## Organizational Chart Exercises:

* Analyze the organizational chart and identify key GRC roles
* Identify potential champions or leaders
* Identify areas of possible resistance
* How would you modify the organizational chart?



|  |  |
| --- | --- |
| GRC Champions or Leaders? |  |
| Areas of Possible Resistance? |  |
| Suggestions for Change? |  |

# **LEARN COMPONENT MODULE**

|  |  |
| --- | --- |
|  | Influencing factors on the external context include: |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |

## L1: External Context Exercise

* Write down external context items for your organization
* Share and see what external context items you have in common w

Your Thoughts

## L3: Types of Culture in Organizations

|  |  |
| --- | --- |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |

**L4: Common Stakeholders**

* Owners (shareholders)
* Investors
* Creditors
* Customers
* Directors
* Employees
* Governments
* Suppliers
* Unions
* Non-governmental organizations (NGOs)
* Community
* Governing authority

## A2: Objectives Group Discussion

Write down some of your organization’s objectives considering:

* Strategic,
* Financial,
* Customer,
* Operational,
* Learning and Growth,
* Reporting, etc…

**A5: Technology Quiz**

|  |  |  |
| --- | --- | --- |
| T / F |  | Question |
|  | 1 | Everything must be automated in order to optimize the GRC program. |
|  | 2 | Using consistent tools offers efficiency and more accurate information. |
|  | 3 | GRC professionals should implement technology without the help of IT professionals. |
|  | 4 | An organization should be able to deliver consistent information to those who need it, when they need to know it. |
|  | 5 | It is not necessary to have a single information management system across the organization. |
|  | 6 | Consistent policies and procedures should be implemented regarding the retention and retrieval of information. |
|  | 7 | Communications within the organization and to external stakeholders should be done on an ad hoc basis. |
|  | 8 | GRC is really just a technology solution. |
|  | 9 | Most organizations will require multiple technology solutions that work together. |
|  | 10 | It is unacceptable to use any existing processes or solutions. New GRC technology solutions must be installed for an effective GRC program. |

## R2: Assurance Exercise

For each assurance project listed, determine the best group to provide assurance from the following list:

* External auditor
* Internal auditor
* Second line of defense function
* Control owners or management
* Government regulator
* Third-party expert

|  |  |
| --- | --- |
| Assurance Project | Assurance Provider |
| 1 - Fair presentation of the annual financial statements in accordance with generally accepted accounting principles (GAAP). |  |
| 2 - Operating effectiveness of actions and controls, implemented by control owners to manage risk to be within the decision-making criteria, set by the governing authority. |  |
| 3 - An organization’s compliance with national tax laws. |  |
| 4 - The effectiveness of the organization’s commodity risk management trading operations and its use of derivatives, futures and forward contracts compared to the industry. |  |
| 5 - Determine the operating effectiveness of the organization’s education process related to bribery and corruption risk. |  |
| 6 - Self-assessment on the use of actions and controls related to financial reporting risks. |  |
| 7 - Assurance to the governing authority that the annual risk assessment and risk management action plans by management are in accordance with the decision-making criteria. |  |

P1: Controls Exercise

From the listing of example actions and controls, select the type of control from the following options:

* Proactive
  + Incentive
  + Preventive
* Detective
* Responsive
  + Corrective
  + Rewarding

|  |  |
| --- | --- |
| Sample Action & Control | Type of Control |
| 1 - Requiring a manager approval for any expenditure processed through accounts payable greater than $500. |  |
| 2 - Providing a cash payment (up to 5%) of fraudulent expenses or recoveries to individuals who notify the organization of fraud, abuse or undesirable activities, through the organization’s whistleblower hotline. |  |
| 3 - Paying a salesperson a percentage of gross margin on sales he/she makes during a month. |  |
| 4 - A system generated exception report listing potential duplicate payments from accounts payable. |  |
| 5 - Disciplinary actions for employees who have been found to have engaged in undesirable actions as a result of an internal investigation. |  |
| 6 - A management dashboard tracking the progress of IT system implementation projects. |  |
| 7 - A knowledge assessment quiz for new employees at the end of the code of conduct training. |  |
| 8 - Safety guards on machinery. |  |
| 9 - Project team party upon successful completion of a project milestone. |  |

|  |  |
| --- | --- |
| 10 - A policy requiring all contracts with indemnity clause, duration of more than one year or total obligation of more than $10,000 to be reviewed and approved by the legal department. |  |

## P3: Communication Exercise

For each example provided, determine the most appropriate communication method from the following:

* Paper-based
* E-mail
* Websites
* Postings
* Live events or meetings
* Video / audio broadcasts
* Face-to-face personal communication

|  |  |
| --- | --- |
| Example | Communication Method |
| 1 - Announce a new dress code policy for a specific organizational location. |  |
| 2 - Provide a listing of all policies and copies of all current policies. |  |
| 3 - Reminder training about key aspects of the organization’s code of conduct. |  |
| 4 - Provide real-time feedback on an employee’s performance. |  |
| 5 - Provide information on a new policy that affects employees who do not have a computer in their job space. |  |
| 6 - Update on a change in procedure to accounts payable employees. |  |
| 7 - Provide information about an upcoming internal audit to an auditee. |  |

## P7: Exercise - Survey Questions

Assess the survey questions asked in the prior year and determine what changes may be necessary for this year’s survey.

|  |  |
| --- | --- |
| Prior Year Survey Questions | Suggestions & Comments |
| My supervisor sets a good example of how to live up to the Company’s values |  |
| I have observed misconduct during the last year |  |
| Pleasing and delighting the customer at all cost is my most important job |  |
| Management sets a good example of how to live up to the value of Speed to Market |  |
| I am given the resources I need to do my job effectively |  |
| I am personally responsible to ensure the company meets its profitability goals |  |
| I agree with the Code of Conduct |  |
| I know we have a company hotline |  |
| I have informed my supervisor of any misconduct I have observed during the last year |  |
| ABC Company is a great place to work |  |

