

Foster a Culture of Compliance Making Use of Technology

Presented by Michelle Coussens, Business Strategist, Plan B Consulting

Agenda

- Why compliance matters
- Associated risks to address
- Ways to reinforce compliance training
- Motivating employees to care about it
- What technology can do to assist



Meet the Expert

Michelle Coussens | Business Strategist | Plan B Consulting



Michelle Coussens is a frequently sought-after speaker and business strategist for numerous types of organizations on a wide range of topics related to the workplace, including but not limited to talent management, business strategy, and operational effectiveness.



She is a resourceful, resilient, and relentless business professional with demonstrated success in building new programs, driving short-term efficiencies, and improving long-term effectiveness all through innovation, rigor, and courageous leadership.



She has direct experience with a variety of industries, as well as in consulting, education, and not-for-profit organizations. With consistently high participant ratings, her webinars, seminars, and speaking engagements bring practical value to businesses of every size and type.

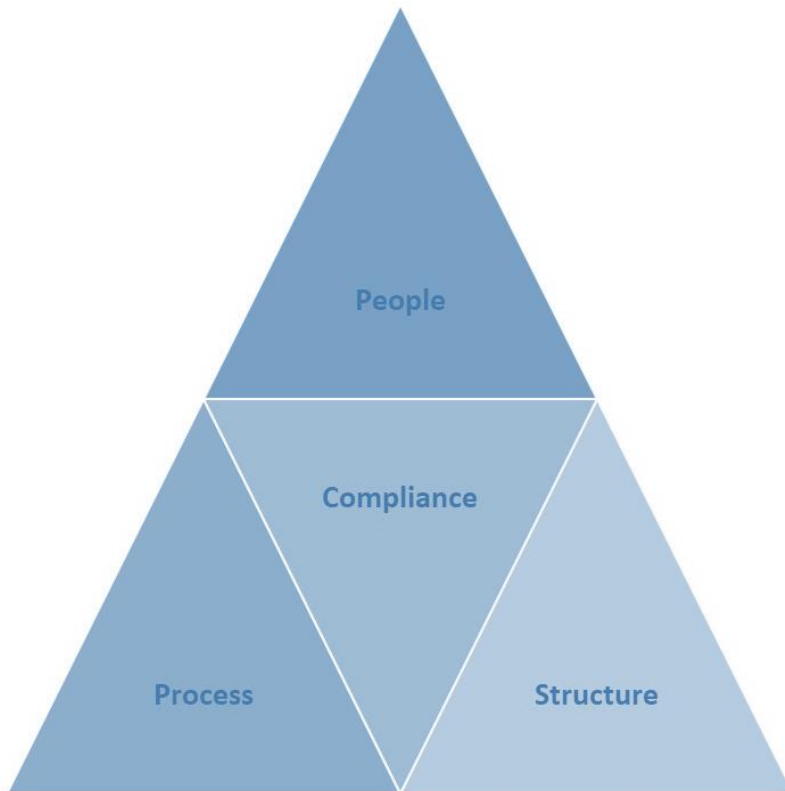
Disclaimer: Note that this webinar is intended to provide useful information but should not be construed as individual legal or financial fact, advice, or opinion. Ms. Coussens is not a representative of today's sponsors.

Why compliance matters



What is “compliance”?

“In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Compliance has traditionally been explained by reference to the deterrence theory, according to which punishing a behavior will decrease the violations both by the wrongdoer and by others” (Wikipedia)



- **Compliance in business**
 - General federal, state, and local regulations, as well as those that are industry-specific
 - Associations and other industry group specifications or best practices
 - Contractual requirements when contracting with others, such as vendors
- **HR compliance**
 - Regards adherence to all applicable labor laws
 - Requires an understanding of the interplay of people, processes, and structure

Compliance impacts to your business

- **Strengthens organizational operations and continuous improvement while simultaneously protecting your workers and your business**
- **Characteristics**
 - Institutes procedures to identify and address variations from required practices
 - Includes training and procedures around ongoing incident prevention and response, contingency planning, and even emergency preparedness
- **Benefits**
 - Avoid fines and civil actions against the business
 - Encourages environmentally friendly processes
 - Helps avoid and mitigate negative risk
 - Saves on resources (time and money)
 - Provides fail-safe systems and builds them into day-to-day routines
 - Enhances your organization's reputation

