How to Purchase Risk Management Solutions & Platforms

Critical Capabilities & Considerations for Evaluation of Solutions

January 2016

Michael Rasmussen, J.D., GRCP, CCEP

The GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

Licensed Subscriber Use Only. Do Not Distribute

Terms & Conditions . . .

- ✓ **GRC 20/20 Research Briefings are copyrighted and protected material**. Content cannot be reused or distributed without written permission from GRC 20/20 Research, LLC.

- ✓ ***GRC Advisor Enterprise Subscribers*** get access to live and recorded Research Briefings for all employees for INTERNAL use only through the GRC 20/20 website. If they wish to have a recording to host internally there is a fee for this.

- ✓ ***GRC Basic Subscribers*** pay for either **individual** access to specific GRC 20/20 Research Briefings. ***Individual access*** is for the individual only and slides or login are not to be shared with others or viewed as a group.

Licensed Subscriber Use Only, Do Not Distribute

Two Things to Note . . .

Complimentary Inquiry

- Organizations evaluating or considering GRC solutions are free to ask GRC 20/20 on our understanding and comparison of solutions in the market to meet your GRC requirements.
- Inquiries are single focused questions that can be answered in under 30 minutes.
- Complimentary inquiry is only available to organizations evaluating or considering GRC solutions for their internal use.

RFP Development & Support

- GRC 20/20 has an extensive library of RFP requirements across a range of GRC capability areas presented in this presentation.
- GRC 20/20 can be engaged in RFP development and support projects to streamline your process, gain perspectives learned from other organizations, and to keep solution providers honest in their responses.

Licensed Subscriber Use Only, Do Not Distribute

Our Agenda . . .

- **Defining & Understanding Risk Management**

  Definition, Drivers, Trends & Best Practices

- **Critical Capabilities of a Risk Management Solution/Platform**

  What Differentiates Basic, Common, & Advanced Solutions

- **Considerations in Selection of a Risk Management Solution/Platform**

  Decision Framework & Considerations to Keep in Mind

- **Building a Business Case for a Risk Management Solution/Platform**

  Trajectory of Value in Effectiveness, Efficiency & Agility

Licensed Subscriber Use Only, Do Not Distribute

Realize that everything connects to everything else.

Leonardo da Vinci

Licensed Subscriber Use Only, Do Not Distribute

Chaos Theory: the simple flutter of a butterfly's wings creates tiny changes in atmosphere that can ultimately impact the development and path of a hurricane.

Business is chaos theory realized in which a small event actually develops and influences what ends up being a significant event.

If we fail to see the interconnections of risk on the non-linear world of business the result is often exponential to unpredictable.

In a linear system effect is proportional with cause, in the non-linear world of business it is exponential. It is not a simple equation of 1 + 1 = 2. It is a mesh of exponential relationship and impact in which 1 + 1 = 3 or 30 or 300.

Licensed Subscriber Use Only, Do Not Distribute

The Chaos of Risk Interconnectedness

Are you truly aware of your risks?

Never in all history have we harnessed such formidable technology. Every scientific advancement known to man has been incorporated into its design. The operational controls are sound and foolproof!

E.J. Smith,
Captain of the Titanic

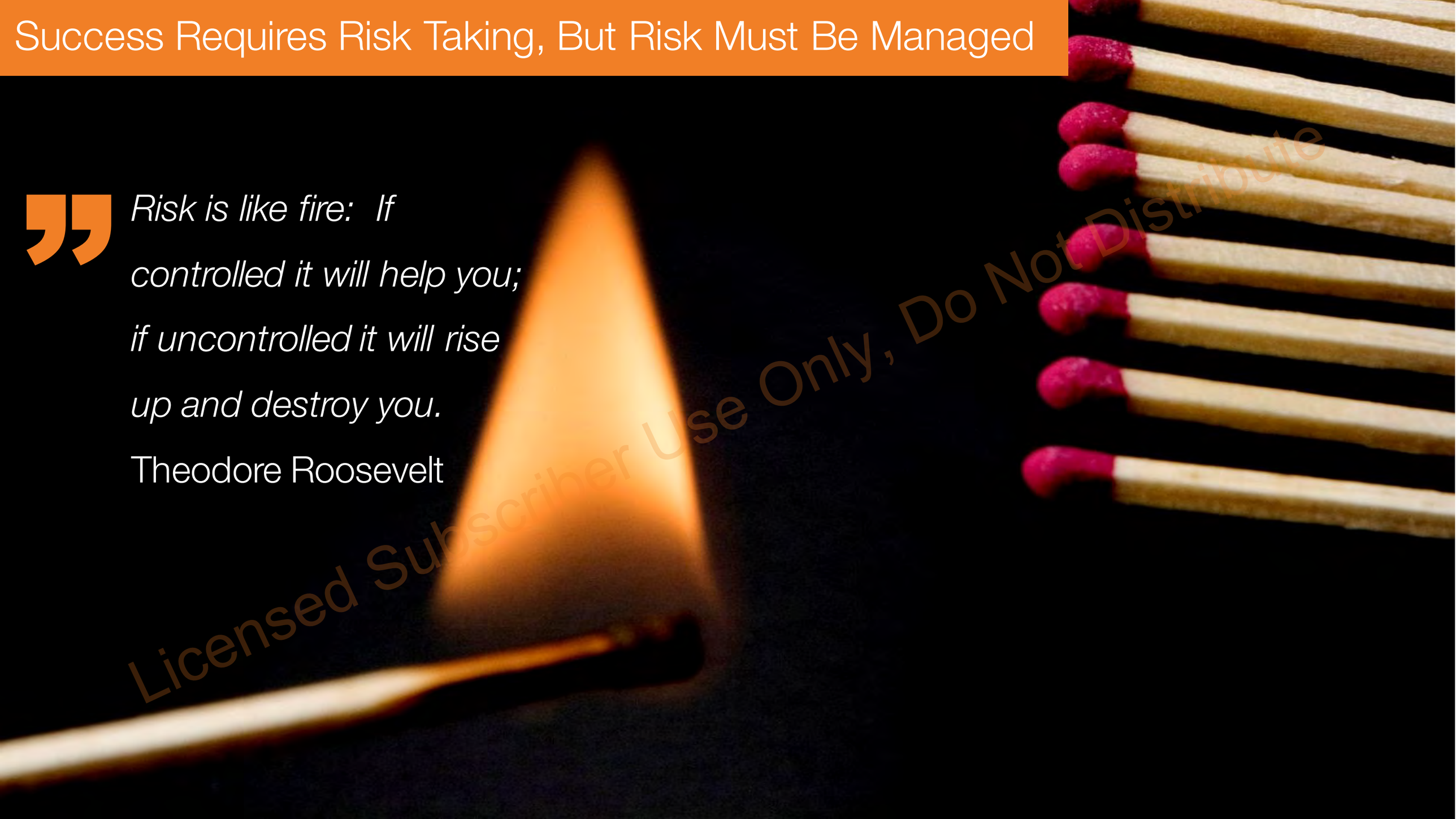
Licensed Subscriber Use Only. Do Not Distribute

The Organization Has to be Able to See . . .

- ❑ **The Tree.** The individual area of risk
- ❑ **The Forest.** The interconnectedness of risks

Licensed Subscriber Use
Do Not Distribute

Success Requires Risk Taking, But Risk Must Be Managed



Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.

Theodore Roosevelt

Licensed Subscriber Use Only, Do Not Distribute

Change is the Greatest Challenge Impacting Risk Management

REGULATIONS

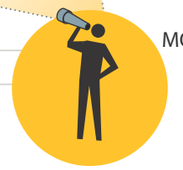
COURT RULINGS

LEGISLATION

ENFORCEMENT

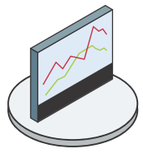
Regulatory/Legal Change

Monitor change in the legal and regulatory environment to determine how pending legislation, court decisions, new/changing regulations, and enforcement actions affect current and needed policies.



MONITOR

contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series



MARKET FORCES

GEO-POLITICAL

COMPETITIVE FORCES

INDUSTRY

SOCIETAL FORCES

TECHNOLOGY

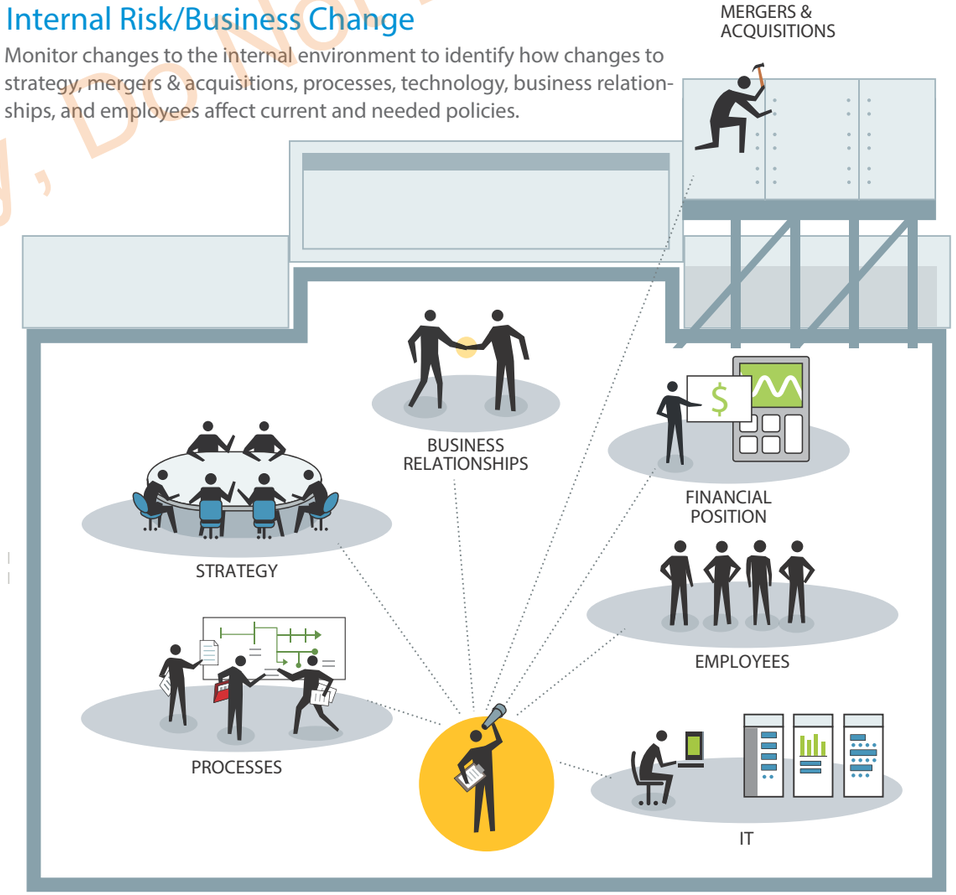
External Risk Change

Monitor change in the external risk environment to determine how uncertainty in economic, geo-political, environmental, industry, societal, and market forces affect current and needed policies.

contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series

Internal Risk/Business Change

Monitor changes to the internal environment to identify how changes to strategy, mergers & acquisitions, processes, technology, business relationships, and employees affect current and needed policies.



contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series

Licensed Subscriber Use Only, Do Not Distribute

Inevitability of Failure: Too Many Approaches

There are too many departments sending too many communications in different formats. Risk management is buried in documents, spreadsheets & emails.

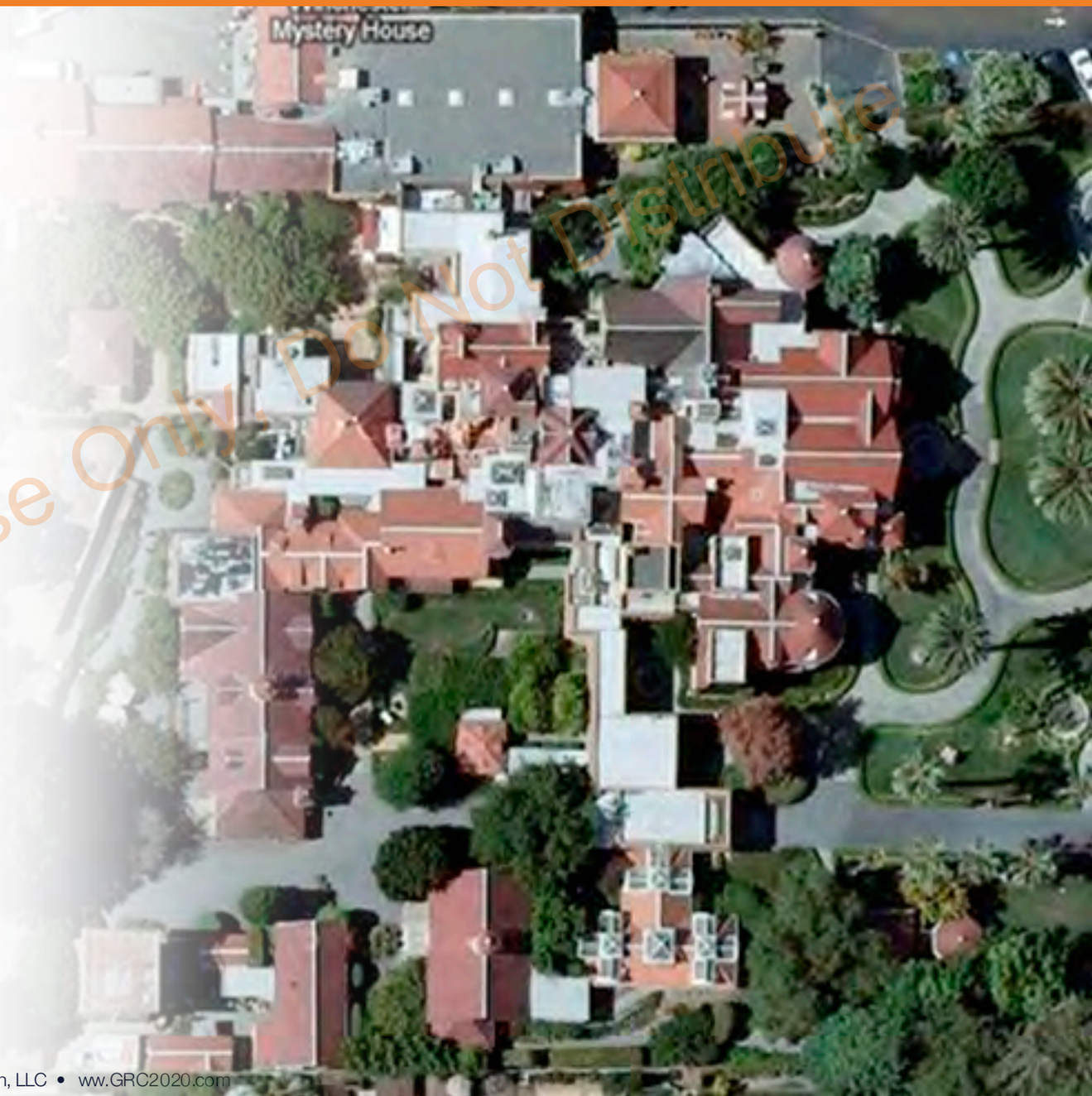
- Wasted resources through redundancy & overlap
- Excessive emails, documents, and paper trails
- Poor visibility & reporting
- Files and documents out of sync
- Overwhelming complexity
- Lack of accountability

Licensed Subscriber Use Only, Do Not Distribute

Confusing Conundrum of Risk Management Processes & Information

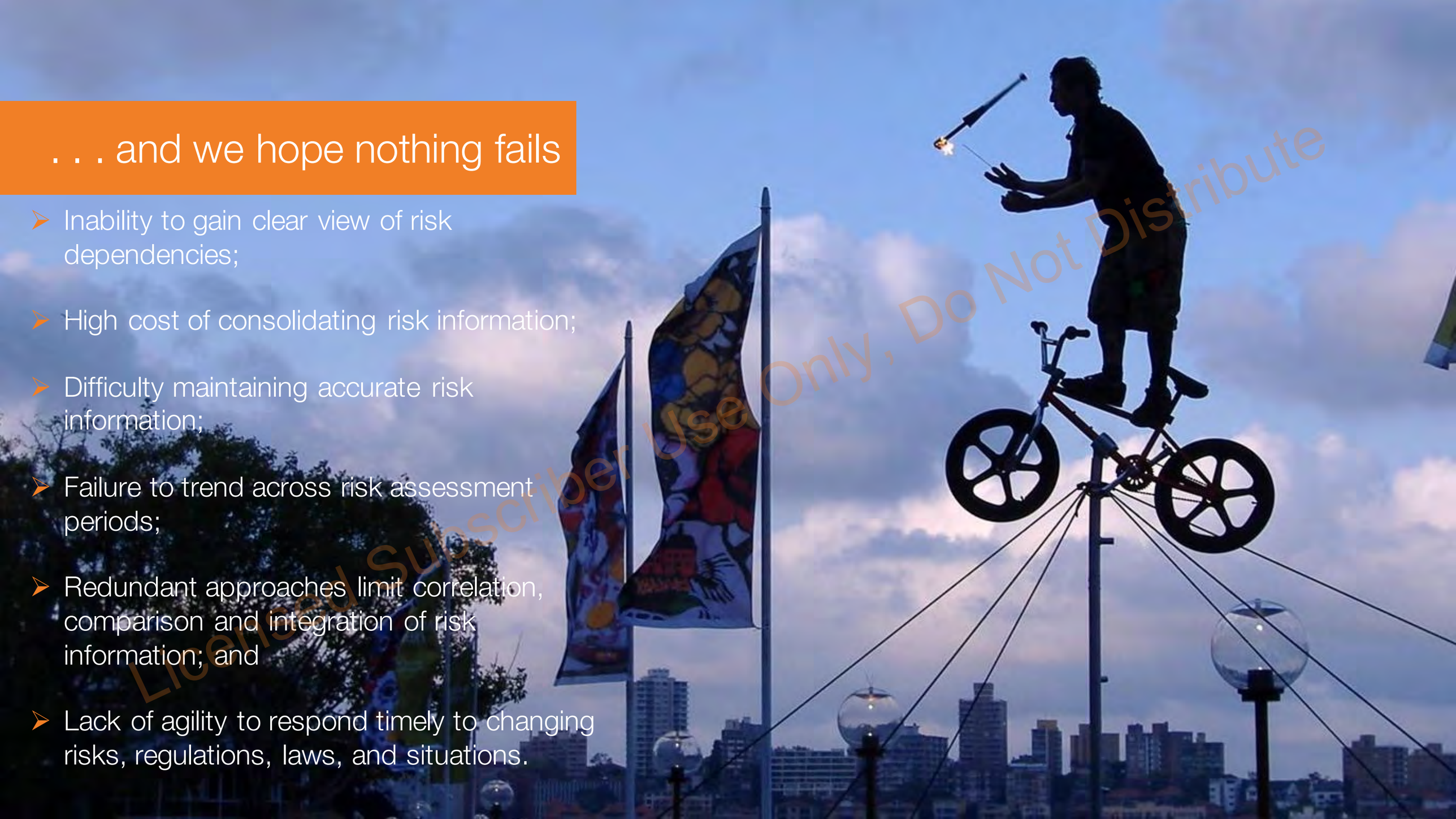
The Winchester Mystery House

- 160 rooms
- 47 fireplaces
- 6 kitchens
- 10,000 windows
- 65 doors to blank walls
- 13 staircases abandoned
- 25 skylights – in floors
- 147 builders/no architects
- Built without a blueprint
- $5.5 million over 38 years



