QBOS® | Design. Develop. Deliver.

White Paper: Effective Risk Management through Workforce Automation

Author: James R. Lord
Date: August 28th, 2008
DOCID: 0-112268-6

Table of Contents

OVERVIEW......3

RISK MANAGEMENT......4
Mitigating Strategies......4
Normal Adoption Methods Lead to Failures in Policy Execution......6

WORKFORCE AUTOMATION......8
Consistency and Persistence......8
Workforce Automation as a form of Workforce Management......9
Further Defining Workforce Automation......10
Convert a Manager into a Process to Obtain Measurable Consistency......11

IMPLEMENTING WORKFORCE AUTOMATION WITH RISK MANAGEMENT......13

SUMMARY......15

APPENDIX A – TERMINOLOGY......16

APPENDIX B – PRIORITIZATION FOR RISK MANAGEMENT......17
Scoring Model......17
Scoring the Mitigating Strategy......18
Scoring the Risk Event......18
Scoring the Risk Management Plan......18

APPENDIX C – BETTER ROI THRU WORKFORCE AUTOMATION......20

Overview

This document identifies and expounds upon the relationship between BPM (Business Process Management), Workforce Automation and Risk Management for the purpose of demonstrating that the adoption required for effective risk management control is best implemented by means of workforce automation.

By defining risk as the occurrence or non-occurrence of certain events and risk management as the process of putting controls in place to manage the outcome of resource expenditure in response to the risk events, we set the stage for associating risk management to workforce automation. In corporate environments involving large numbers of human resources, risk management without workforce automation will by necessity devolve into a reactive management process. In other words, the adoption necessary will have to be continually reinforced by management at an ongoing high cost in both management resources and realized losses due to human inefficiencies in enforcing policy.

The goal of this document is to highlight workforce automation as the path for achieving the highest levels of risk management control adoption with the least reliance upon management reinforcement with the result of reducing costs and risk exposure simultaneously. By doing so, this document will provide a direction for business analysts, comptrollers and executives alike who have been tasked with implementing strong and measurable risk management – the creation of risk management controls via process control in workforce automation.

Appendix A is provided for clarification of terms used.

Appendix B is provided as a risk management plan scoring methodology.

Appendix C is provided to help identify the ROI on workforce automation-implemented risk management.

Risk Management

RULE 1: The objective of risk management is the overall risk reduction to the organization[1]

Risk management is the process of identifying, prioritizing and managing threats to the ongoing operations of an organization.

While identifying and prioritizing risks could be conjointly referred to as "risk assessment," the act of separately prioritizing risks is an admission to the fact that controls for risk management follow an evolutionary design and implementation cycle and are not incorporated into the organizational structure simultaneously. By prioritizing risks as a part of your risk assessment, you are able to allocate resources to mitigating the most significant forms of risk first with the lesser forms of risk being managed by subsequent efforts.

Note that prioritization is not meant here simply as a measure of just the risk, itself (in which case, it would be the cost of recovery from the realized risk event[2]). Rather, prioritization must also take into account the probability of the risk event occurring and even extend to the mitigating strategies by considering the cost of avoidance and containment and the impact on the probability of occurrence. The fact that the prioritizing aspect of risk assessment involves valuing the mitigating strategies as well as the risk events, themselves, means that we can use the sum (or instead, a form of average if the company is experiencing significant change year-to-year) of the prioritization values as a metric for the overall value of a particular risk management plan. See Appendix B – Prioritizing for Risk Management for information on how to implement a risk management plan scoring methodology.

Mitigating Strategies

A mitigating strategy is the collection of policies implemented to address a particular risk event (or particular collection of risk events).

RULE 2: Risk is addressed through either avoidance or containment[3]

Risk mitigating strategies are comprised of two general classes of policies: avoidance and containment. External threats (e.g., flooding, earthquakes, market downturns, traffic

[1] http://en.wikipedia.org/wiki/Risk_management & http://it.toolbox.com/wiki/index.php/Risk_Analysis & http://www.answers.com/topic/risk-management & http://www.ifebp.org/pdf/harker/Risk_Management_Theory.pdf

[2] Where this article talks in terms of risk events "occurring", it is also implying the case where the risk event is actually the "non-occurrence" of some event.

[3] Ibid & http://www.ifebp.org/pdf/harker/Plan_Underwriting.pdf
There are other risk addressing models such as ARTR (Avoid, Reduce, Transfer, Retain) or ACAT (similar). However, we are abstracting risk to an event-driven model. As such, there are only two reactions: assuring the event does/does not occur (avoidance) and, in the event it does/does not occur, managing the ramifications thereof (containment). ARTR/ACAT can both be handled within this framework.

accidents (eliminating key personnel), etc.) are almost exclusively managed by containment policies because you generally cannot have much (if any) impact on the likelihood of an external risk event happening. Avoidance policies (*meaning you are reducing the likelihood of a risk event occurring*) can generally only be applied to risk events within the scope of the business operations (shop/warehouse floor accidents, security breaches, organizational turbulence (see: “Reducing Organizational Turbulence through Process Normalization”), etc.)

Examples of containment policies would be liability insurance, key personnel insurance, disaster recovery policies or even certain personnel polices (e.g., termination clauses).

Examples of avoidance policies would be, again, certain personnel policies (in this case, for example, anti-discriminatory clauses) as well as documented best practices and process definitions.