“Internal Controls” definition

- **Involves organizational policies, procedures, and tools to help the organization achieve results within legal requirements while safeguarding its integrity**
- **Objectives:**
 - Effectiveness and efficiency of operations
 - Reliability of financial reporting
 - Accomplishment of established goals & objectives
 - Compliance with laws and regulations
- **Provides reasonable assurance that:**
 - Functions and processes are achieving their intended results
 - Resources are protected from waste, fraud, abuse, and mismanagement
 - Laws and regulations are being followed
- **Additional benefits**
 - Operate more effectively and efficiently
 - Protects the organization from loss (including fraud)
 - Provides reliable financial data

Financial compliance considerations

- **Financial governance:** how a firm collects, manages, monitors and controls financial information
- **Businesses must follow federal and state rules, laws, and regulations for financial transactions, as well as related data**
- **Transaction monitoring analytics can assess integrated risk and compliance management across the organization**



Questions to consider

- Does your organization maintain a financial management system that complies with generally accepted accounting principles (GAAP) and includes adequate internal control systems?
- Is your organization willing to submit reports to funders and other relevant parties in the form, detail and timeframes required and to comply with reasonable changes in reporting requirements over time?
- Standard required reporting often includes detailed quarterly production reports and comprehensive annual reports.
- Is your organization willing to abide by the performance standards and associated organizational health ratings that may be required?

It starts with clear policies, processes, and SOPs

- Empower your own staff, as well as other employees with knowledge and operating guidelines needed to effectively and efficiently do their jobs
- Provides effective first line of defense against potential of regulatory non-compliance
- Help your organization operate more smoothly and efficiently

Policy	<ul style="list-style-type: none">• A mandate and directive from the board, regulatory bodies or executive director• Its primary purpose is to influence behavior in a very specific manner• Overarching principles under which your organization operates
Process	<ul style="list-style-type: none">• A high-level set of related tasks that must be completed to deliver to your customers or ensure compliance with a policy• Usually involves several tasks or sub-tasks, more than one person, more than one department and multiple procedures and work instructions
Procedure	<ul style="list-style-type: none">• A specific, detailed series of actions that staff must take in order to implement a process and comply with a policy• More specific about how a specific task or activity in a process will be accomplished

Standard protocols all businesses should adopt

- **Separation of duties**
 - Divide responsibilities between different employees or areas so one individual doesn't control all aspects of a transaction
 - **Reduces the opportunity for an employee to commit and conceal errors (intentional or unintentional) or perpetrate fraud**
- **Create documentation**
 - Critical Decisions and significant events that typically involve the use, commitment, or transfer of resources
 - Transactions should be traceable from inception through completion
 - SOPs (Standard Operating Procedures) should be prepared, shared and stored for reference and consistency
- **Authorizations & approvals**
 - Clarity on which activities require approval, and by whom, based on the level of risk to the organization
 - Performance expectations should represent appropriate lines of authority

Standard protocols all businesses should adopt (cont'd)