Licensed Subscriber Use Only. Do Not Distribute

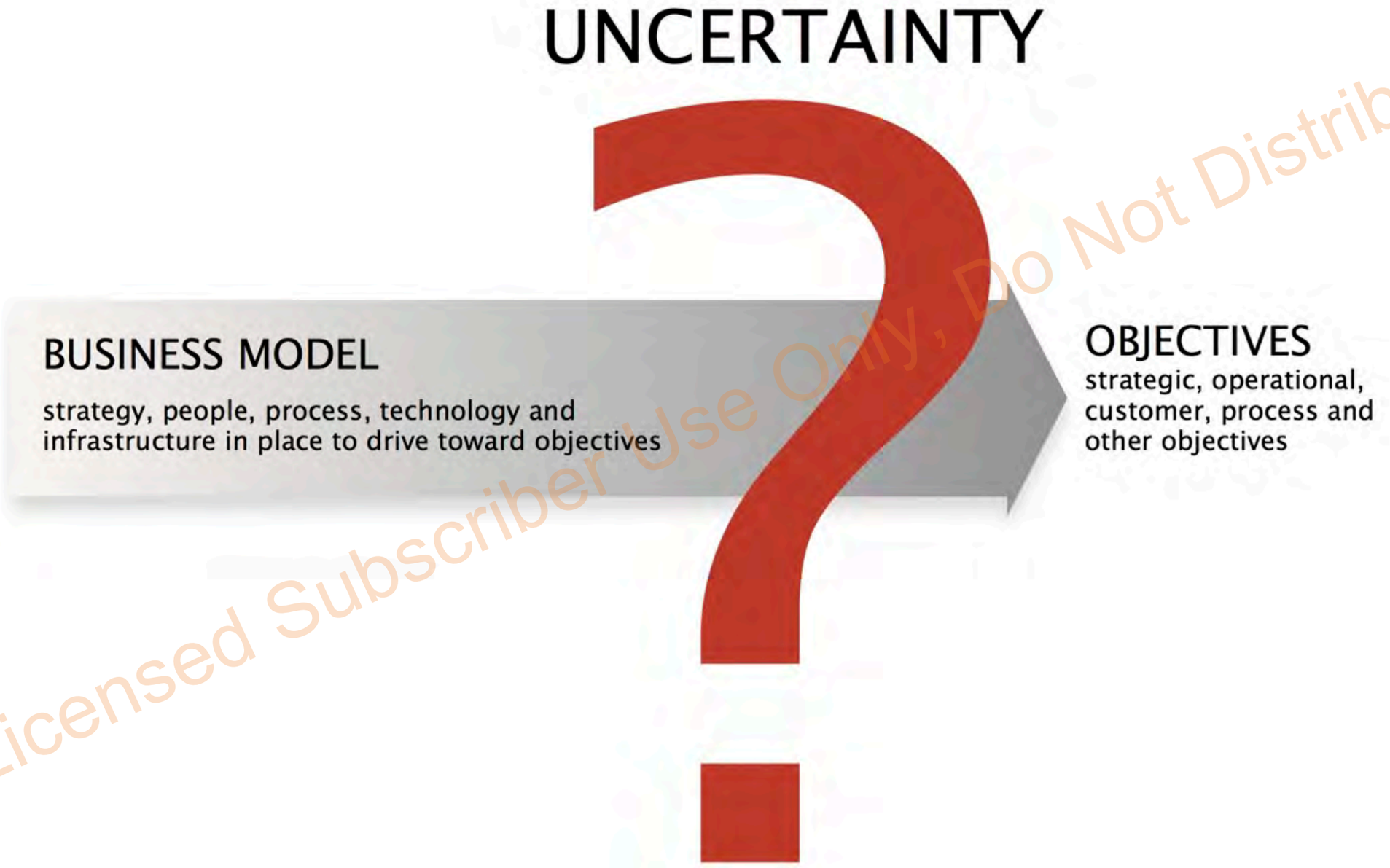
. . . and we hope nothing fails



- Inability to gain clear view of risk dependencies;
- High cost of consolidating risk information;
- Difficulty maintaining accurate risk information;
- Failure to trend across risk assessment periods;
- Redundant approaches limit correlation, comparison and integration of risk information; and
- Lack of agility to respond timely to changing risks, regulations, laws, and situations.

Licensed Subscriber Use Only, Do Not Distribute

Risk Management = Managing Uncertainty in Context of Objectives



Licensed Subscriber Use Only, Do Not Distribute

Risk management is the core of GRC . . .

> *GRC is the integrated collection of capabilities that enable an organization to:*
>
> ***G)*** *reliably achieve objectives*
>
> ***R) while addressing uncertainty*** *and*
>
> ***C)*** *acting with integrity.*

SOURCE: OCEG GRC Capability Model

Governance, Risk Management & Compliance in Context

Governance

Governance sets the context for risk management, without context risk management fails.

Risk Management

Risk management assesses and monitors risk within the context to take action on risk through acceptance, avoidance, mitigation, or transfer.

Compliance

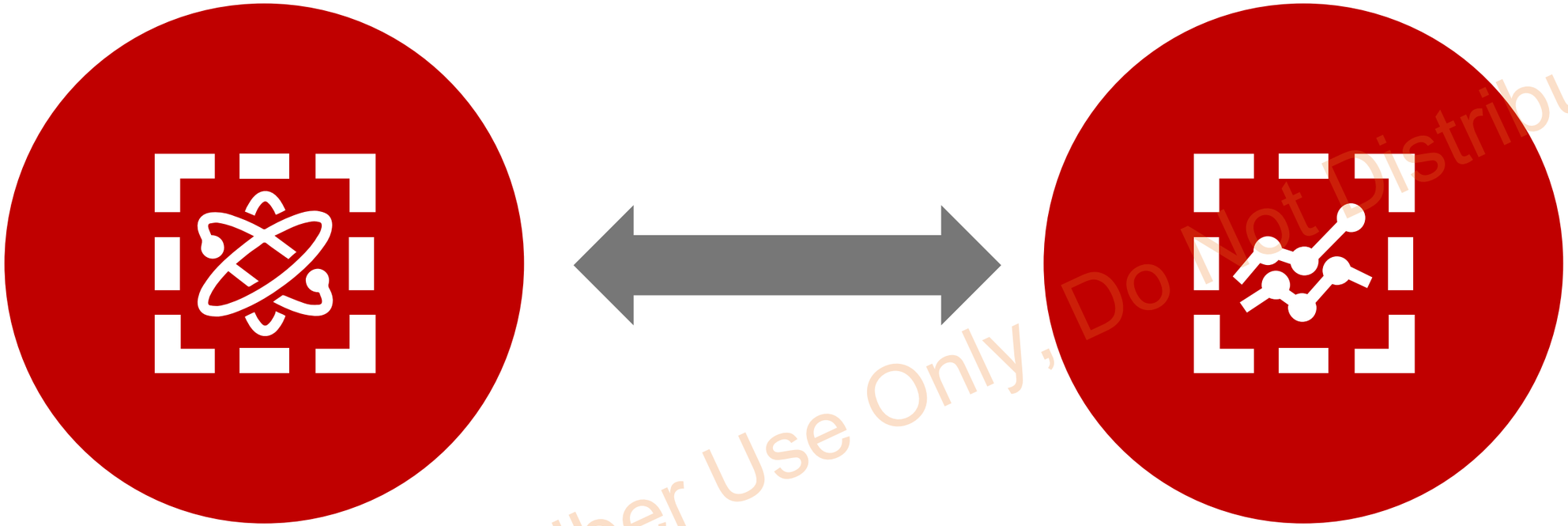
Compliance follows through on risk treatment plans to assure that risk is being managed within limits and controls are in place and functioning.

Licensed Subscribe , Do No tribute

Risk Management is Often a Distributed & Disconnected Function

Licensed Subscriber Use Only - Not Distributable

Catch 22: The Risk in Risk Management



Model Risk

Interpretation Risk

Subscriber Use Only, Do Not Distribute

> *It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit.*
>
> Sir Arthur Conan Doyle
> (British Physician and Writer)