## SAMPLE QUESTIONS AND ANSWERS GRC PROFESSIONAL EXAM v3.0

1. Principled Performance represents the achievement of:
   1. Senior management supported objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
   2. Fully funded objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
   3. All of the objectives that an organization chooses to pursue while employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
   4. The most critical objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
2. An integrated approach to GRC involves:
   1. Consolidation of the technology infrastructure related to GRC processes
   2. Consolidation of the various risk silos
   3. Applying a common vocabulary, approach and technology infrastructure to GRC processes
   4. Consolidation of governance, risk and compliance processes
3. Which is the best description of a Risk Management Action Plan?
   1. A document that sets out the strategy, structures, processes, activities and resources to appropriately manage the organization's risks to reduce or avoid adverse effects and grasp opportunities
   2. A document that identifies each risk and its classification by type, source and level of impact
   3. A plan for how the organization will identify and grasp opportunities presented to it
   4. A plan that includes the strategy and rationale for addressing each category of risk with particular approaches
4. A threat is:
   1. A type of risk
   2. A measure of likelihood that an adverse event will take place
   3. An event or condition that has, on balance, an undesirable effect on achieving objectives
   4. Always an external force that can harm the organization
5. Which of the following would NOT be appropriate when monitoring the external context?
   1. Having only one source of information about each item being monitored
   2. Changing approaches to monitoring when entering new markets or geographies
   3. Monitoring the development of new technologies
   4. Identifying a key owner for each aspect of the external environment being monitored
6. Why do you need to analyze the current and planned approaches to addressing opportunities, threats and requirements?
   1. To be able to determine if the inherent, actual and planned residual levels of risk, reward and conformance are acceptable
   2. To be able to assign responsibility for monitoring changes in approaches to risks, rewards and conformance in a given category to one person
   3. To be able to have the same crisis management plan for all risks
   4. To be able to take steps to mitigate entire categories of risks or address entire categories of a potential reward
7. Which of the following is NOT true?
   1. A code of conduct may be required by law, regulation or other authority for certain roles or positions in the organization
   2. An organization should always have only one code of conduct that applies to everyone throughout the organization
   3. The code of conduct may contain guidelines for responsible decision-making when the code, other guidance or law, is unclear
   4. The code of conduct will be ineffective if it is written at a level of language its intended audience does not understand
8. When establishing procedures for investigating complaints or reports about compliance or ethical issues, an organization must:
   1. Define policies and procedures designed to make sure that the confidentiality of all reported information is protected
   2. Define policies and procedures to ensure that the board is aware of all compliance and ethical issues
   3. Define categories of issues that are significant enough to be escalated to senior management and/or an outside counsel immediately upon validation
   4. Define policies and procedures that ensure that such complaints or reports are never handled directly by the line management
9. Which of the following would not be considered an external stakeholder or influencer of opinion?
   1. The Board of Directors
   2. A non-governmental organization
   3. Local media in areas where the organization operates
   4. Regulators
10. Why is it important to establish formal values and objectives for the organization?
    1. In the absence of a clear mission, vision and values statement, the organization will operate on the values defined ad hoc or by individuals based on their own beliefs and interests
    2. A written values statement can substitute for leadership demonstrating the desired behavior of the workforce
    3. In the absence of organizational values and objectives, legal mandates will replace the organization's right to establish its own values
    4. Organizational values and objectives provide a defense to charges that the organization does not have an effective compliance program
11. Which of the following is a potential source of failure when establishing an approach to integrate and align the GRC capability with the business?
    1. Re-using technologies that are already serving needs in the organization for some aspects of the GRC capability, rather than putting all new technology in a place that is designed to manage and analyze GRC information
    2. Establishing a centralized system for maintaining GRC information in a way that it can be accessed by different departments and functions
    3. Not assigning a clear accountability for all key aspects of the GRC capability
    4. Viewing establishment or alteration of the GRC capability as a change activity that requires special management rather than it being just a part of ongoing business
12. A common mistake in setting up notification pathways is:
    1. Designing the capability so stakeholders can trust that concerns are taken seriously
    2. Encouraging stakeholders to raise concerns directly with the organization instead of going directly to external channels
    3. Using technology resources as the pathway to provide notification
    4. Not capturing all notifications made via informal methods or unstructured channels
13. What is a GRC curriculum plan?
    1. A plan setting out the order and timing of all courses for a particular role or family of roles, which may include a description of each course, its objectives and method/mode of delivery
    2. A plan setting out the names of all courses and training programs offered to the workforce by the organization
    3. A plan describing what the organization intends to offer as training about GRC to the workforce, for approval by the board
    4. A table of contents for the organization's training course about the GRC capability
14. What are proactive actions and controls?
    1. Specified process steps or actions that will allow the organization to identify misconduct as it occurs
    2. Specified process steps or actions that will reduce the likelihood and impact of undesirable events, activities or behavior
    3. Technology controls that detect the opportunity for misconduct or adverse events and prevent them from occurring
    4. Technology and processes that help the organization to correct any detected instances of misconduct before an adverse impact arises
15. Which of the following statements is NOT correct?
    1. Assurance should focus on the ability of the GRC capability to meet its objectives while being consistent to the decision-making criteria
    2. Assurance desired may vary at different times and for different purposes
    3. Assurance efforts are most effective when a risk-based approach is used
    4. Assurance should be performed by individuals who have the deepest understanding of the actions and controls