RULE 3: Avoidance policies overall are less costly than containment policies[4]

Since avoidance policies reduce the cost of recovery through reduced frequency of occurrence and containment policies accept the cost of recovery as-is, all other aspects being the same, the cost of containment policies generally exceeds that of avoidance policies. The cost of an avoidance policy would have to exceed that of the risk event’s corresponding containment policy plus the associated reduction in the cost of recovery before the organization should consider implementing a containment-only policy.

As a result, threats can and should be managed where possible by avoidance policies combined with follow-up containment policies (e.g., controls to reduce shop floor accidents combined with liability insurance should an accident occur anyway).

RULE 4: An organization gains control over its risk events by implementing a policy-based culture.[5]

Where the policy-based culture is absent within an organization, the de-facto risk management method is dependent upon the common sense and performance of the human resources which, by nature, is very reactive (containment). As a policy-based culture spreads throughout the organization, the nature of internal risk management shifts from reactive containment to proactive avoidance. And as the policy management systems are transferred from human management to machine management, policy execution becomes more consistent and measurable, rendering efficiencies that lower the cost of execution and allow implementation across larger segments of the organization.

[4] Ibid
[5] Ibid

Normal Adoption Methods Lead to Failures in Policy Execution

There are some differences between the execution of avoidance and containment policies to manage risk.

Generally, the execution of a containment policy occurs as a result of the risk event occurring. Given the risk event is the trigger to fire off the containment policy, we can conclude that containment policies are executed as exception processes.

Conversely, the execution of avoidance policies is predominately a matter of persistence (and therefore, a subset of normal processes).

Although the execution methods of each policy type may be well defined as a singular event, managing the intersection, or transition, between these events can lead to failure as a result of their diverse recognition and execution methods. It must be recognized that the execution of a containment policy in one organization may trigger the execution of avoidance policies in other organizations resulting in the further triggering of additional containment events[6]. To reduce this exposure, mitigating strategies should be implemented and executed as part of your organization's BPM (Business Process Management) model to understand these events and the relationships between them.

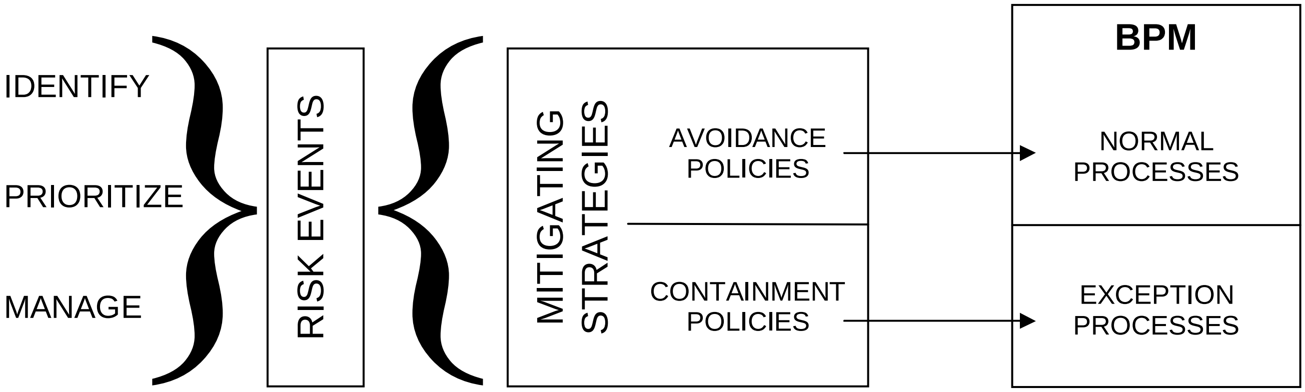


Figure 1: Risk Management should be a part of your BPM process model

However the processes, procedures and policies are defined that make up the mitigating strategies, good management and oversight practices must be in place to assure that staff is following and adhering to these processes, procedures and policies. Where management fails to enforce adherence, workers will not comply and any gains in the reduction of risk events will be lost. Workforce automation mitigates this loss by transferring the enforcement of adherence, transition and other management activities to automated systems. This can

[6] "containment events' refers to risk events managed predominantly by containment policies.

significantly speed up the policy maturation process within an organization[7] or even make the difference as to whether maturation (cultural acceptance within the organization) even occurs. In addition, automation should be implemented to manage the cascading effects of events, and normalization, across the business enterprise.

[7] See "The Process Maturity Framework" within PCMM
http://www.sei.cmu.edu/pub/documents/01.reports/pdf/01mm001.pdf

Workforce Automation

In classic management, the majority of a supervisor's job is *instructing*, *reviewing* and *correcting*.

- **Instructing** their staff in what to do.
- **Reviewing** to see that their staff members are performing correctly and in a timely fashion.
- **Correcting** any staff member who is performing incorrectly or inefficiently.

In this classic supervisory model, we are relying on all of the managers not only to impose good management style, but to impose good management style *consistently day-to-day and consistently manager-to-manager*.

RULE 5: Risk management must be performed consistently and persistently

Consistency and Persistence

Consistency means that processes are performed within the same scope of definition every time. In other words, arbitrariness and ambiguity are given no quarter. And what is actually performed in the execution of the process is that which is expected by the definition of the process, itself.

Persistence, on the other hand, means that every time an event occurs, the corresponding process is executed.

IMPORTANT!