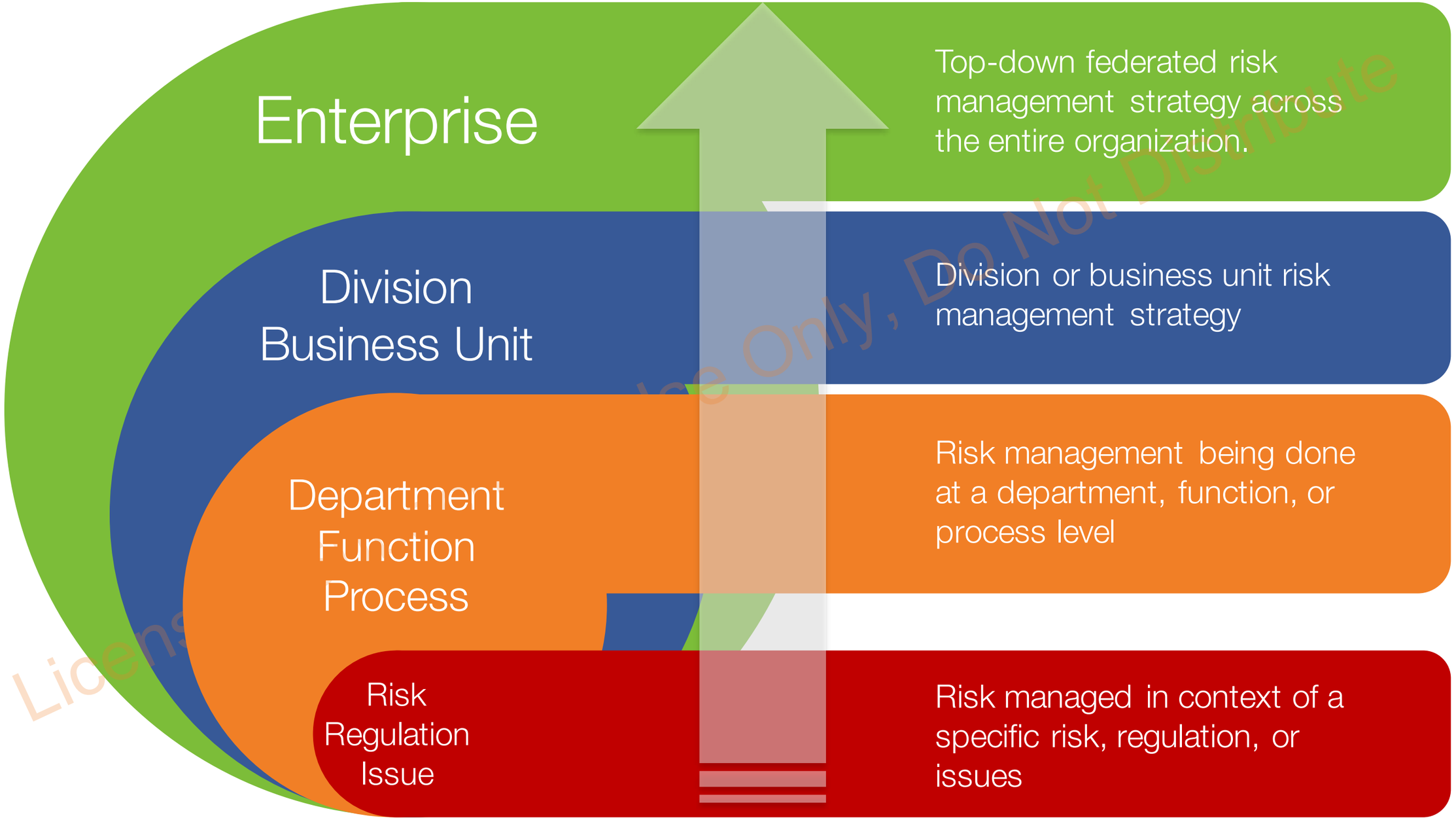
> *You can use all the quantitative data you can get, but you still have to distrust it and use your own intelligence and judgment.*
>
> Alvin Toffler
> (American Author and Futurist)

Risk Questions the Organization Needs to Ask . . .

- ✓ Does the organization have enough information to make decisions about the future of the company, when they don't have a clear view of risk that impacts critical business operations and processes?
- ✓ Does the organization know its risk exposure at the enterprise, business process, and technology levels and how they interrelate?
- ✓ How does the organization know it is managing and mitigating risk effectively in the context of the business to achieve business goals?
- ✓ Can the organization accurately gauge the impact of risk on business strategy, objectives, and operations?
- ✓ Does the organization get the information it needs to take timely action to risk exposure to avoid or mitigate loss and situations of non-compliance?
- ✓ Does the organization monitor key risk indicators across key IT systems, processes, and information?
- ✓ Does the organization optimally measure and model risk in a business context?

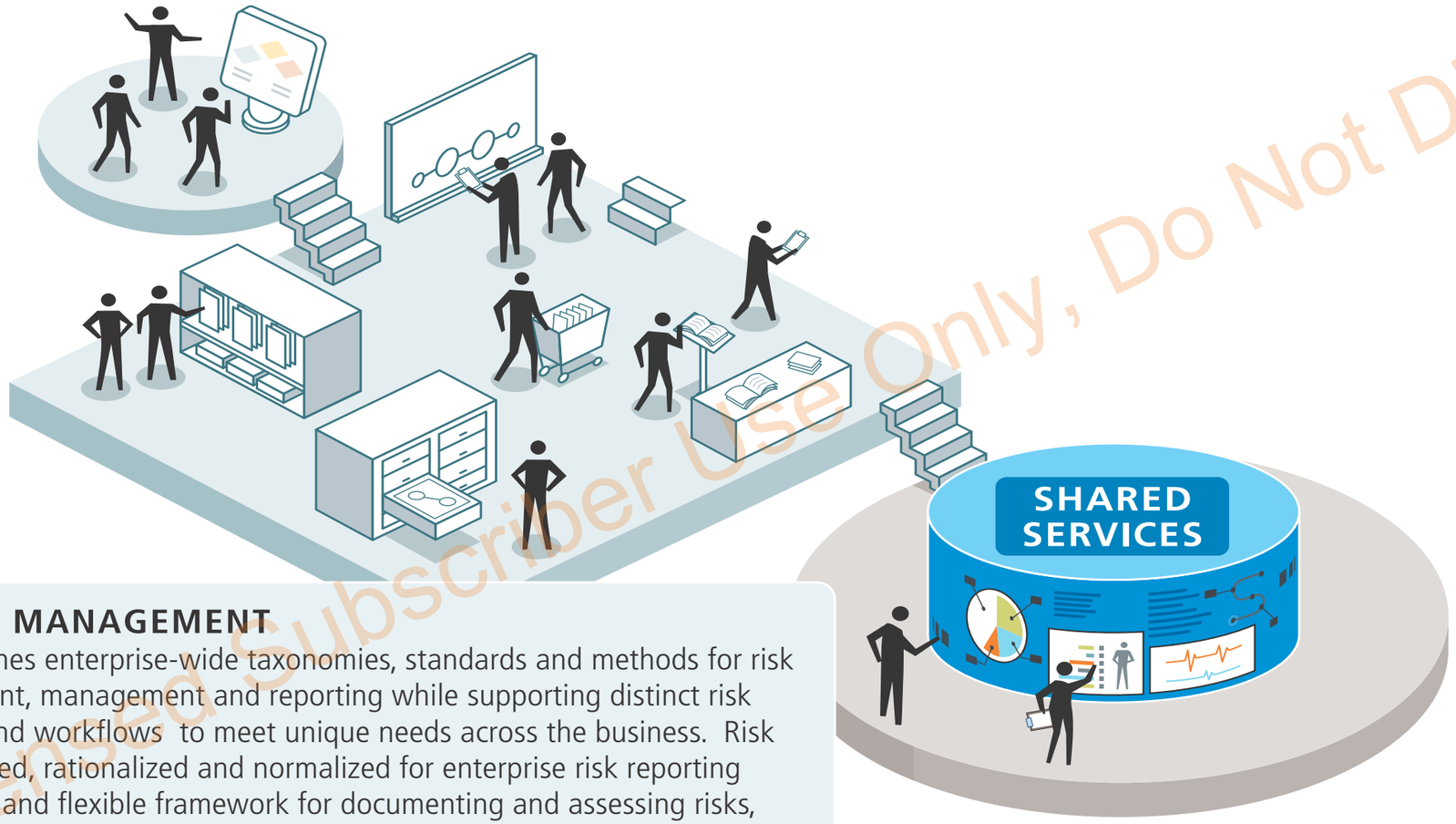
Licensed Subscriber Use Only, Do Not Distribute

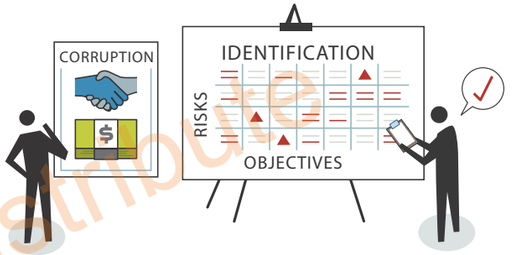
Varying Levels of Risk Management



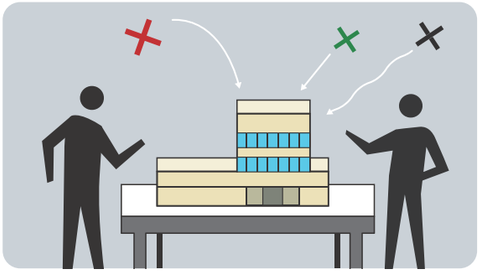
Licensed for Use Only, Do Not Distribute

