Process Improvement Credentialing Standards
A Division of the Management and Strategy Institute

Risk Management Standards

Introduction

These open source standards represent the minimum required standards for credentialing the above-named process improvement methodology. To comply with Process Improvement Credentialing Standards, organizations must conduct testing which covers all body of knowledge elements below. Organizations must also comply with Process Improvement Credentialing Standards 15-point organization standard v 0.1.115 or higher. Elements do not necessarily need to be presented in the order shown below. These standards are completely independent of ISO 31000 standards. Practitioners involved in risk management should be familiar with both **MSI 07.06.115** and **ISO 31000** standards. Trainers and organizations are encouraged to teach additional information above and beyond these standards.

Body of Knowledge

1. What is Risk Management
   1.1. Define a Risk
   1.2. Define a Hazard
   1.3. Examples of Risks and Hazards

2. Communication
   2.1. Consulting within the corporate hierarchy

3. Likelihood Scale
   3.1. Impossible
   3.2. Low possibility / Remote possibility
   3.3. Medium possibility / Possible
   3.4. High possibility / Probable

4. Seeking out problems
    4.1. Problems unique to the practitioner's business and industry
    4.2. Physical risks
    4.3. Location risks
    4.4. Human risks
    4.5. Technology risks

5. How to identify risks
    5.1. Doing walk-arounds
    5.2. Long term / Short term
    5.3. Common Issues
        5.3.1. Slip and fall
        5.3.2. Clutter
        5.3.3. Tripping
        5.3.4. Falling objects
        5.3.5. Pollutants

6. Levels of impact
    6.1. Low Impact
    6.2. Medium Impact
    6.3. High Impact

7. External Events
    7.1. Suppliers
    7.2. Customers
    7.3. Visitors
    7.4. Traffic
    7.5. Parking
    7.6. Environment

8. Worst Case Scenarios
    8.1. Having a plan

9. Consequence Scale
    9.1. Insignificant
    9.2. Minor
    9.3. Moderate
    9.4. Major
    9.5. Catastrophic

10. Responsibility
    - 10.1. List of responsible parties, all organizational levels

11. Reporting
    - 11.1. Who should report
    - 11.2. What should be reported
        - 11.2.1. Unauthorized individuals
        - 11.2.2. Leaks
        - 11.2.3. Smells
        - 11.2.4. Broken locks
        - 11.2.5. Broken equipment
        - 11.2.6. Slippery floors
        - 11.2.7. Specific to practitioner industry

12. Appropriate Precautions
    - 12.1. Safety equipment
    - 12.2. Accessible exits
    - 12.3. Fire alarms
    - 12.4. Safety training
    - 12.5. Ergonomic work stations
    - 12.6. Security
    - 12.7. Ventilation
    - 12.8. Specific to practitioner industry

13. Communication Strategy
    - 13.1. Identify the information you need to communicate
    - 13.2. Consider the audience
    - 13.3. Create the communication strategy
    - 13.4. Choose communication methods

14. Tracking and Updating Control Measures
    - 14.1. What Is a Control Measure
    - 14.2. Control Measure Hierarchy
        - 14.2.1. Eliminate
        - 14.2.2. Substitute
        - 14.2.3. Isolate
        - 14.2.4. Engineered controls
        - 14.2.5. Administrative controls
        - 14.2.6. Protective equipment

15. Business Procedures
    - 15.1. Understanding "Are They Adequate"
    - 15.2. Evaluations
        - 15.2.1. At least once a year (Industry specific)
        - 15.2.2. After new procedures are implemented
        - 15.2.3. After any change in the organization

16. Updating and Maintaining
    - 16.1. Training
    - 16.2. Written procedures
    - 16.3. Documentation

17. Risk Management Techniques
    - 17.1. Examples of Risk Reduction
    - 17.2. Transfer the Risk
        - 17.2.1. Indemnification
        - 17.2.2. Certificates of insurance
    - 17.3. Avoid the Risk
    - 17.4. Accept the Risk

18. General Office Safety and Reporting
    - 18.1. Accident Reports
        - 18.1.1. Employee
        - 18.1.2. Supervisor
        - 18.1.3. Medical Provider
    - 18.2. Accident Response Plans
        - 18.2.1. Plan Elements
    - 18.3. Emergency Action Plan
        - 18.3.1. What to Include
    - 18.4. Training and Education

19. Business Impact Analysis
    - 19.1. Conducting a business impact analysis
        - 19.1.1. Reports
        - 19.1.2. Research
        - 19.1.3. Interviews
    - 19.2. Identify Vulnerabilities
    - 19.3. Analyze Information
    - 19.4. Implement Recommendations

20. Disaster Recovery Plan
    - 20.1. When to develop
    - 20.2. Necessary Factors
        - 20.2.1. People
        - 20.2.2. Facilities
        - 20.2.3. Technology
        - 20.2.4. Data
        - 20.2.5. Suppliers
        - 20.2.6. Policies and procedures

21. Disaster Recovery Sites
    - 21.1. Hot Site
    - 21.2. Warm Site
    - 21.3. Cold Site

22. Documentation
    - 22.1. Information to document

23. Methods of Risk Identification
    - 23.1. Who Might Be Harmed
    - 23.2. Are Current Control Measures Sufficient
    - 23.3. Change Control Measures