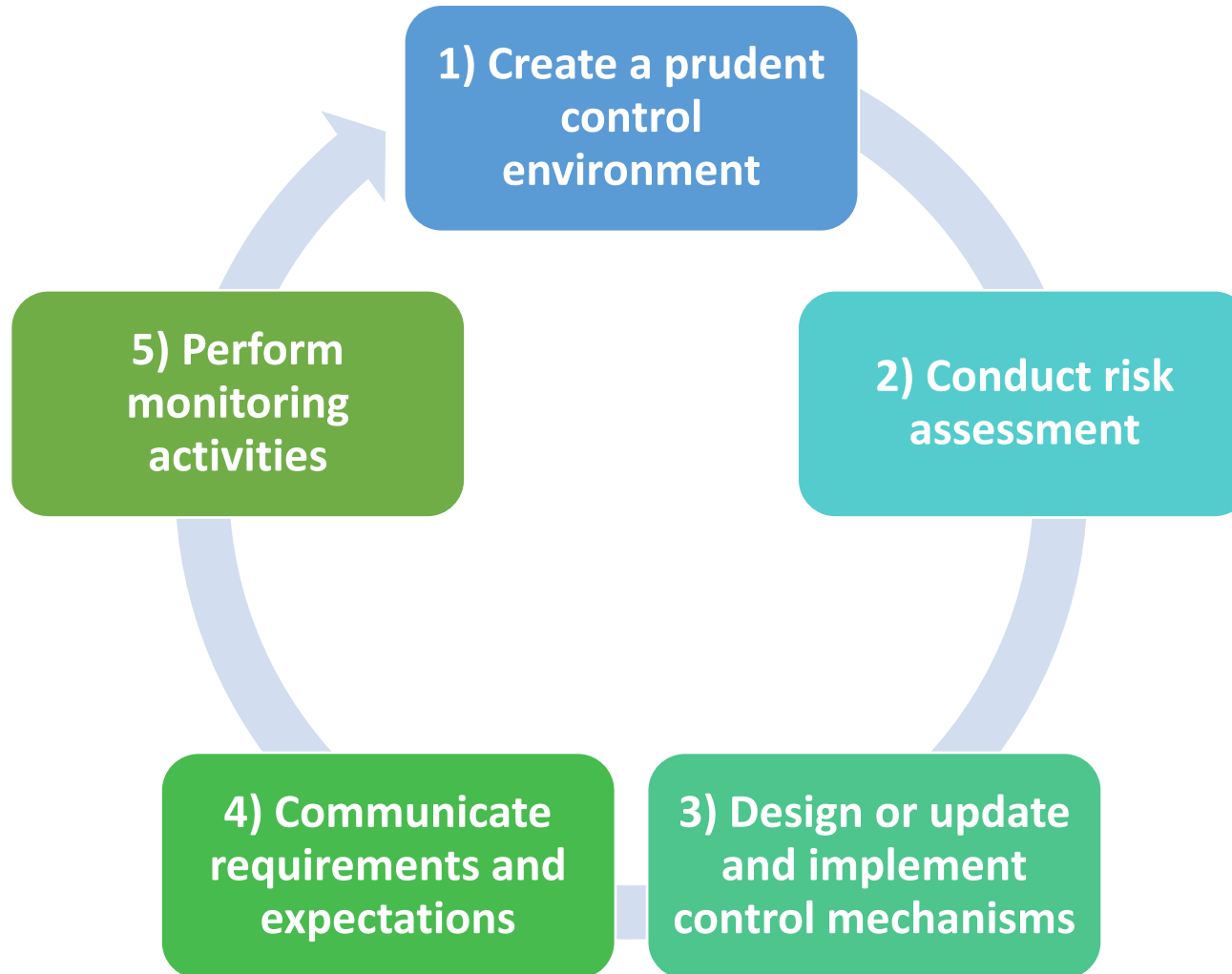
- **Asset security protocols**

- Secure and restricted access to equipment, cash, inventory, and confidential information to reduce the risk of loss or unauthorized use
- Take periodic physical inventories to verify existence, quantities, location, condition, and utilization
- Align the level of security with the degree of value and vulnerability of items being secured, based on probability and severity of potential loss

- **Reconciliation & review**

- Ensure transactions, information, and events are accurate, complete, appropriate, and compliant
- Base the level of review on materiality, risk, and overall importance to the organization's objectives
- Conduct review frequently enough to detect and take any needed action in a timely manner

The Internal Control Process



Process components

1) Create a prudent control environment

- Demonstrate commitment to integrity and ethical behavior
- Exercise appropriate oversight responsibility
- Establish boundaries around structure, responsibility, and authority
- Enforce accountability

2) Conduct risk assessment

- Define business objectives and acceptable risk tolerances
- Identify, analyze, and respond to risk potential
- Assess fraud risk
- Analyze and respond to various types of change

3) Design/Update and implement control mechanisms

- Match business activities to associated control needs
- Create/update SOPs

4) Communicate requirements and expectations

- Internal staff
 - Reinforce through reminders and performance expectations
- External stakeholders

5) Perform monitoring activities

- Identify any inappropriate variances, along with associated reasons
- Remediate individual issues, as well as systemic deficiencies

Align control types with organizational accountability

- **Directive**
 - Setting policies/procedures, spending limits, work and tech standards, etc.
- **Preventative**
 - Train staff on applicable policies/procedures
 - Incorporate a review and approval process for purchase requisitions to make sure they are appropriate before any purchase
- **Detective**
 - Conduct supervisory reviews
 - Compare transactions on reports to source documents
- **Corrective**
 - Document revisions after identifying an error or variance
 - Update access lists if individual's role changes
- **Recovery**
 - Prepare data backups from current systems
 - Storing documents in a protected environment to ensure availability and security
- **Automated**
 - Engage technology for card usage, entry control systems, & password requirements