Federated Risk Management: Layered Approach to Risk Governance

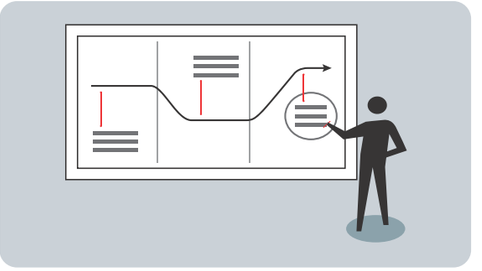




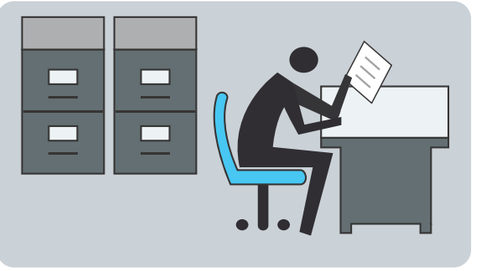
ANALYZE RISKS



UNDERSTAND HISTORY



REVIEW EXISTING POLICIES



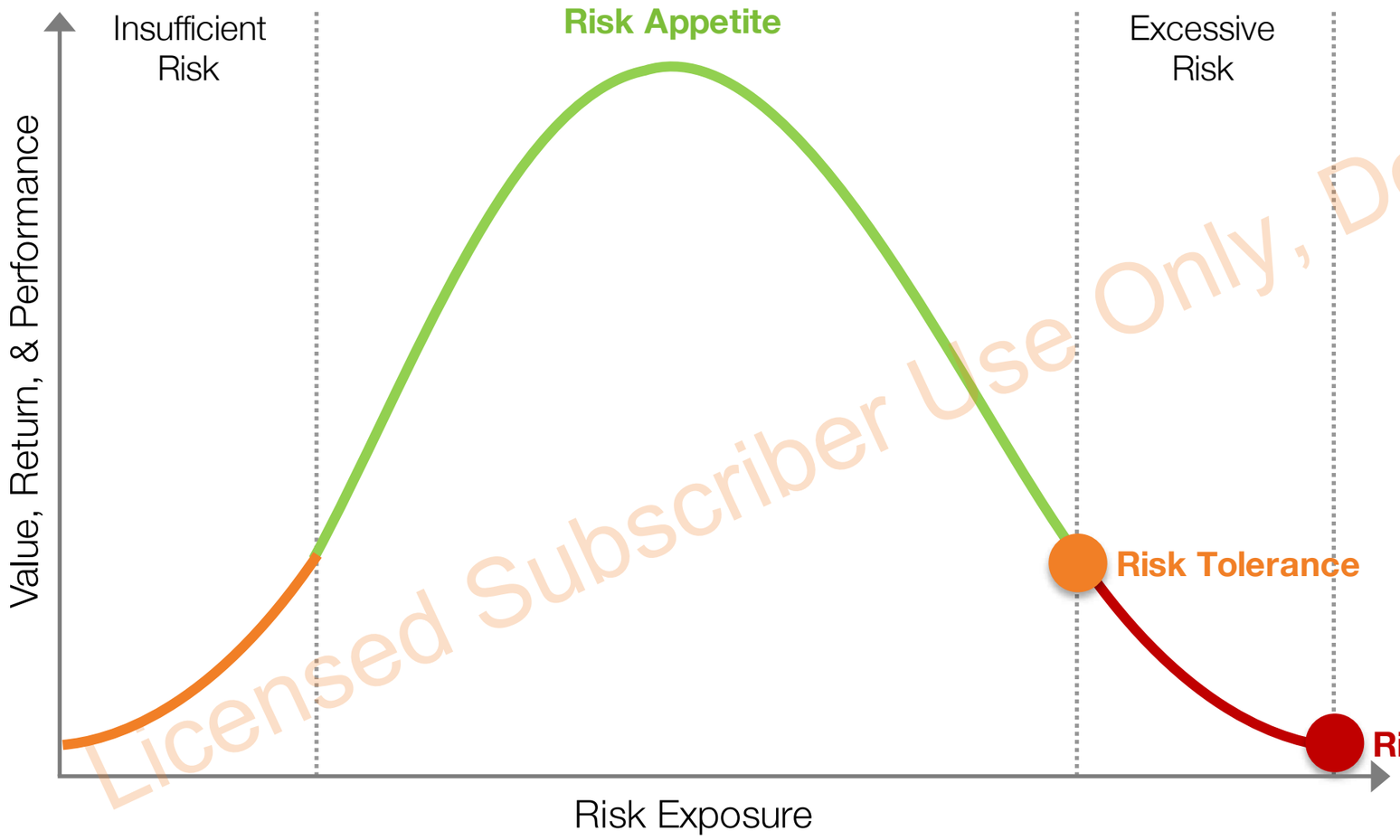
FEDERATED RISK MANAGEMENT

Federated GRC establishes enterprise-wide taxonomies, standards and methods for risk identification, assessment, management and reporting while supporting distinct risk methods, taxonomies and workflows to meet unique needs across the business. Risk information is aggregated, rationalized and normalized for enterprise risk reporting based on an integrated and flexible framework for documenting and assessing risks, defining controls, managing assessments, identifying issues, and implementing recommendations and remediation plans.

Licensed Subscriber Use Only, Do Not Distribute

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests
©2013 OCEG visit www.oceg.org for other installments in the GRC Illustrated Series

Understanding the Balance of Risk Management

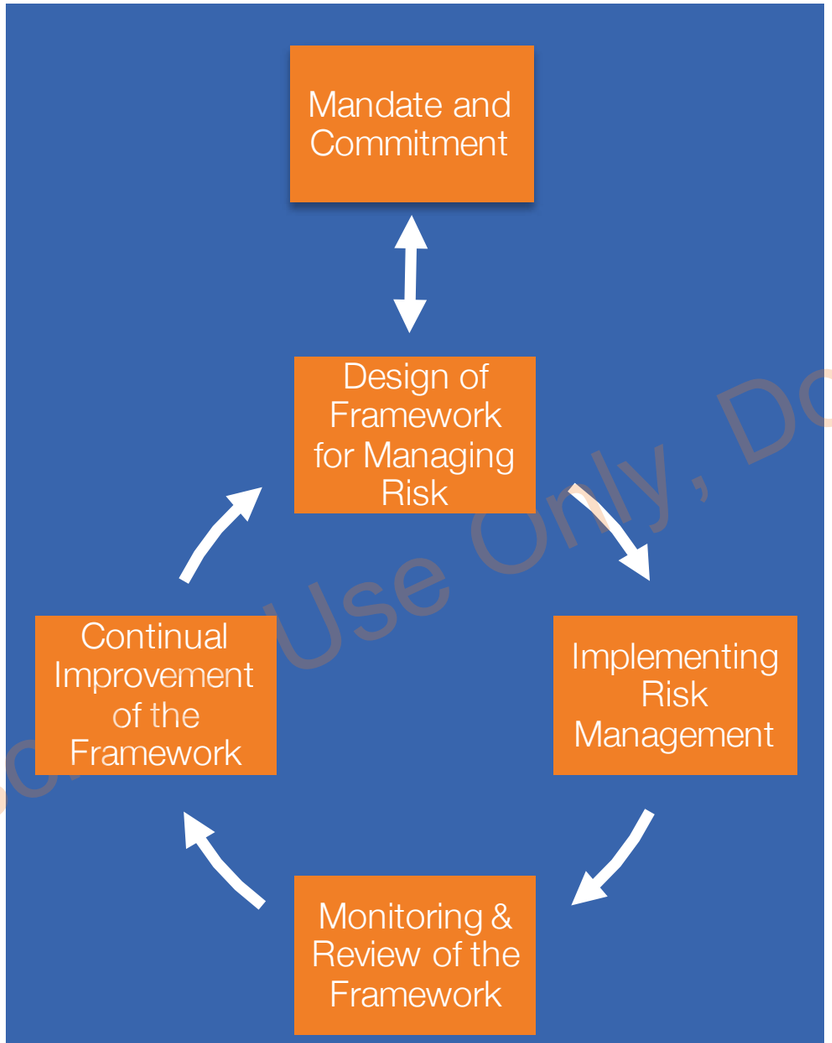


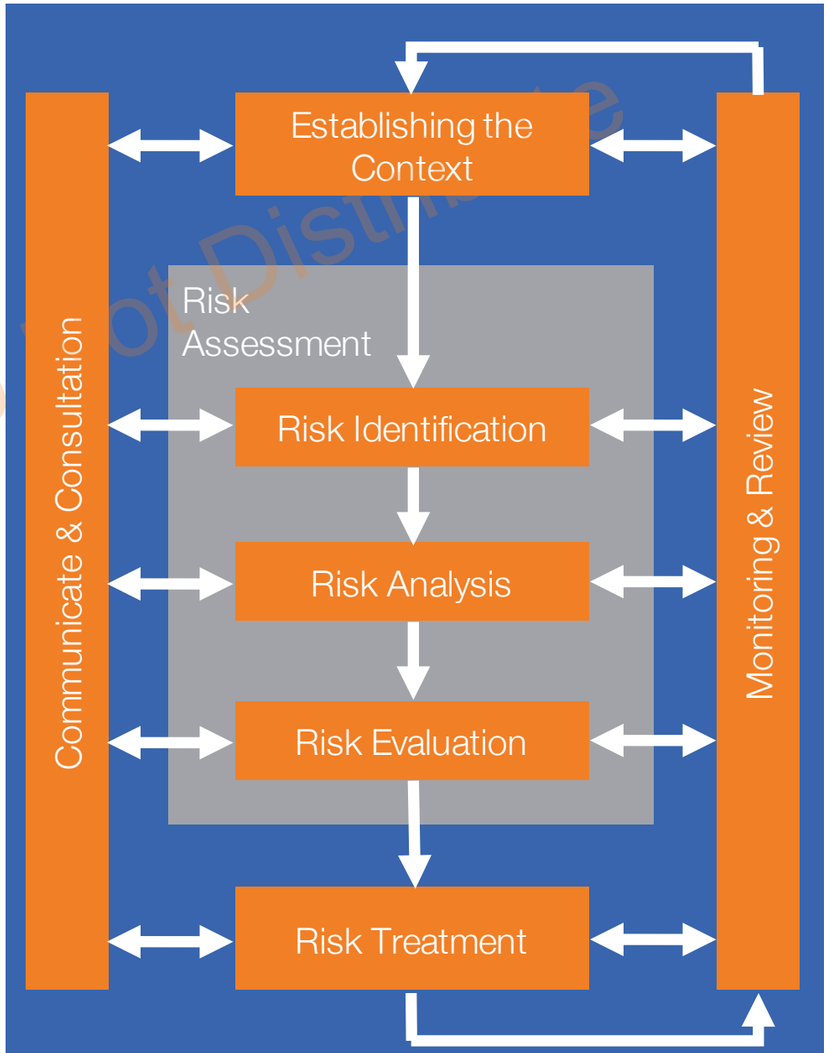
- **Risk Appetite** the level of risk that the organization is willing to accept to achieve objectives
- **Risk Tolerance** the level of risk that the organization is unwilling to exceed to achieve objectives.
- **Risk Capacity** the maximum level of risk that the organization is able to address.