> **Without consistency and persistence in the adherence to supporting processes, any value put on your risk management plan is unsupportable.**

This is because the avoidance policies necessary for internal risk mitigation are highly dependent upon human beings (managers and supervisors) behaving both consistently and persistently. The only thing consistent about human beings is that we do not behave consistently. Persistence and consistency in human beings equates to strong self-discipline. Although you may have an excellent management team in place today, tomorrow may be a different story. As a result, the quality of your risk management plan may vary out of control over time, and any value statement you have made about your risk management plan will no longer be valid.

The failure to implement policy both consistently and persistently results in increased risk to the organization on a compounding scale. Once a risk event occurs, it increases the likelihood of another risk event occurring for a period of time after the first event (called the *relaxation period*). As a result, if management falters in its role of enforcing adherence to policy upon the workforce, the organization's risk management plan is undermined to the point of being non-deterministic. You may as well not have a risk management plan.

So the success of a risk management plan is directly related to the consistency and persistence with which management enforces policy. Yet human management as a whole is by nature neither. So to make workforce policy management effective to the point of truly managing risk, we have to move toward automated workforce management, aka workforce automation. The tool for accomplishing this is a robust and fully integrated BPM system.

Workforce Automation as a form of Workforce Management

Workforce automation is the ultimate form of workforce management, meaning *most controllable*, *most measurable*, *most consistent and most persistent*.

If we look at any business as a collection of processes whereby the business manages cash flow, provides whatever services and/or products it may, manages its resources and relationships and any other task that may be deemed a part of that business' operations, we can quickly see that a majority of these processes describe the work being performed by the rank and file workers of the business. How the workers are made to follow these processes is a matter of three different styles of workforce management.

1. **Classic Supervisory Model** – workers are trained in the various tasks they must perform. The workers rely on their memory, fellow workers and supervisors for guidance re the correctness and timeliness of their performance. In effect, *the business is in the head of the workers* ("…our employees are our greatest asset"), and as such, control over performance is inconsistent and there is little or no control over the evolution of processes. While traditional and still pervasive, this model can never get beyond CMMI/CoBIT maturity levels 0 to 1 (Chaos)[8].

2. **Management by Process Documentation** – all tasks that workers perform are documented as processes and procedures. The workers are trained from the documentation and work by reference from the documentation until they have memorized the processes. The vagaries of different workers doing the same job differently are slightly reduced, a benchmark now exists against which to measure worker performance and control over business process evolution can now be centralized. However, as the processes evolve, the documentation must be kept up to date to reflect the processes, the employees must still "unlearn" the old process and learn the new, and the company is still entirely dependent upon the performance of managers to enforce adherence to procedures and policy. This model attains CMMI/CoBIT maturity levels 2 to 3 (Controllable).

3. **Workforce Automation** – all or most of an organization's processes are documented and implemented into a system that detects triggering events occurring throughout the organization and then renders the documented processes as workflow to the workers on a task-by-task basis. The instructions within the workflow are automatically changed to reflect the data and conditions of the actual event instance. At this point, the actual behavior of the

[8] http://en.wikipedia.org/wiki/Capability_Maturity_Model

company and its centralized documentation are synchronized in a controllable fashion. This model results in CMMI/CoBIT maturity levels 4 to 5 (Repeatable, Measurable and Optimizable) and makes its practicing organizations ISO900x Quality Management certifiable.

These three styles represent an evolution of workforce management from the classic supervisory model to complete workforce automation.

Further Defining Workforce Automation

Workforce automation is about automating two things: task-level instruction and the handoff of tasks between workers. Everything else about workforce automation arises out of these two areas of automation and its demonstrated value should be: that it eliminates the need for training, that it manages the flow of work throughout an organization, that it guarantees consistent/persistent behavior, and culminates in significant overall risk reduction (i.e., good risk management).

In automating task-level instruction, a BPM system that can visually render work items to the user is a necessity. An analyst would document all of the tasks that a worker would have to perform into various processes within the BPM. The source for this knowledge may come from the workers and/or the managers, but would undergo review from a risk assessment perspective. The BPM used should also support the ability to evolve the processes over time. The BPM would then render workflow as events occur across the organization. The clause, “render workflow”, means to deliver work items to the appropriate workers. The work items generated by the BPM should explicitly state what needs to be done and include any specific data needed by the worker to perform his/her task. As a result, full workforce automation requires a robust BPM system fully integrated across all of the systems of the organization.

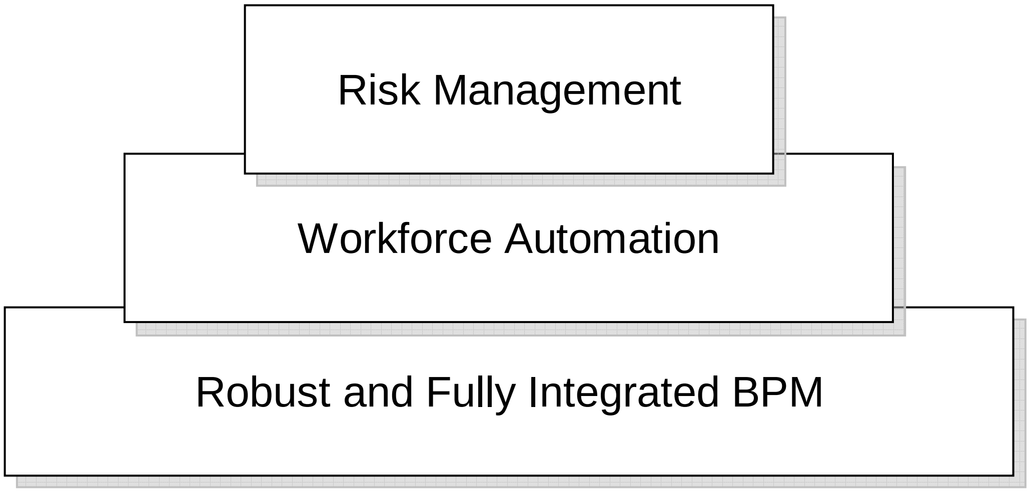


Figure 2: Risk Management is built upon Workforce Automation, which is built upon a robust and fully integrated BPM system