Obligations to hold people accountable for

- Ensuring that computer passwords are periodically changed and are not written down, shared with others, or kept nearby
- That purchase card charges are checked against authorizing documents
- Management reports are compared against source documents
- Only authorized personnel are admitted to facilities
- Documented confirmation that a particular policy or procedure was followed (receipts, tracking for mandatory training, account reconciliations).
- Safeguards are built in whenever creating a new process or procedure
- Sampling and cross-checking of activities is done
- Formal/informal observations, inspections, walk-throughs, and interviews are executed

Associated risks to address



Conducting business carries risks

- **Risk represents uncertainty; can be positive or negative**
 - In the context of controls, it refers to something that may prevent an organization from meeting its goals and objectives
 - The possibility that an event may occur and adversely affect the organization's standing
- **Measured by the likelihood of an event occurring (probability) and the impact of the event having a negative effect (severity)**
- **Types of risks:** Strategic, Financial, Regulatory, Reputational, Operational
- **Risk categories:**
 - High risk financial transactions
 - Critical functions
 - Adherence to other legal and regulatory requirements

Management's responsibility

- **Managers are agents of the company with heightened responsibility and liability**
- **Hold them responsible for:**
 - Establishing and maintaining internal controls to ensure:
 - Effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations
 - Application of standards to meet the organization's objectives
 - Assessing internal control effectiveness
 - Communicating updates and changes to internal control policies
 - Training others in associated expectations and role modeling prudent behavior
- **Evaluate them regarding controls:**
 - How they communicate Internal Control requirements and best practices with their staff
 - What they do proactively to prevent issues and mitigate risk
 - Do they demonstrate sound compliance with requirements?
 - Do they appropriately make use of resources?

Compliance risk considerations

Questions to Ask

- What could go wrong? Where could things fall down?
- What must go right to succeed?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- Where do we spend the most money?
- What assets do we need to protect?
- What information do we most rely upon?
- How could someone or something disrupt our operations?

Event Drivers

- Lack of duty segregation
- Approval of documents without review,
- No follow-up when things appear “questionable” or “not reasonable”
- Lack of controls over cash/petty cash, purchasing of materials/supplies, etc.
- Lack of knowledge of policies and procedures and documentation

The risk management process

- **Risk:** Uncertain or chance events that you may or may not be able to overcome or control.

Types:

- Preventable
- Strategy
- External
- **Risk Management**
 - An attempt to recognize and manage potential and unforeseen events that may occur
- **Risk varies widely between functions and activities.**
- **Types:**
 - Biological, chemical, physical
 - Production
 - Ergonomic
 - Psychosocial
 - Compliance
 - Emergency
- **Involve:** IT, operations, HR, and leadership, as well as outside consultants and experts



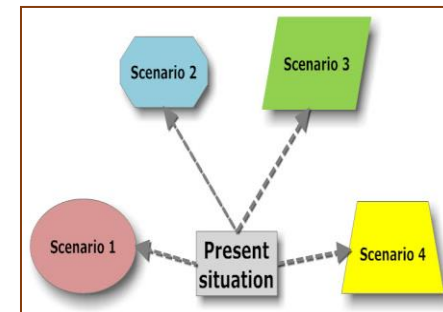
1) Risk identification

- Generate a list of possible risks through brainstorming, problem identification and risk profiling
- Break down processes into steps
 - Identify macro risks first, then those within steps
- **Methods:**
 - brainstorming, nominal group techniques, checklists, attribute listing...
 - Cause-effect diagrams, flow charts, influence charts, SWOT analysis



2) Risk assessment

- Any option or situation involves some level of risk. The key is to consider taking *calculated risks*.
- Conduct a risk assessment based on different degrees of uncertainty
 - Consider probability (likelihood) of occurrence
 - Consider severity (impact) of occurrence
 - Factor in compounding factors



3) Contingency planning

- **Strategize how to minimize or eliminate potential effects**
 - Mitigating Risk
 - Avoiding Risk
 - Transferring Risk
 - Accepting Risk
- **An alternative plan that will be used if a possible foreseen risk event actually occurs**
- **A plan of actions that will reduce or mitigate the negative impact (consequences) of a risk event**
- **Risks of Not Having a Contingency Plan**