Licensed Subscriber Use Only, Do Not Distribute

ISO 31000:2009 Risk Management

- ✓ Creates value
- ✓ Integral part of organizational processes
- ✓ Part of decision making
- ✓ Explicitly addresses uncertainty
- ✓ Systematic, structured and timely
- ✓ Based on the best available information
- ✓ Tailored
- ✓ Takes human and cultural factors into account
- ✓ Transparent and inclusive
- ✓ Dynamic, iterative and responsive to change
- ✓ Facilitates continual improvement and enhancement of the organization





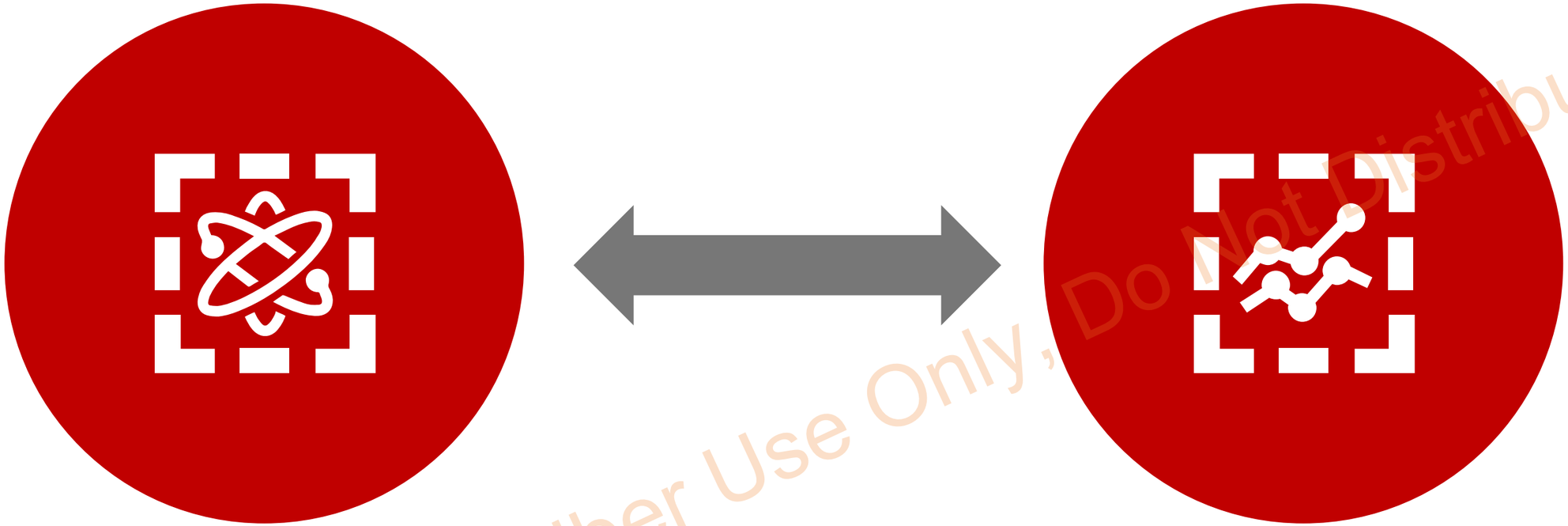
1) Risk Management Principles

2) Risk Management Framework

3) Risk Management Process

Licensed Subscription Use Only, Do Not Distribute

Catch 22: The Risk in Risk Management



Model Risk

Interpretation Risk

Subscriber Use Only, Do Not Distribute

> It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit.
>
> Sir Arthur Conan Doyle
> (British Physician and Writer)

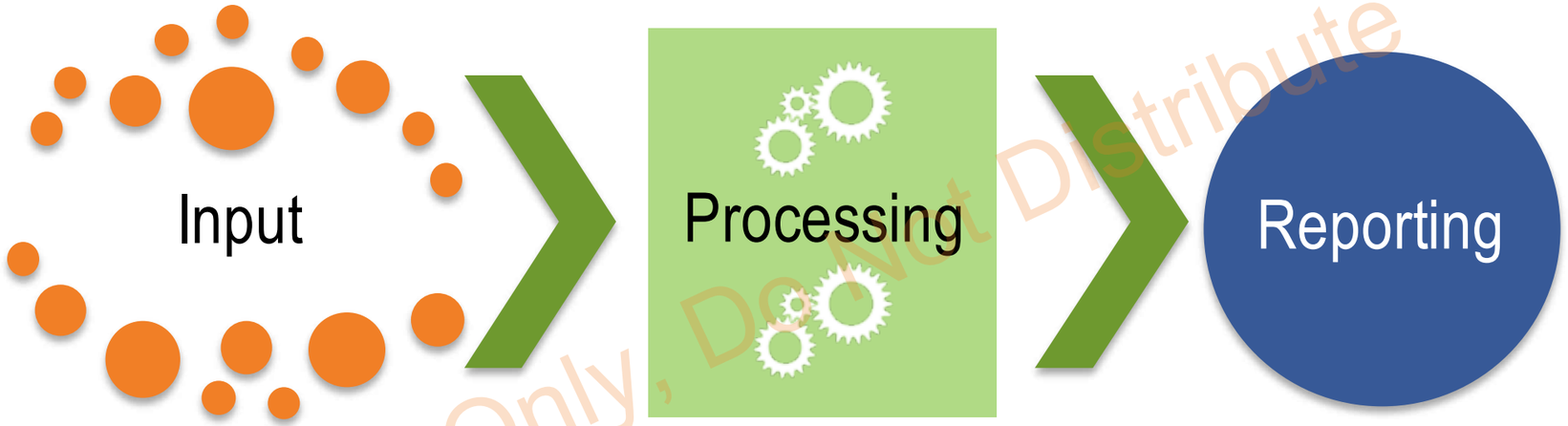
> You can use all the quantitative data you can get, but you still have to distrust it and use your own intelligence and judgment.
>
> Alvin Toffler
> (American Author and Futurist)

Understanding models and their use

The Core Components that Make a Model

Models are understood to be quantitative in nature but also include inputs that are qualitative or based on expert judgment, but the model output is quantitative in nature. There are three core components to a model:

1. **Input Component(s).** Delivers assumptions and data to a model.
2. **Processing Component(s).** Transforms inputs into estimates.
3. **Reporting Component(s).** Translates the estimates into useful business information.



- Instruments & positions
- Measuring risk
- Risk appetite, tolerance & capacity
- Underwriting credits
- Valuing Exposures
- Business strategy analysis
- Managing & safeguarding assets
- Predictive analysis
- Credit & counterparty risk
- Derivatives & hedging
- Market risks

- Valuation
- Pricing
- Exposure measurements
- Stress testing
- Capital reserve adequacy
- Liquidity planning
- Asset management
- Regulatory models
- Insurance planning
- Fraud analytics
- Anti-money laundering

Subscriber Use Only, Do Not Distribute

Our Agenda . . .

- ✓ **Defining & Understanding Risk Management**

  Definition, Drivers, Trends & Best Practices

- ❑ **Critical Capabilities of a Risk Management Solution/Platform**

  What Differentiates Basic, Common, & Advanced Solutions

- ❑ **Considerations in Selection of a Risk Management Solution/Platform**

  Decision Framework & Considerations to Keep in Mind

- ❑ **Building a Business Case for a Risk Management Solution/Platform**

  Trajectory of Value in Effectiveness, Efficiency & Agility

Licensed Subscriber Use Only, Do Not Distribute

The GRC Market: Technology, Information,& Professional Services

GRC Technology Solutions

731 technology solution providers that offer solutions related to GRC

GRC Intelligence & Content Solutions

112 providers with 384 content/intelligence solutions across a range of GRC areas