Convert a Manager into a Process to Obtain Measurable Consistency

With workforce automation, the Instruction part of what a supervisor does is embedded into a process for delivery to the workers performing the various tasks. The company is no longer dependent upon the manager to exhibit consistent behavior with regards to at least the Instruction phase of his/her work. And likewise, the company is no longer dependent upon the worker's understanding of the task at hand or decision-making abilities on that particular day to achieve a more consistent behavior from the worker. Every time a worker must perform a particular task, the appropriate instructions are presented as part of the workflow process.

As for the Review part of what a supervisor does, the three most common causes for correction are:

- Failure to Complete Within the Allotted Time
- Failure to Complete Correctly
- Failure to Hand-off to Another Worker or Receive a Hand-off from Another Worker

With workforce automation, the Review component that uncovers Failure to Complete Within the Allotted Time situations is addressed via an escalation subsystem within the BPM system. Meaning that the BPM system must have the ability to track the work that has been assigned and run an alternate or complimentary process if the work is not completed (or about to not be completed) within a particular time frame. Most often, this will simply be an alert to the supervisor that the worker is falling behind. It could even be preceded by an alert to the worker that their task is about to be tagged as tardy, thus stimulating the worker towards timely completion. The result of an escalation subsystem in your BPM system is (1) tardiness is reduced and (2) the supervisor does not have to repeatedly poll his/her staff, but rather simply receives alerts when tardiness does occur.

Similarly, the Review component that uncovers Failure to Complete Correctly situations is handled via an audit subsystem of the BPM system. Meaning that the BPM must support a complete history of all work completed, allowing the supervisor (or a designated auditor) to peruse the audit at will. Once again, the supervisor does not have to poll his/her staff directly nor have to interpret their explanations of what they have accomplished. Rather, the supervisor can directly access the actual work performed and make a quick and transparent determination as to the accuracy of the staff member's work. An additional benefit of such an audit trail is the ability to directly compare different workers' throughput. Ideally, the BPM system can include quality validation metrics by automated analysis of the audit trails.

Finally, Failure to Hand-off to Another Worker or Receive a Hand-off from Another Worker is one of the most significant causes of turbulence and the need for correction during Review, yet ironically, it is also one of the hardest to detect. The reason for a hand-off failure in traditional workforce management scenarios is that both the sending worker and the receiving worker are responsible for the hand-off being successful. Failure can occur for many reasons (e.g., the first worker has completed her task and emailed the second worker who did not see the email in his inbox before it disappeared under a flood of other emails).

Hand-off failures are the number one reason for processes failing to complete on time, and thus contribute to significant turbulence within the organization.

Every BPM system that renders workflow should detect the completion of a work item and automatically send the next one, thus automating the hand-off. Display of work items should be via an interface that:

- segregates workflow from general messaging
- organizes workflow by urgency
- escalates items to greater urgency as they approach their cut-off date
- accelerates the escalation process based upon items' importance attribute
- informs the worker of the risk of supervisor notification

Departmental boundaries represent the most common fail point for hand-offs. As a result, any BPM used for workforce automation should extend across departmental boundaries at a minimum. Next generation BPM systems should extend across corporate boundaries for the larger enterprise
.

All hand-off failures, representing a significant source of organizational turbulence, can be eliminated under workforce automation.

Shifting a supervisor's Instruction and Review efforts to automated processes makes Instruction and Review completely consistent and persistent.

The supervisor is freed up to both handle a larger number of staff members and to address correction more effectively. Workforce automation can even track correction efforts to gauge the effectiveness of the efforts on the staff member(s).

In addition to the risk reduction brought about by imposing consistent and persistent business process execution, workforce automation also reduces risk by shrinking the training window required by staff members to become fully productive and by the transference of business process knowledge from the staff to the BPM system, preventing loss of such knowledge every time a staff member leaves the organization.

Implementing Workforce Automation with Risk Management

As Figure 2 (pg 9) states, Workforce Automation requires a robust and fully integrated BPM system. To be defined as robust, the BPM system must:

- be able to render workflow (some BPM systems are only modelers)
- include a flexible escalation subsystem
- include full audit trails with contextual access
- support evolutionary redesign of processes
- allow multiple versions of the same process to run concurrently
- include instance-based process control (e.g., allowing a process to run one way for one customer but a completely different way for another customer)
- include rate-based process control—meaning a process can change the way it runs based upon the rate at which the triggering event is occurring (this is an important mechanism for short-circuiting the feedback loops that lead to organizational turbulence)
- include process flow transfer—meaning a process that is running against one object can kick off a process running against a different object (e.g. a process running against a product order can kick off a process running against the associated customer)
- support event accumulation triggers—allowing a process to be triggered not by a single event, as is normal, but by the n^{th} occurrence of the event with a specific time period (the process must have access to all of the objects bound to the various n events)

And to be defined as fully integrated, the BPM system must be tied into all of the various systems the organization uses to where the BPM can react to any business event that occurs

Once your organization has such a BPM in place (not in the scope of this document and not a simple effort in and of itself (unless of course you are on QBOS where the BPM is universally integrated)), follow the steps below as a guideline to implementing workforce automation with risk management embedded.