4) Ongoing monitoring & control

- **Allocate contingency funds and time buffers**
- **Review critical actions, tasks, and deliverables**
 - Monitor triggering events
- **Compensate for unplanned delays and other disruptive effects**
- **Watch for new risks**
- **Foster an open environment to encourage updates**

Ways to reinforce compliance training



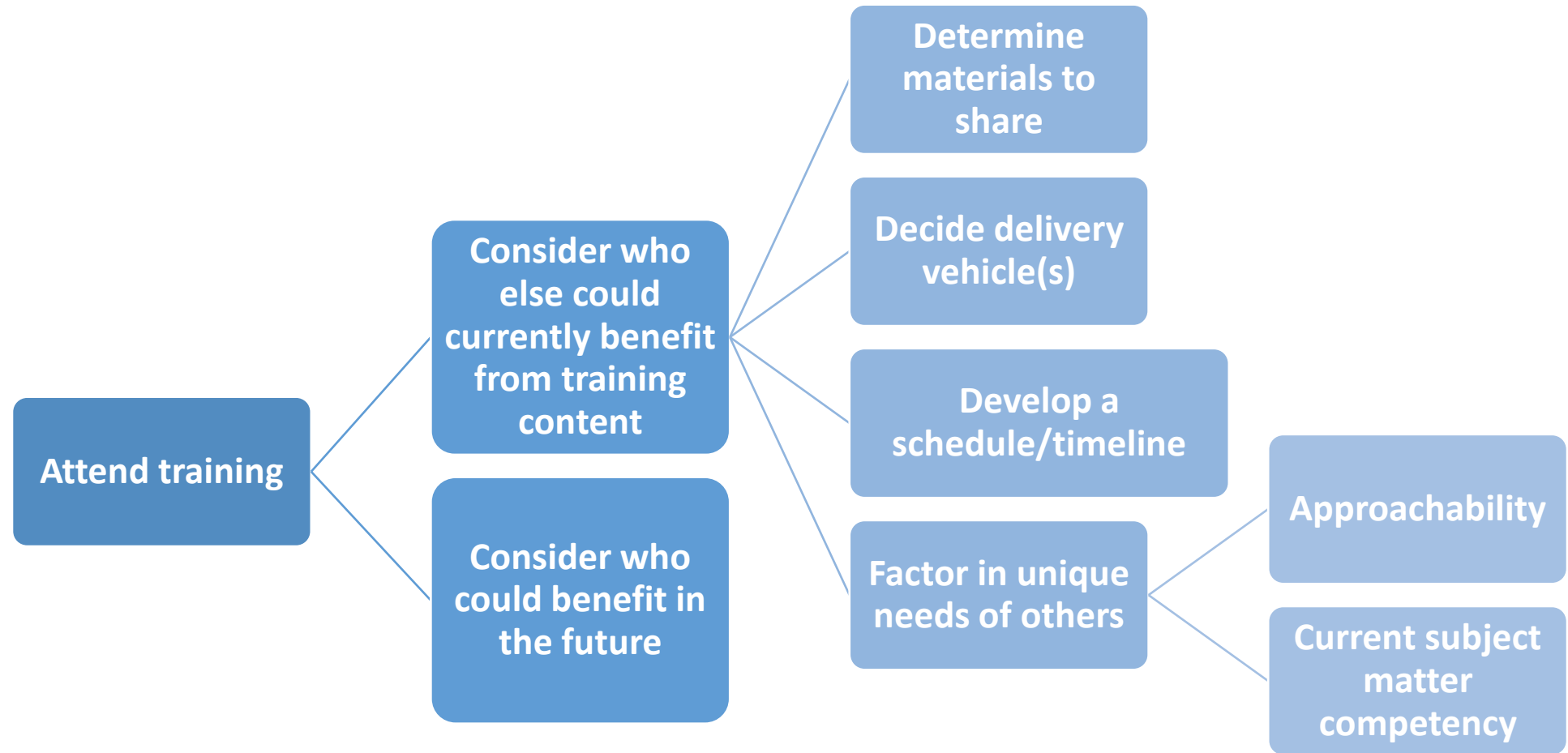
The 70-20-10 Mindset

In a report on trends in executive development, research analysts Bonnie Hagemann and John Mattone describe training and development today and into the future as follows:

As the workplace revolutionizes, learning methods are continuing to shift with the 70-20-10 learning and development model becoming prevalent:

- “70% of learning and development takes place from real-life and on-the-job experiences, tasks, and problem solving. This is the most important aspect of any learning and development plan. For example, the real learning from a skill acquired in a training program, or from feedback, takes place back on the job when the skill of feedback is applied to a real situation
- 20% comes from feedback and from observing and working with role models
- [only] 10% of learning and development comes from formal training”
(Hagemann & Mattone, 2011, p. 3).

