness. In many cases, there is increased risk of impact on the organization, either directly and immediately (such as causing damage to organizational assets) or after termination (such as causing reputation damage or by exposing confidential information). To the extent possible, the organization must act to minimize impact through proactive actions that occur before termination and through resilience practices that allow the organization to swiftly address issues and ensure affected services are sustained.

Typical work products

1. Criteria for involuntary terminations

2. Procedures for managing involuntary terminations

Subpractices

1. Establish criteria for determining potential risks related to involuntary terminations.

   Because the effects of involuntary terminations can be unpredictable, criteria should be established for advance consideration of possible effects. This helps the organization to predetermine the type and extent of response necessary during the termination process and the immediate aftereffects.

   These are examples of criteria that should be considered with involuntary terminations:

   - Employee (or consultant) is disgruntled or is considered to be psychologically unstable.
   - Employee (or consultant) has committed serious violations of organizational policies or is under suspicion for such violations.
   - Employee (or consultant) has been charged with or convicted of a felony offense under the law.
   - Employee (or consultant) has exhibited violent behaviors or tendencies.

2. Establish procedures for managing involuntary terminations.

   Procedures should be established for managing involuntary terminations. Ideally, these procedures should be implemented in advance of termination activities so that the impact of the termination and the potential effects are minimized.

   These are examples of procedures that may be appropriate in involuntary terminations:

   - cessation of access privileges prior to or precisely concurrent with announcing an involuntary termination
   - escort from the organization's premises
   - coordination with public law enforcement authorities
   - identification, isolation, and review of systems or information that may have been compromised by the employee

Elaborated Generic Practices by Goal

Refer to the Generic Goals and Practices document in Appendix A for general guidance that applies to all process areas. This section provides elaborations relative to the application of the Generic Goals and Practices to the Human Resource Management process area.

HRM:GG1 Achieve Specific Goals

The operational resilience management system supports and enables achievement of the specific goals of the Human Resource Management process area by transforming identifiable input work products to produce identifiable output work products.

HRM:GG1.GP1 Perform Specific Practices

Perform the specific practices of the Human Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices HRM:SG1.SP1 through HRM:SG4.SP3 are performed to achieve the goals of the human resource management process.

HRM:GG2 Institutionalize a Managed Process

Human resource management is institutionalized as a managed process.

HRM:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the human resource management process.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the human resource management process.

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the human resource management process may be exhibited by

   - developing and publicizing higher level managers' objectives and requirements for the process
   - establishing a higher level position, such as the director of human resources or the equivalent, responsible for the resilience of the organization's human resources
   - establishing oversight over the verification, acquisition, management, and termination of human resources, including terms and conditions of employment, confidentiality agreements, and the plan for sustaining and reassigning roles and responsibilities for vital positions
   - establishing acceptable performance behaviors to build a resilience-aware and -ready culture, and establishing measures that demonstrate compliance with these behaviors
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for the acceptable performance of human resources, the disciplinary process for non-compliance with policy, and establishing personal ownership and responsibility for resilience
   - providing oversight over the establishment, implementation, and maintenance of the organization's internal control system for human resources

- making higher level managers aware of applicable laws, compliance obligations, collective bargaining agreements, and contracts related to human resources, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- sponsoring and funding process activities
- providing guidance for identifying skill requirements and suitability of candidates to meet resilience objectives, including the identification of vital positions
- regular reporting from organizational units to higher level managers on process activities and results
- creating dedicated higher level management feedback loops on decisions about the process and recommendations for improving the process
- providing input on identifying, assessing, and managing operational risks related to human resources, particularly when managing changes to employment status (e.g., investigation, disciplinary action, layoff, and termination)
- conducting regular internal and external audits and related reporting to appropriate committees on human resource controls and the effectiveness of the process
- creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The human resource management policy should address

- responsibility, authority, and ownership for performing process activities
- acceptable performance of human resources with respect to operational resilience management, including establishing personal ownership and responsibility for resilience
- disciplinary action and termination
- procedures, standards, and guidelines for
  - describing and identifying baseline competencies for resilience staff
  - documenting descriptions, resilience roles, and skills needed for roles
  - criteria for screening and determining suitability of candidates for sensitive positions
  - terms and conditions of employment
  - managing operational risks resulting from human resources
  - sustaining and reassigning vital roles and responsibilities
  - managing the impact of changes to employment status
  - establishing, implementing, and maintaining an internal control system for human resources
- methods for measuring adherence to policy, exceptions granted, policy violations, and for the investigation and discipline process for non-compliance with policy

HRM:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the human resource management process.