1. On a department-by-department basis, identify all events[9] that may occur in the normal course of business. Some events may be universal (e.g., HIRE EMPLOYEE, TERMINATE EMPLOYEE, etc.) and many events will span department boundaries (once again: HIRE EMPLOYEE, TERMINATE EMPLOYEE, etc.). The department-by-department approach to building the event lexicon is simply to avoid overlooking any meaningful business operations events. The processes that will be designed to manage these events will be your *normal processes* and they will include all of your avoidance policies.

2. Design your normal processes to manage the events identified above. Note that the designing of the detailed steps in a business process is itself a skill set and not in the scope of this document. Also note that, with regard to avoidance policies, the actual steps and their details reflect a specific choice of possibly several different mitigation strategies. This choice may reflect the results of the scoring method described in Appendix B.

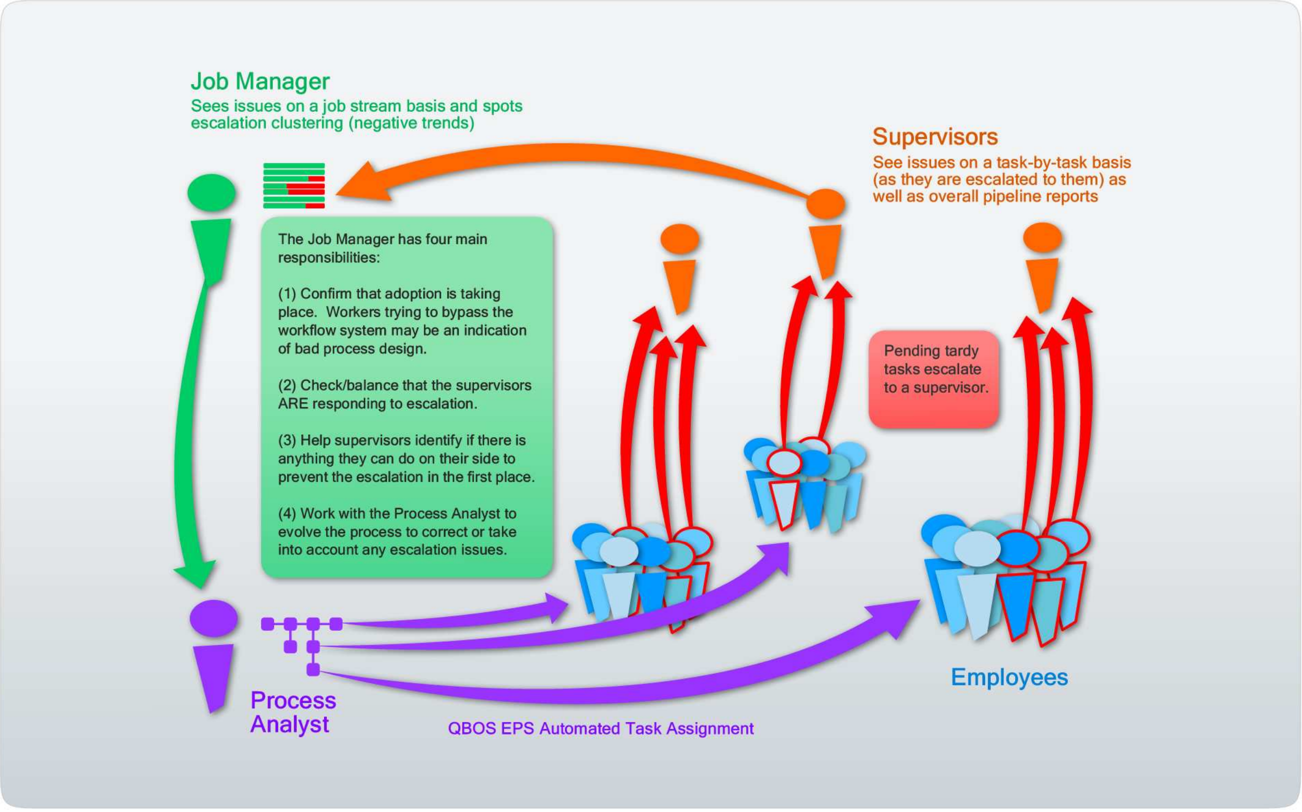
3. Review the event lexicon on a department-by-department basis, this time with an eye toward identifying any risk events that may occur that were not addressed as part of the normal business processes. Some risk events may be entirely new events (e.g., POWER OUTAGE, etc.) in which case they will be handled by their own processes and some risk events will actually be a sub-type of a normal event (e.g., TERMINATE EMPLOYEE—EMPLOYEE REACTING BADLY, etc.) which can be handled either

[9] Including transitional state changes

by a process flow transfer from the root event (TERMINATE EMPLOYEE) to a separate process designed for this event (TERMINATE EMPLOYEE—EMPLOYEE REACTING BADLY) or by simply an adjustment within the root event process. Any new processes created (your *exception processes*) or process changes as a result of this effort will reflect your containment policies.