My ToT (Training of Trainers) model



Make understanding compliance fun!

- **Don't expect people to stay late or fit it in at the expense of other deadlines**
- **Gamify learning into the workplace**
 - Have healthy competitions
 - Example:
 - Divide employees into groups
 - Ask individuals within the groups a question about information covered
 - If someone gets the answer wrong, they are out
 - After a few rounds, the team with the most members remaining wins the game and a prize
 - Mix in a Jeopardy-like game as a way of reinforcing concepts
 - Give out small prizes to the winners and goofy gag gifts to the losers without disparagement
- **Create video or audio recordings**
 - Condense training into key areas or points
 - Chunk the information into small "bites"
 - Push out the recordings rather than just relying on employees to reach out and access them
 - Show how the associated behaviors work, rather than lecturing
 - Periodically resend the information as a reminder
 - Use the recordings as part of new hire orientation
 - Allows people to learn when it is convenient for them

Ways to heighten awareness & educate others

- **People must hear an idea or concept several times (and in multiple ways) before the information is retained**
- **Communicate using both formal and informal means**
- **Associate internal controls with department/organization mission, goals, objectives, and customer stewardship**
- **Initiate a formal communications plan**
- **Sample communication mechanisms:**
 - Staff meetings, informal one on ones, brown bag lunches
 - Posters, message boards, newsletters, email signature lines
 - Recognize achievements and accomplishments and their application in internal controls
 - Encourage questions
 - Provide job-specific training
 - Include in new employee orientation
 - Provide shared site, Wiki's, or web site information

Motivating employees to care about compliance



Drive a need for accountability

- Accountability begins with clearly defining the results you want and need to achieve
- Accountability is determined proactively, before the fact, not reactively, after the fact
- Advantages
 - Motivates unity and consistency
 - Provides improved efficiency and productivity
 - Promotes workplace synergy
- The drive for accountability is increasing
 - Increased scrutiny of organizations
 - Tighter business environment
 - More media attention



Engage staff in a Management Control Review (MCR)

- **Purpose:** Evaluates management controls and determines how well they promote good stewardship of resources
 - Helps offices operate more efficiently and effectively
 - Tactics for identifying inefficient processes & making lasting improvements
 - Provides reasonable assurance towards achieving the organization's objectives
 - Helps determine areas of vulnerability that could be subject to waste, loss, unauthorized use, or misappropriation
- **Actions:**
 - A) Perform a risk assessment
 - B) Review internal controls
 - C) Report findings
 - D) Monitor implementation of findings

How to prioritize and address findings

- **Decide their relevance and significance, categorizing them as:**
 - Material Weakness: a deficiency, or combination of deficiencies, that results in a likelihood that a significant impact to the organization will not be prevented or detected (Show Stopper)
 - Significant Deficiency: a control deficiency, or combination of control deficiencies, that adversely affects the organization's ability to initiate, authorize, record, process, or report data reliability such that there is a realistic possibility that a consequential impact will not be prevented or detected
 - Control Deficiency: exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misrepresentation on a timely basis
- **Tackle the material weaknesses first, engaging others as appropriate to:**
 - Determine root causes
 - Options to rectify
 - Document solutions and any new procedures
 - Track fixes to ensure they worked

Resources to access & review



- Regulations, policies, directives, procedures
- Annual and strategic plans
- Performance measures
- Delegations of authority
- Budget, personnel, and workload data
- Forms, reports, templates
- Position descriptions, interviews
- Past audits and assessments
- Interactions with other areas, departments and outside entities

What technology can do to assist



Technology considerations

- **Benefits**

- Minimize the amount of manual work
- Reduce the chance of problems, delays, omissions, biases and legal or other inconsistencies
- Frees up time for more strategic work and frees up storage space
- Enhances accessibility from anywhere, any time
- Facilitates secured, encrypted storage

- **What can it do?**

- Complete forms and entries digitally
- Provide information
- Answer commonly asked questions and/or provide a digital chat agent
- Allow for company-specific work-flows based on options/customization
- Provide automated reminders to various participants
- Track and document completion and status of various steps
- Perform data-analytics
- Facilitates the conveyance of knowledge and information