Elaboration:

A plan for performing the human resource management process is created to ensure that qualified staff are hired and that they perform in a manner that contributes to the organization's ability to manage operational resilience. The plan must address the resilience requirements of human resources, the dependencies of services on such resources, and the roles that people fulfill at various levels of the organization. In addition, because human resources are the engine behind many services in the organization, the plan must extend to external conditions that can enable or adversely affect the resilience of people.

The plan for the human resource management process should not be confused with the organization's resilience program and plan as described in HRM:SG1.SP1, training plans as described in HRM:SG1.SP3, improvement plans as described in HRM:SG3.SP3, and plans for sustaining and reassigning roles and responsibilities as described in HRM:SG4.SP1. The plan for the human resource management process details how the organization will perform human resource management, including the development of strategies and plans for managing people.

Subpractices

1. Define and document the plan for performing the process.

   Elaboration:

   Special consideration in the plan may have to be given to skill development and planning for sustaining and reassigning various roles. These activities address protecting and sustaining human resources to support operational resilience.

   Special consideration in the plan may have to be given to the establishment, implementation, and maintenance of an internal control system for human resources.

2. Define and document the process description.
3. Review the plan with relevant stakeholders and get their agreement.
4. Revise the plan as necessary.

HRM:GG2.GP3 Provide Resources

Provide adequate resources for performing the human resource management process, developing the work products, and providing the services of the process.

Elaboration:

The diversity of activities required to protect and sustain people requires an extensive level of organizational resources and skills and a significant number of external resources. In addition, these activities require a major commitment of financial resources (both expense and capital) from the organization.

Subpractices

1. Staff the process.

   Elaboration:

   These are examples of staff required to perform the human resource management process:

- staff responsible for
  - information, application, and technical security
  - business continuity and disaster recovery
  - workforce development and benefits administration
  - ensuring the success of the performance management process
  - training and skill development
  - career development counseling
  - managing external entities that have contractual obligations for human
  - resource management activities
- staff involved in operational risk management, including those involved with insurance and risk indemnification
- staff involved in organizational change management
- internal and external auditors responsible for reporting to appropriate committees on process effectiveness

Refer to the Organizational Training and Awareness process area for information about training staff for resilience roles and responsibilities.

2. Fund the process.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for human resource management.

3. Provide necessary tools, techniques, and methods to perform the process.

   Elaboration:

   These are examples of tools, techniques, and methods to support the human resource management process:

   - a performance management system that supports establishing performance goals and objectives and evaluating performance against them
   - job description templates that reflect standard resilience obligations, roles, and responsibilities, required skills, and specific job requirements (e.g., certifications)
   - methods, techniques, and tools for identifying, documenting, maintaining, and validating the resilience skills of current human resources as a skills inventory
   - tools for performing skill gap analysis (between baseline competencies and current skill sets)
   - training plan templates for specific roles and responsibilities
   - methods, techniques, and tools necessary to perform background verification checks
   - methods, techniques, and tools to capture, securely store, and ensure authorized access to sensitive verification data
   - templates for employment agreements, terms and conditions, confidentiality agreements, and non-compete agreements
   - templates for asset inventory checklist capture and sign-off
   - disciplinary process checklists
   - exit interview, termination, and layoff checklists

HRM:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the human resource management process, developing the work products, and providing the services of the process.

Elaboration:

Of paramount importance in assigning responsibility for the human resource management process is establishing job responsibilities and assigned roles for all operational resilience management system activities. Staff are responsible for establishing resilience requirements for all assets and services, ensuring these requirements are met by asset/service owners and custodians, and identifying and remediating gaps where requirements are not being met. Staff also have the responsibility to develop resilience-specific performance goals and objectives and to measure and assess performance against these goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Responsibility and authority may extend not only to staff inside the organization but to those with whom the organization has a contractual (custodial) agreement for managing human resources (by contracting staff or supplementing staff through outsourcing).

2. Assign responsibility and authority for performing the specific tasks of the process.

   Elaboration:

   Responsibility and authority for performing human resource management tasks can be formalized by

   - defining roles and responsibilities in the process plan to include roles responsible for workforce development, performance management, and background verification
   - including process tasks and responsibility for these tasks in specific job descriptions
   - developing policy requiring
     - organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
     - staff to take personal responsibility for acquiring the necessary skill sets to fulfill their job description and roles in sustaining operational resilience
     - compliance with resilience directives
   - including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals
   - developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
   - including process tasks in measuring performance of external entities against contractual instruments

Refer to the External Dependencies Management process area for additional details about managing relationships with external entities.