GRC Professional Services Solutions

1,000+ professional service firms offering services related to GRC

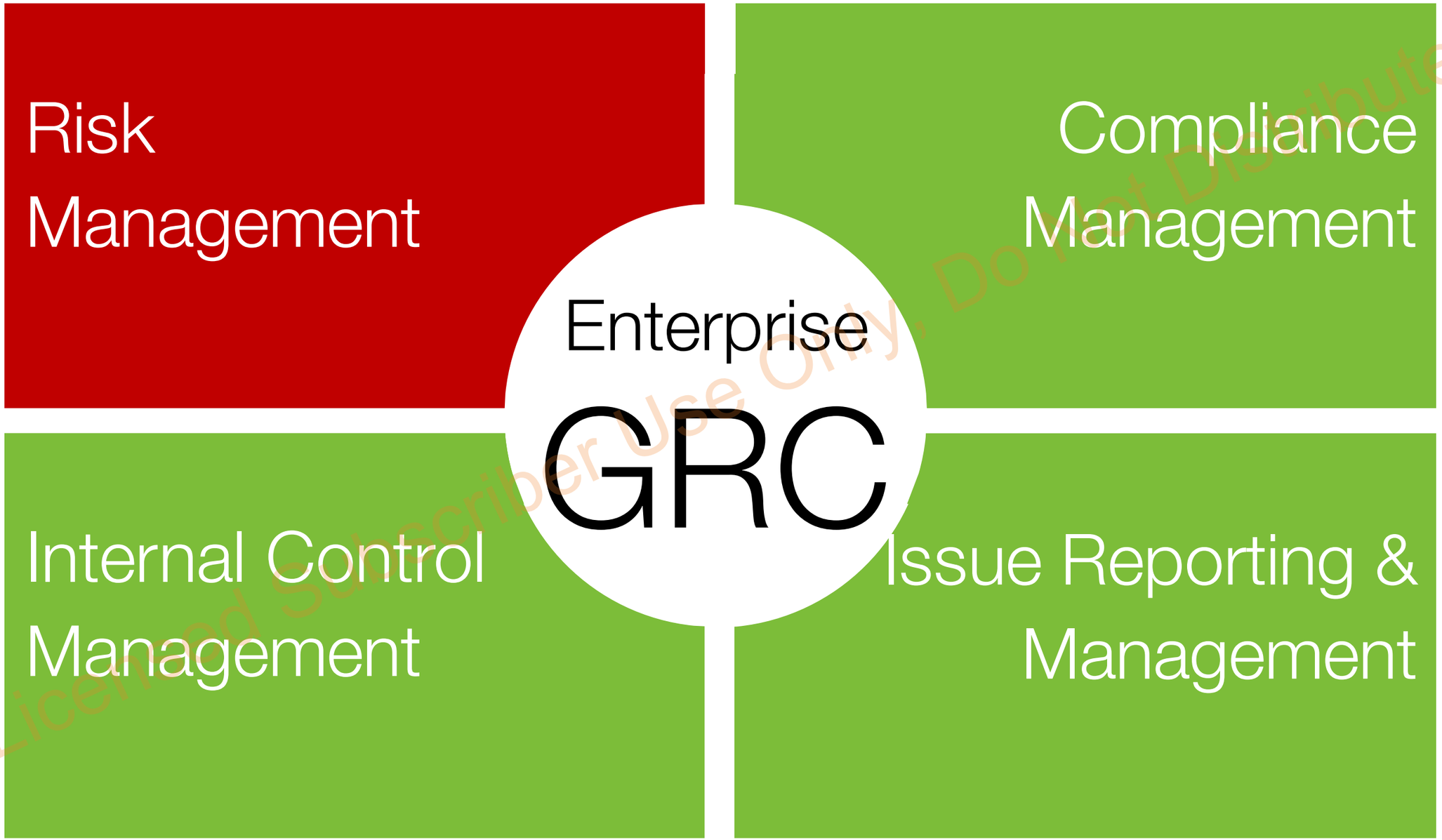
Subscriber Use Only - Do Not Distribute

GRC Technology Market Segments

- Enterprise GRC Platform & Architecture
- Audit Management & Analytic
- Automated Control Enforcement & Monitoring
- Business Continuity Management
- Compliance Management
- Environmental Management
- Health & Safety Management
- Internal Control Management
- IT GRC Management
- Issue Reporting & Management
- Legal Management
- Physical Security Management
- Policy & Training Management
- Quality Management
- Risk Management & Analytics
- Strategy, Performance & Process Management
- Third Party Management

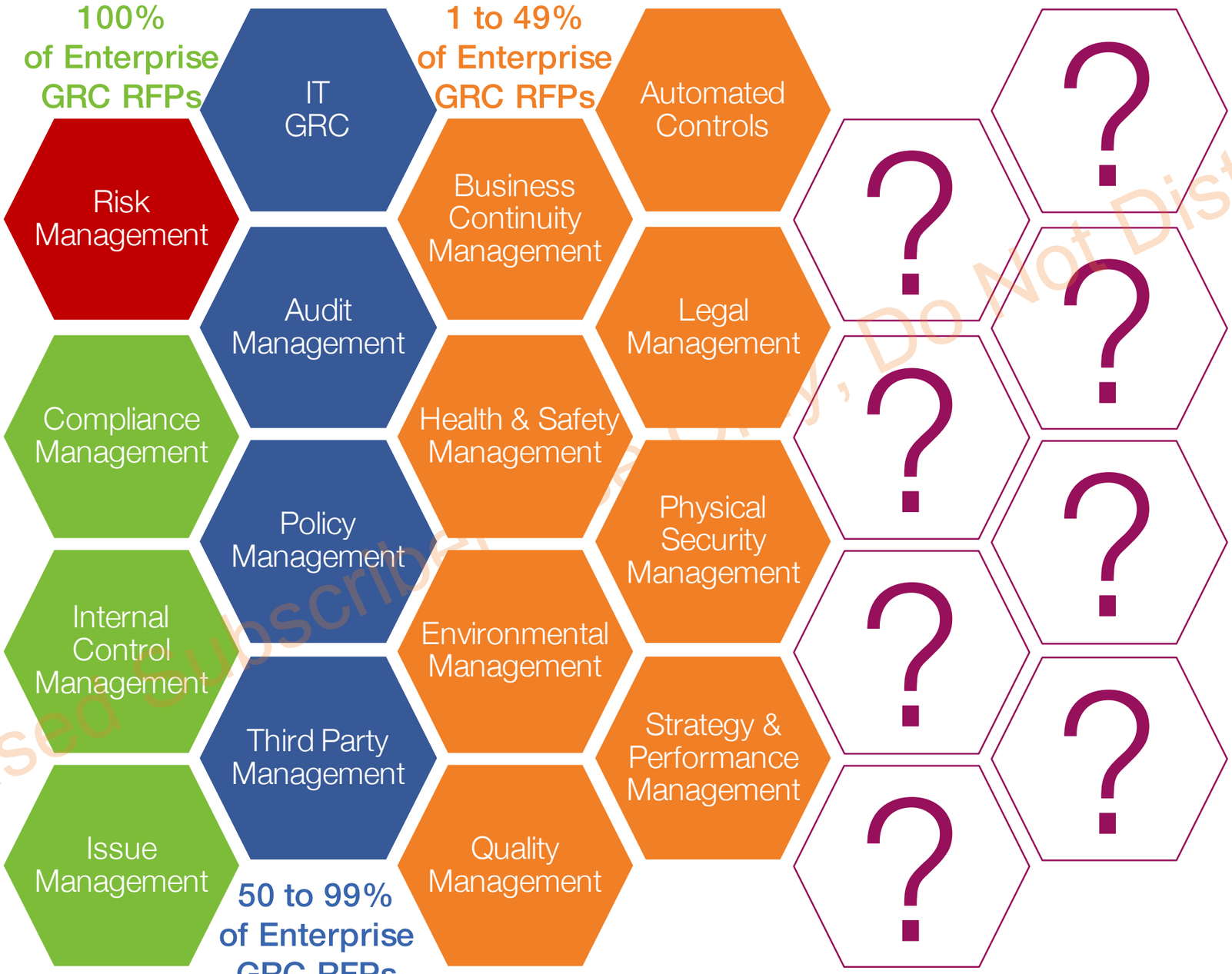
Licensed Subscriber Use Only, Do Not Distribute

Four Critical Capabilities Areas that Define an Enterprise GRC Platform



Licensed Subscriber Use Only, Do Not Distribute

What Are the Critical Components of Your GRC Platform?

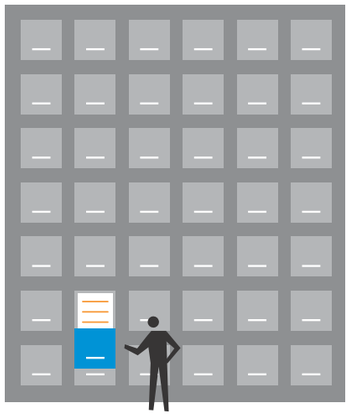


Licensed Subscriber Copy, Do Not Distribute

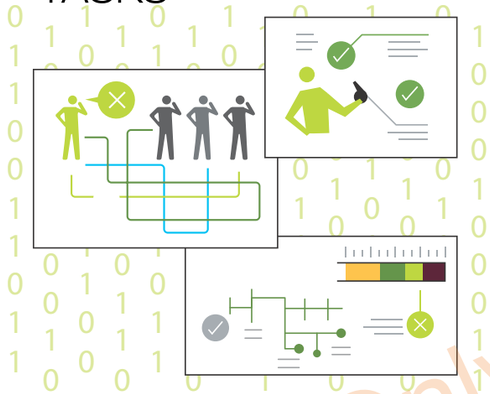
Risk Management Solutions Provide Automation & Tracking

MANAGEMENT REPORTING

AUDIT TRAIL



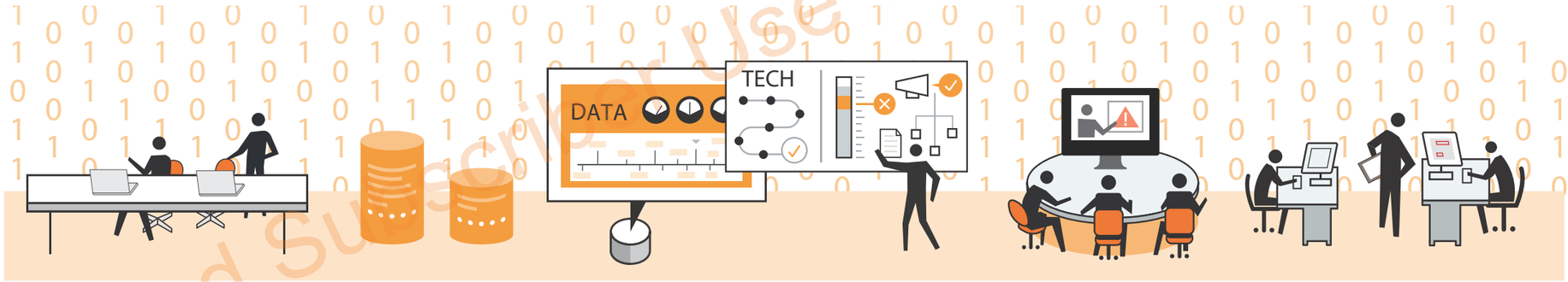
WORKFLOW & TASKS



COLLABORATION

ENFORCEMENT

IFORCE
munication, policies aren't always fol-



Integration

Visibility

Global Reach

Availability

Accountability

Automation

Repository

Consistency

Licensed Subscriber Use Only, Do Not Distribute

GRC Technology Market: Risk Management

Risk Management

- *Enterprise & Operational Risk Mgmt Platforms*
- *Risk Assessment Solutions*
- *Finance & Treasury Risk Management Solutions*
- *Insurance Risk & Claims Management Solutions*
- *Risk Analytics & Modeling Solutions*
- *Model Risk Management Solutions*
- *Project Risk Management Solutions*
- *Loss Collection & Analytic Solutions*
- *Miscellaneous Risk Management Tools*

Risk Intelligence & Content

- *Risk Libraries*
- *Loss Data*
- *Loss Scenarios & Case Studies*
- *Control Libraries*
- *Geo-Political Risk*

Risk Management technologies support the identification, assessment, evaluation and response, and monitoring of risks and opportunities of risk across the organization.