4. Design any new processes or process changes needed to address the identified risk events.

5. Bring your various processes online one at a time to assure (see image below):
   a. workforce adoption
   b. supervisory adoption of escalation components
   c. appropriate process-step granularity



Job Manager
Sees issues on a job stream basis and spots escalation clustering (negative trends)
Supervisors
See issues on a task-by-task basis (as they are escalated to them) as well as overall pipeline reports
Pending tardy tasks escalate to a supervisor.
Employees
Process Analyst
QBOS EPS Automated Task Assignment

The Job Manager has four main responsibilities:

(1) Confirm that adoption is taking place. Workers trying to bypass the workflow system may be an indication of bad process design.

(2) Check/balance that the supervisors ARE responding to escalation.

(3) Help supervisors identify if there is anything they can do on their side to prevent the escalation in the first place.

(4) Work with the Process Analyst to evolve the process to correct or take into account any escalation issues.

6. As Job History Streams accumulate, the Job Manager must compare against the original risk lexicon to confirm that:
   a. avoidance policies are executing
   b. pre-risk event containment policies (insurance policy review, insurance payments, etc.) are executing
   c. all other normal processes are executing as expected

7. Post-risk event containment policies must generally be tested through simulation. For this purpose, each post-risk event containment policy process is copied to a new version and labeled as a test version and executed to test the efficacy of the process design. This harkens back to the BPM robustness requirement of allowing multiple versions of the same process to run concurrently.

8. Maintain a Job Manager role on an ongoing basis to monitor job stream throughput.

9. Maintain a Process Analyst role on an ongoing basis to monitor process efficacy and coordinate the evolution of the processes to match the evolution of the organization.

Summary

In summation, the controls, consistent behavior and persistence necessary to implement truly measurable and therefore effective risk management can only be implemented via workforce automation. Anything less allows for turbulence to creep into the organization, undermining risk management efforts.

Workforce automation is the ultimate form of workforce management and requires a robust and fully integrated BPM system to support it. Process control via BPMS requires the support of Job Manager and Process/Business Analyst roles in the organization. These roles centralize and abstract process control knowledge for the organization.

The mitigating strategies for a risk management plan take the form of avoidance and containment policies. Avoidance policies are integrated into process control as normal processes, whereas containment policies are integrated into process control as exception processes.

Workforce automation frees up a significant amount of management resources, flattens an organization and reduces losses resulting in significant costs reductions to the practicing organization.

Appendix A – Terminology

Avoidance Policy Part of a mitigating strategy. Any policy that affects the likelihood of a candidate event becoming a risk event is an avoidance policy.

BPMS Business Process Management System automates the BPM approach using technology or software such as QBOS®.

Candidate Event Any event that includes the risk event as one of its possible outcomes. For example, processing-an-order is a candidate event that includes the risk event of shipping-the-incorrect-product. In formal process normalization, candidate events trigger your normal processes while risk events trigger your exception processes (as a result, your exception processes align with your containment policies). Depending upon the nature of the candidate event, the risk event exception process may compliment or override the associated normal process. See: "Reducing Organizational Turbulence through Process Normalization" for information on the formal methodology of process normalization.

Containment Policy Part of a mitigating strategy. Any policy that assumes the risk event will occur and is implemented to offset the cost of the risk event when it does occur. A containment policy does not affect the likelihood of a risk event occurring.

Mitigating Strategy A method designed to eliminate or diminish the effects of risk by any combination of the following:

1) Avoiding certain candidate events altogether or…
2) Where a candidate event is a necessary part of the business model, reducing the likelihood of a risk event occurring or…
3) Reducing the cost/impact of the risk event once occurred.

The first two forms above involve *avoidance* with the third being *containment*.

Risk The degree of lack of control over outcomes of various processes.

Risk Event An outcome that is not a desired outcome. Power outage, flooding, death or sidelining injury of an employee, false negative (or false positive) provisioning of services or products (such as shipping the wrong product) are all examples of risk events.

Appendix B – Prioritization for Risk Management

The concept behind prioritizing for risk management is based on the fact that judgment to allocate resources to assuaging a particular risk event cannot be made in isolation (although *identifying* what resources are necessary to apply can be made in isolation). If such judgment was made in isolation, then resources may not be available to address other risk events that represent greater risk to the organization.

Scoring Model

What is needed is a way to compare risk events against one-another on a common scoring model that takes into account the use of resources. This would allow us to calculate the risk profile for the company in such a way that:

- risk events can be addressed based upon which event has the highest score
- the risk management plan would then have its own score (a function of the overall risk event scores) which can be used to ratchet improvement of the overall risk management plan
- mitigating strategies can then evolve to result in lower risk event scores over time

At first glance, we tend to think of realized risk events in terms of their Direct Cost to Recover. This is the actual cost to the company to return to normal operations should the risk event occur[10]. However, by itself this is insufficient as a comparative metric as it does not take into consideration any of the following:

- direct/indirect losses suffered during the recovery period
- the likelihood of the risk event actually occurring within a common time period (if two different risks both have a Direct Cost to Recover of $100,000 but the first risk is more likely to occur, you would want to address it first)
- any costs associated with the mitigating strategy (including costs realized prior to the event)