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

HRM:GG2.GP5 Train People

Train the people performing or supporting the human resource management process as needed.

Elaboration:

The basis for determining training needs for operational resilience management derives from having a comprehensive inventory of current skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill set deficiencies.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Subpractices

1. Identify process skill needs.

   Elaboration:

   These are examples of skills required in the human resource management process:

   - knowledge of tools, techniques, and methods necessary to perform process tasks, including those identified in HRM:GG2.GP3 subpractice 3
   - knowledge necessary to elicit baseline competencies from the organization's resilience program and plan as well as from resilience job descriptions
   - knowledge necessary to develop, populate, and maintain a skills inventory
   - knowledge necessary to compare baseline competencies with current skills and identify and prioritize key skill gaps and deficiencies requiring action
   - knowledge necessary to identify operational risks emerging from the process that should be referred to the risk management process for disposition
   - knowledge necessary to establish and conduct verification programs and procedures in support of candidate screening
   - knowledge necessary to establish the appropriate terms and conditions of employment that reflect the resilience obligations of the job as well as applicable laws and regulations
   - knowledge necessary to evaluate staff performance against resilience goals and objectives, identify improvements, and take corrective actions
   - knowledge necessary to investigate resilience and security breaches and take necessary disciplinary action
   - knowledge necessary to manage sustaining and reassigning resilience roles and responsibilities regardless of cause or initiating event

2. Identify process skill gaps based on available resources and their current skill levels.

3. Identify training opportunities to address skill gaps.

Elaboration:

These are examples of training topics:

- skill deficiencies of existing staff *(The development of training plans is addressed in the Organizational Training and Awareness process area.)*
- general awareness training on the importance of operational resilience in ensuring that all categories of assets (people, information, technology, and facilities) are protected and sustained
- training for human resources practitioners (such as placement specialists, compensation analysts, and benefits managers) who do not have specific experience in resilience job roles or skills
- working with external entities that have responsibility for process activities
- using process methods, tools, and techniques, including those identified in HRM:GG2.GP3 subpractice 3

4. Provide training and review the training needs as necessary.

HRM:GG2.GP6 Control Work Products

Place designated work products of the human resource management process under appropriate levels of control.

Elaboration:

All work products related to human resources documents, such as personal information about pre-employment verification data and performance evaluations, should be placed under control, with appropriate levels of access privileges.

These are examples of human resource management work products placed under control:

- baseline competencies
- job descriptions
- skills inventory, including skill gaps and deficiencies
- training plans
- job requisitions
- outsourcing agreements
- verification procedures and guidelines
- screening criteria
- employment agreements, including terms and conditions of employment
- resilience goals and objectives
- performance evaluations
- disciplinary process investigation reports and supporting documentation
- confidentiality and non-compete agreements
- notes from exit interviews
- signed-off versions of asset inventories for all terminated staff
- process plan
- policies and procedures
- contracts with external entities

HRM:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the human resource management process as planned.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the human resource management process:

   - staff involved in identifying resilience baseline competencies and skills
   - owners and custodians of information, technology, and facility assets to which people need access
   - staff responsible for
     - managing operational risks that involve people
     - establishing, implementing, and maintaining an internal control system for human resources
     - developing, testing, implementing, and executing service continuity plans involving people
     - developing, implementing, or managing organizational training, skill development, and knowledge transfer
   - external entities such as employment recruiters, temporary placement agencies, and contractors that provide human resources services
   - staff in other organizational support functions such as payroll or general services administration
   - human resources staff
   - legal counsel
   - public authorities such as law enforcement that may have to be involved in disciplinary actions
   - internal and external auditors

   Stakeholders are involved in various tasks in the human resource management process, such as

   - planning for human resource recruiting and placement
   - planning for compensation, benefits, and skills analysis
   - establishing baseline competencies required to meet resilience requirements
   - creating human resource job role profiles and skills inventory
   - associating human resources with services and analyzing service dependencies
   - establishing, implementing, and managing human resource access controls
   - developing service continuity and succession plans for job roles
   - managing operational risks from people
   - assessing the adequacy of internal controls and separation of duties
   - training and development of people
   - managing external dependencies on people
   - overseeing industrial relations, collective bargaining, and grievance procedures for human resources

- providing feedback to the organization on resilience job roles and skills
- reviewing and appraising the effectiveness of process activities
- resolving issues in the process

2. Communicate the list of stakeholders to planners and those responsible for process performance.
3. Involve relevant stakeholders in the process as planned.