How technology can help

- Assess risk
- Locate impacted people and assets
- Act more rapidly
- Analyze potential outcomes
- Assist in keeping employees safe
- Alerts visitors, vendors, and customers
- Automates digital operations
- Anticipate and prevent operational disruption
- Accelerated assistance
- Use of drones or robots for surveillance and recovery
- Predictive data analytics
- Security
- Sensors & “Digital twins”
- Provides training and timely resources

Optimize your tech platform

- **Define the expected benefits of your technology in quantifiable terms and how it can help support your business goals**
- **Continuously evaluate and improve the technology with the objective of continuously streamlining your processes**
- **Establish metrics and systems of measurement to monitor success and performance**
- **Regularly review performance reports and goals to inform your organization's performance dashboard**
- **Periodically evaluate what external tech solutions exist that may assist you**
 - May be less expensive than doing so in-house
 - May provide superior quality in software and support
 - May assist you in staying compliance
 - May provide early warning signs of potential future issues

What an LMS system can do for you

- **Learning Management System**

- Online integrated software can be used to create, deliver, track, and report educational learning and associated outcomes
- A well-designed LMS allows the business to more easily, quickly, and accurately track utilization, goal progress, knowledge gains, and rate of return on investment (ROI)
- Connects training to learning and learning to results, demonstrating cost savings for individual training investment as well as for reinforcement of compliance requirements, as well as other business expectations
 - Provides robust features that help ensure awareness and understanding of compliance requirements for various laws and regulations
 - Typical training addresses various labor-related topics, such as sexual harassment prevention training, OSHA requirements, HIPAA provisions, workplace diversity expectations related to the U.S. Equal Employment Opportunity Commission (EEOC) and the Americans with Disabilities Act (ADA), as well as company-specific compliance training needs
 - Also helps businesses help their employees stay current with changes and evolutions in laws and regulations



Determine net benefits of external vendors

- **In purchase decisions**
 - Is the solution user-friendly? Push-based or pull-based?
 - Are there reliable measures that demonstrate how it can benefit your organization?
 - Is it flexible? Can it be easily updated? Expanded?
 - Is customization required to meet your needs? How will that be done? Maintained? Evolve?
- **Conduct cost-benefit analysis**
 - Cost-benefit analysis is used to weigh the financial and nonfinancial costs and benefits.
 - Nonfinancial or qualitative data is often assigned a value.
 - There are many ways to do this, from a simple T-chart to a detailed financial analysis.
 - A “break-even analysis” is done to determine at what point the cost equals the benefit.
- **Consider “soft,” indirect costs, such as:**
 - Transition and change management costs
 - Implementation costs (including time)
 - Potential staff replacement costs

Enacting compliant remote work expectations

- **Create a remote work policy**
 - A general policy that addresses position eligibility, work hours, accessibility, and deliverables
 - A policy as part of your company contingency plan
- **Follow legal requirements and constraints**
 - FLSA rules regarding non-exempt employees
 - NLRA rules on “concerted activity” protections to increase workplace safety
 - ADA considerations
 - General health and safety rules and off-site but on-the-job potential liability
 - Paid time off practices
- **Other considerations**
 - Data and record security protocols
 - Required equipment, tools and work environment
 - Technology and other support
 - Off-site inspection and approval protocols
 - *Home, as well as other locations*
 - Creation of objective, verifiable performance criteria

Ways to ensure compliance with laws, regulations, & industry standards

- Include reminders on calendars to check applicable websites
- Reflect associated responsibilities in performance reviews that hold people accountable
- Partner with your legal team and/or outside vendors to screen developments and notify you of updates
- Ensure that all employee handbooks reflect requirements
- Make sure that information is proactively pushed out to employees and also accessible
- Alleviate excess burden by periodically streamlining operations in conjunction with compliance updates
- Be consistent in your expectations of yourself and others
- Reinforce policies through ongoing training and reminders



Today's takeaways...

- Better acknowledge and manage compliance through tracking, engagement, data, and technology
- Create a culture of compliance that motivates employees to care about it

Let's stay in touch!

Michelle Coussens
Plan B Consulting
*practical business planning with you,
for you*

michelledcoussens@yahoo.com

www.linkedin.com/in/michellecoussens/

(312) 685-0055



*Contact me for a
complimentary copy of my
latest monthly newsletter!*