Any scoring model must take losses, adjusted frequency and mitigating strategy costs into account along with the Direct Costs to Recover. But before the risk event frequency can be adjusted by the selection of any particular avoidance policy, all risk events' frequencies must first be normalized to a common time period. Call this the Base Period (e.g., one year). Each risk event is then considered to determine its number of Occurrences Per Base Period (its normalized frequency). This number should be derived from industry empiricals where possible, so that a benchmark is created against which to evaluate avoidance policies in retrospect. Notice that in the final scoring model below, the adjusted frequency is a part of the formula only as its component multiplicands: [Occurrences Per Base Period] and [Impact of Avoidance Policy on Frequency]. This is because the latter is more of a subjective coefficient and should be segregated within the formula for later review once empirical data has accumulated

[10] subsequent risk management plan analysis may incorporate return-to-alternate-normal processing opportunities

Scoring the Mitigating Strategy

In order to compare one risk event against another, the scores for both have to first be determined, meaning that the mitigating strategies for both have to have already been selected. Should a single risk event have multiple possible mitigating strategies to choose from, the mechanism for doing so is by comparing the costs and impacts of the different strategies against one another. In other words, the mitigating strategies themselves are effectively scored. The way to "score" competing mitigating strategies is to enter the costs and impacts of the various avoidance (and containment) options into the risk event scoring formula (see below) and select the mitigating strategy that produces the lowest overall score for the risk event.

Scoring the Risk Event

The policy that produces the lowest score for the risk event becomes *the* avoidance (and/or containment) policy for that risk event.

The formula for determining the risk event score is:

$$\text{Score} = \begin{array}{l}\text{Occurrences Per}\\ \text{Base Period}\end{array} \; \text{x} \left(\begin{array}{c}\text{Direct Cost to Recover}\\ + \text{ Losses}\\ + \text{ Cost of Avoidance}\\ + \text{ Cost of Containment}\end{array} \right) \text{x} \; \begin{array}{l}\text{Impact of Avoidance}\\ \text{Policy on Frequency}\end{array}$$

Note that each of the terms in the parenthesis is considered *per incident*. I.e., the Cost of Avoidance is actually Cost of Avoidance Per Incident, etc.

Once your various risk events have been scored, address them in order of descending scores as the higher the score, the more damaging the actual risk event will actually be to the organization.

Document your risk event scores in a system that labels the risk event and stores with it each of the components of the formula above[11]. This system should be able to also give you a sum of all the risk event scores – your Total Adjusted Risk.

Scoring the Risk Management Plan

[11] In this manner, the same data can be used to derive the ROI value of any particular risk management plan. While both ROI and the TAR model show herein can be used to compare risk management plans, the TAR model provides additional information in terms of the total amount of risk being managed by the company.

Your Total Adjusted Risk (TAR) can be used as a comparative metric for your overall risk management plan to gauge improvement of the plan year-to-year. However, if you do so, you must bear in mind that total risk grows inline with corporate growth. In other words, there are more risk events that have to be addressed as an organization expands into new territories, lines of business and modes of operation. So in order to use Total Adjusted Risk (TAR) as your plan metric, you must actually store two numbers: the ratio of this year's TAR against last year's TAR (adjusted to common risk events) and this year's TAR (including all risk events).

$$\text{Risk Management Plan Score} = \frac{\text{This Year's TAR}^{[12]}}{\text{Last Year's TAR}^{[11]}} \;:\; \textbf{This Year's TAR}$$

The first number, the ratio, indicates whether the plan is improving (<1) or not improving (>=1) compared with the previous year's plan.

The second number gives the total adjusted risk being managed by your risk management plan.

[12] these are adjusted TARs including only scores for risk events being managed in both years

Appendix C – Better ROI through Workforce Automation

The purpose of this document has been to show that risk management plans achieve greater adoption, and therefore greater efficacy, when implemented via workforce automation. Hopefully, this has been demonstrated to the reader's satisfaction.

One might think that greater efficacy should always translate to greater ROI. If that is true, then can we then make the following global statement?

"Risk management plans produce greater ROI when implemented via workforce automation"

This appendix serves to prove the above statement, identifying whatever constraints may be needed to make it a global statement.

Note that all variables given below pull their data from the TAR scoring methodology laid out in Appendix B.

First, let's express the term "greater efficacy" in terms that can be applied in the formulas below. We used the term "greater efficacy" to mean the results of a risk management plan being "most controllable, most measurable, most consistent and most persistent" under workforce automation. These attributes lead to a state of reduced risk-related losses over the same risk management plan implemented without workforce automation. Or to flip that statement around, a non-workforce-automation-implemented risk management plan incurs an additional set of risk-related losses. Using the data collected as part of the TAR scoring method in Appendix B, we can calculate the loss differential and denote it as $\Delta_{\text{addtl losses}}$ in the formulas further below.

Next, lets calculate the ROI on risk management plan X.

The Courtney formula[13] for calculating cost-benefits in risk analysis takes the annualized loss expectancy (ALE) with and without the risk management plan in place as well as the costs of implementing the risk management plan (RMP_{cost}), as a basis for determining ROI.

The ALE is derived from the total Direct Costs to Recover and total Losses identified in Appendix B[14] (thus, the greater efficacy mentioned above corresponds to a lower ALE due to fewer realized losses).

The RMP_{cost} is derived from the sum of the avoidance and containment costs likewise specified in Appendix B.