HRM:GG2.GP8 Measure and Control the Process

Measure and control the human resource management process against the plan for performing the process and take appropriate corrective action.

Elaboration:

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for measuring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

   Elaboration:

   These are examples of metrics for the human resource management process:
   - percentage of job descriptions in which resilience competencies and skills are identified
   - percentage of job descriptions with documented terms and conditions
   - percentage of job descriptions with documented resilience obligations
   - percentage of vital staff with resilience skill deficiencies
   - cost required to address resilience skill gaps
   - schedule required to address resilience skill gaps
   - effort required to address resilience skill gaps
   - percentage of resilience training delivered as scheduled
   - rate of changes to the resilience skills inventory
   - elapsed time since the resilience skills inventory was compared to baseline resilience competencies and skills
   - percentage of acquired vital staff that have met pre-employment verification criteria (baseline and job-specific)
   - percentage of acquired staff that have signed agreements to acknowledge and consent to employment terms and conditions

- percentage of confidentiality and non-compete agreements executed for people in sensitive positions
- number of performance reviews performed (by type)
- percentage of staff that have resilience performance goals and objectives
- percentage of staff that have met/not met their resilience performance goals and objectives
- number of infractions referred to the incident management process
- number of infractions requiring coordination with public authorities
- number of violations of resilience policies subject to disciplinary action
- elapsed time since measures of resilience policy compliance were collected and reviewed
- number of skill gaps referred to the risk management process
- percentage of departing staff (from a position, from the organization) that participate in an exit interview
- percentage of departing staff (from a position, from the organization) that have returned all organizational assets, property, and information
- percentage of departing staff (from a position, from the organization) whose access rights have been discontinued as scheduled
- percentage of involuntary terminations that are processed in accordance with established criteria and procedures

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

   Elaboration:

   Periodic reviews of the human resource management process are needed to ensure that

   - recruiting and hiring reflect the identified skill gaps that have to be filled
   - changes to human resources are accurately communicated, implemented, and documented. (This is particularly critical when dealing with terminations and layoffs.)
   - resilience roles are included in job descriptions
   - actions requiring management involvement are elevated in a timely manner
   - the performance of process activities is being monitored and regularly reported
   - key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
   - administrative, technical, and physical controls are operating as intended
   - controls are meeting the stated intent of the resilience requirements
   - actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.
5. Identify problems in the plan for performing and executing the process.
6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.

7. Track corrective action to closure.

HRM:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the human resource management process against its process description, standards, and procedures, and address non-compliance.

Elaboration:

These are examples of activities to be reviewed:

- assignment of responsibility, accountability, and authority for process activities
- determination of the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- validation of the organization's hiring, background check, and other vetting processes for new and continuing employees as well as external entities
- verification of the internal control system for human resources

These are examples of work products to be reviewed:

- process plan and policies
- disciplinary process reports, particularly for repeat offenders
- layoff and involuntary termination reports
- metrics for the process *(Refer to HRM:GG2.GP8 subpractice 2.)*
- contracts with external entities

HRM:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the human resource management process with higher level managers and resolve issues.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management system.

HRM:GG3 Institutionalize a Defined Process

Human resource management is institutionalized as a defined process.

HRM:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined human resource management process.

Establishing and tailoring process assets, including standard processes, are addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, are addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization's set of standard processes those processes that cover the human resource management process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization's tailoring guidelines.
3. Ensure that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

HRM:GG3.GP2 Collect Improvement Information

Collect human resource management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- the status of human resources with respect to skill currency, skill gaps, and skill deficiencies
- metrics and measurements of the viability of the process *(Refer to HRM:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned in post-event review of incidents and disruptions in continuity
- process lessons learned that can be applied to improve operational resilience management performance
- reports on the effectiveness and weaknesses of controls
- process action plans and strategies that are not being satisfied and the risks associated with these
- the disposition of process risks that have been referred to the risk management process
- resilience requirements that are not being satisfied or are being exceeded

Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process improvement and deployment is addressed in the Organizational Process Focus process area.

Subpractices

1. Store process and work product measures in the organization's measurement repository.
2. Submit documentation for inclusion in the organization's process asset library.

3. Document lessons learned from the process for inclusion in the organization's process asset library.
4. Propose improvements to the organizational process assets.