[13] Robert Courtney Jr. (IBM, 1970); http://en.wikipedia.org/wiki/Risk_management
[14] See footnote 10 on page 17

Using the Courtney formula, for any one risk management plan, RMP^{x}, we get:

Return **O**n **I**nvestment of **R**isk **M**gt **P**lan **X**

Annualized **L**oss **E**xpectancy (*without* Risk Management in place)

$$\mathrm{ROI}_{\mathrm{RMP}^{x}} = (\mathrm{ALE}_{\text{with RMP}^{x}} + \mathrm{RMP}^{x}_{\text{cost}}) - \mathrm{ALE}$$

Annualized **L**oss **E**xpectancy **+** Costs of **R**isk **M**gt **P**lan (with Risk Management in place)

Notice that RMP$^{x}_{\text{cost}}$ in a system with no workforce automation in place translates into the costs of management oversight.

When comparing risk management plans with (^{WA}) and without workforce automation (^{x}), we get

$$\mathrm{ROI}_{\mathrm{RMP}^{WA}} = (\mathrm{ALE}_{\text{with RMP}^{WA}} + \mathrm{RMP}^{WA}_{\text{cost}}) - \mathrm{ALE}$$

vs

$$\mathrm{ROI}_{\mathrm{RMP}^{x}} = (\mathrm{ALE}_{\text{with RMP}^{x}} + \mathrm{RMP}^{x}_{\text{cost}}) - \mathrm{ALE}$$

we can eliminate the rightmost ALE as a common value if we restate the comparison like so:

$$\mathrm{ROI}_{\mathrm{RMP}^{WA}} : \mathrm{ROI}_{\mathrm{RMP}^{x}} \equiv (\mathrm{ALE}_{\text{with RMP}^{WA}} + \mathrm{RMP}^{WA}_{\text{cost}}) : (\mathrm{ALE}_{\text{with RMP}^{x}} + \mathrm{RMP}^{x}_{\text{cost}})$$[15]

Also, since ALE corresponds to the risk-related losses mentioned in the first paragraph above, then the greater efficacy mentioned corresponds to a lower value for ALE$_{\text{with RMP}^{WA}}$ than for ALE$_{\text{with RMP}^{x}}$, meaning we can restate ALE$_{\text{with RMP}^{x}}$ in terms of ALE$_{\text{with RMP}^{WA}}$ plus additional losses ($\Delta_{\text{addtl losses}}$). Our comparison now looks like this:

$$\mathrm{ROI}_{\mathrm{RMP}^{WA}} : \mathrm{ROI}_{\mathrm{RMP}^{x}} \equiv (\mathrm{ALE}_{\text{with RMP}^{WA}} + \mathrm{RMP}^{WA}_{\text{cost}}) : (\mathrm{ALE}_{\text{with RMP}^{WA}} + \Delta_{\text{addtl losses}} + \mathrm{RMP}^{x}_{\text{cost}})$$

allowing us to again eliminate common elements:

$$\mathrm{ROI}_{\mathrm{RMP}^{WA}} : \mathrm{ROI}_{\mathrm{RMP}^{x}} \equiv \mathrm{RMP}^{WA}_{\text{cost}} : \Delta_{\text{addtl losses}} + \mathrm{RMP}^{x}_{\text{cost}}$$

[15] This notation reads as, “the relationship between (**:**)… and … is identical to (≡) the relationship between (**:**)… and …”

and we can now see why greater efficacy alone is not enough to unilaterally state that the ROI on risk management via workforce automation is greater than that without. We have one last item to demonstrate to be able to make that statement – that ($\Delta_{\text{addtl losses}}$ + $\text{RMP}^{\text{x}}_{\text{cost}}$) is always greater in the long run than ($\text{RMP}^{\text{WA}}_{\text{cost}}$).

The simplest way to do this is to start with the contrary position and see where it takes us.

So let's start by assuming ($\text{RMP}^{\text{WA}}_{\text{cost}}$) is far more expensive than ($\Delta_{\text{addtl losses}}$ + $\text{RMP}^{\text{x}}_{\text{cost}}$), say N times more expensive:

$$(\text{RMP}^{\text{WA}}_{\text{cost}}) = \text{N x } (\Delta_{\text{addtl losses}} + \text{RMP}^{\text{x}}_{\text{cost}})$$

Note that implementing workforce automation is a ratcheting process. As effort (costs) are put into implementing a workforce automation environment, the gains are persistent. This is not true regarding the costs associated with risk management via pure managerial oversight – there the effort (costs) must be repeated for as long as the gains are desired (and the costs on a per human resource level remain approximately the same year-to-year).

What this means is that over time, whatever N we begin with above decreases as less and less effort (costs) are required to implement (and maintain) workforce automation. At some point, implementation is effectively complete with only changes in the business model/environment requiring new implementation efforts[16]. At that point, ($\text{RMP}^{\text{WA}}_{\text{cost}}$) has resolved to the cost of the BPM system rendering workforce automation. This results in the following relation:

$$\text{ROI}_{\text{RMP}^{\text{WA}}} : \text{ROI}_{\text{RMP}^{\text{x}}} \equiv \text{BPMS}_{\text{cost}} : \Delta_{\text{addtl losses}} + \text{RMP}^{\text{x}}_{\text{cost}}$$

Translating this back into English, we get the following global statement:

"The positive ROI of implementing risk management through workforce automation equals the costs of management oversight plus the costs of additional losses incurred (due to failures in consistent/persistent performance) minus the cost of the supporting BPM system[17] and nothing else[18]."

[16] For organizations experiencing a high rate of significant business model change over long periods of time, this argument must be restated in a different manner not within the scope of this article.
[17] …the negative value thereof. Meaning that the formula is tallied and then negated to show the positive ROI.
[18] The "…and nothing else…" means that all other constraints and variables fall out as shown in the formulas above.