This includes the ability to monitor changes in the external and internal contexts to alert an organization to changing risk conditions (e.g., geo-political, economic, competitor, technology, and natural disaster) that can impact business. These systems help identify specific causes and execute historical review, simulation, interpretation and projection of impacts on an organization's operations or assets given the potential consequences of events and the likelihood of events occurring sequentially or simultaneously.

This category includes enterprise risk management systems, operational risk management systems, as well as specialized risk applications.

Finance/Treasury Risk Management - involves an array of applications and systems used to identify and manage the risk factors, causes and response procedures in an organization's financial and treasury management. These include risk technology focused on specific areas such as liquidity, credit, market, and commodity risk management that help identify risk and execute historical review, simulation, interpretation and projection of impacts on an organization's financial assets given the potential consequences of events and the likelihood of events occurring sequentially or simultaneously.

Licensed Subscriber Use Only, Do Not Distribute

Issues in Enterprise & Operational Risk Management

1) No Multi-Dimensional Mapping of Risk Relationships & Impacts

- A single risk can impact the organization in different ways and have exponential impact when considered in context of other risks managed in other areas but no one sees the range of related risks.
- Organizations fail to map risks into different hierarchies of relationships and show a multi-dimensional view of risks and their impact and relationships across the organization.

2) Forcing Everyone into a One-Size Fits All Risk Analysis Methodology

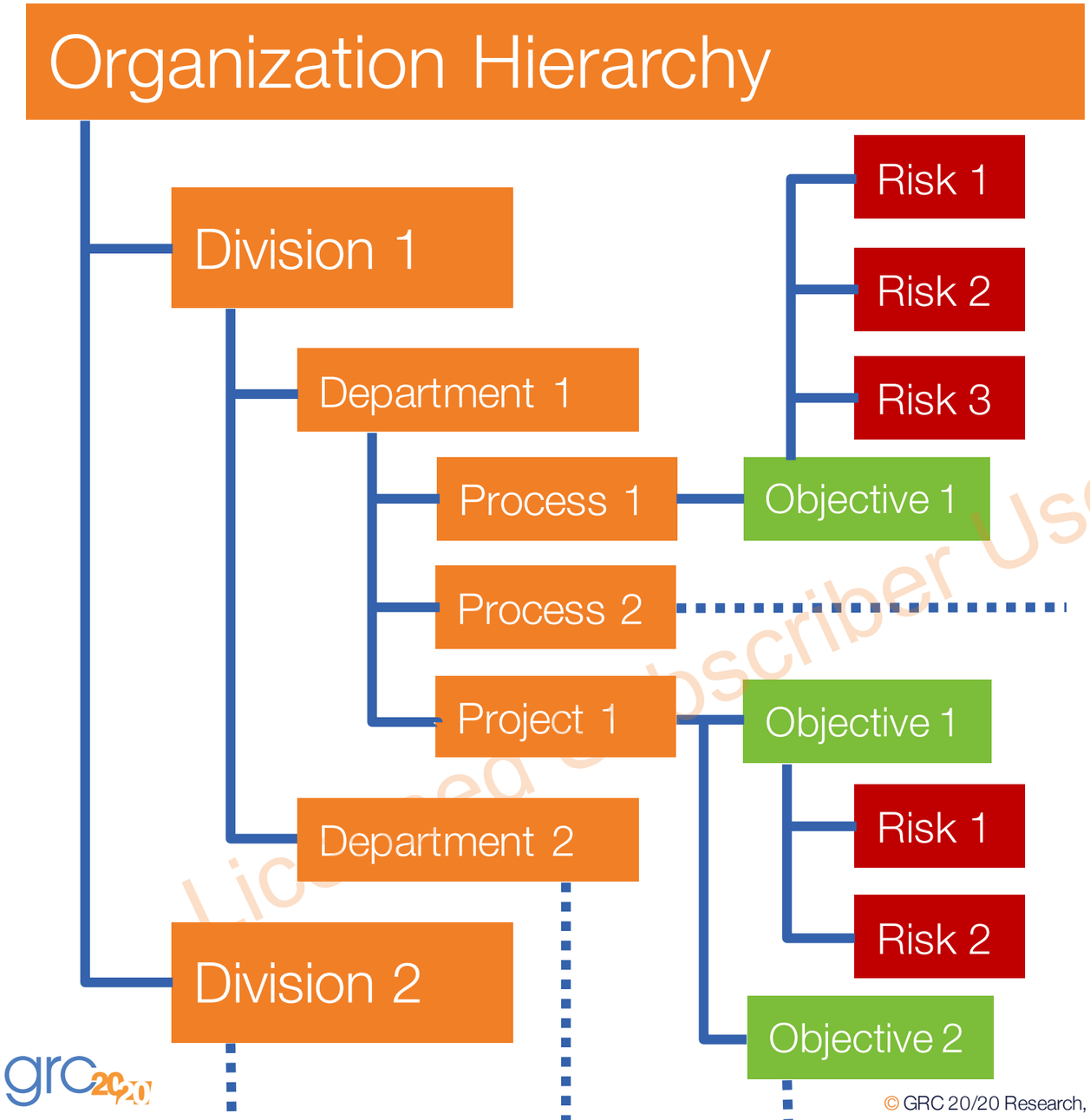
- Organizations try to implement a one-size fits all approach to risk analysis that ends up watering down risk assessments to the lowest common denominator.
- Well established approaches for managing risk in areas of the organization get pushed aside and the particular specialized views and details are lost leading to greater exposure.

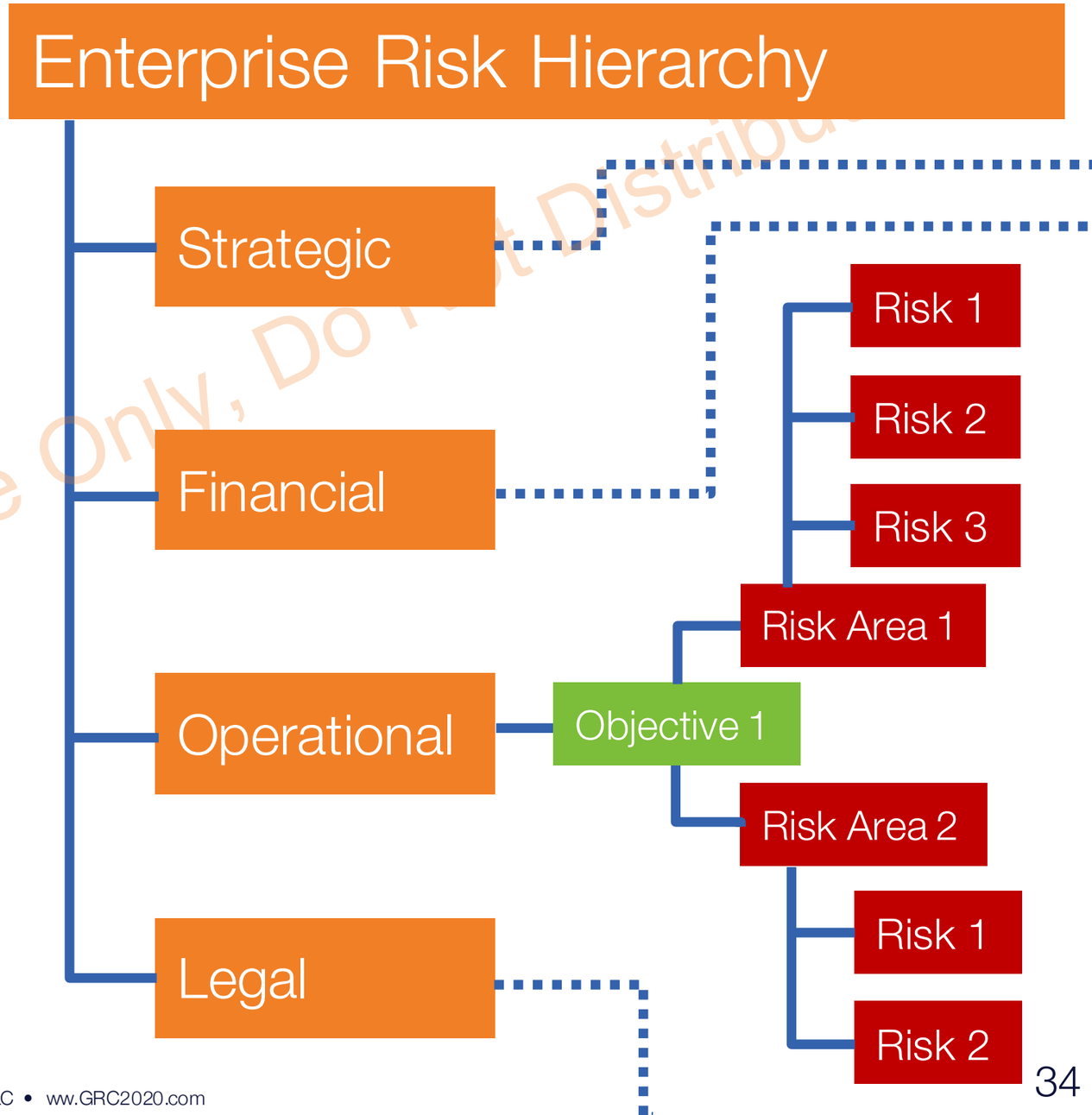
3) Lack of Risk Normalization & Aggregation

- Organizations attempt enterprise risk management by standardizing on a single flat view of risk scoring and appetite that creates issues when identifying and managing localized operational threats and opportunities as everything is scaled to an enterprise view.
- For effective risk normalization and aggregation, risks must be assessed both qualitatively and quantitatively with standardized methodologies that alow for a view of risk at an enterprise level as well as lower localized levels.

Licensed Subscriber Use Only, Do Not Distribute

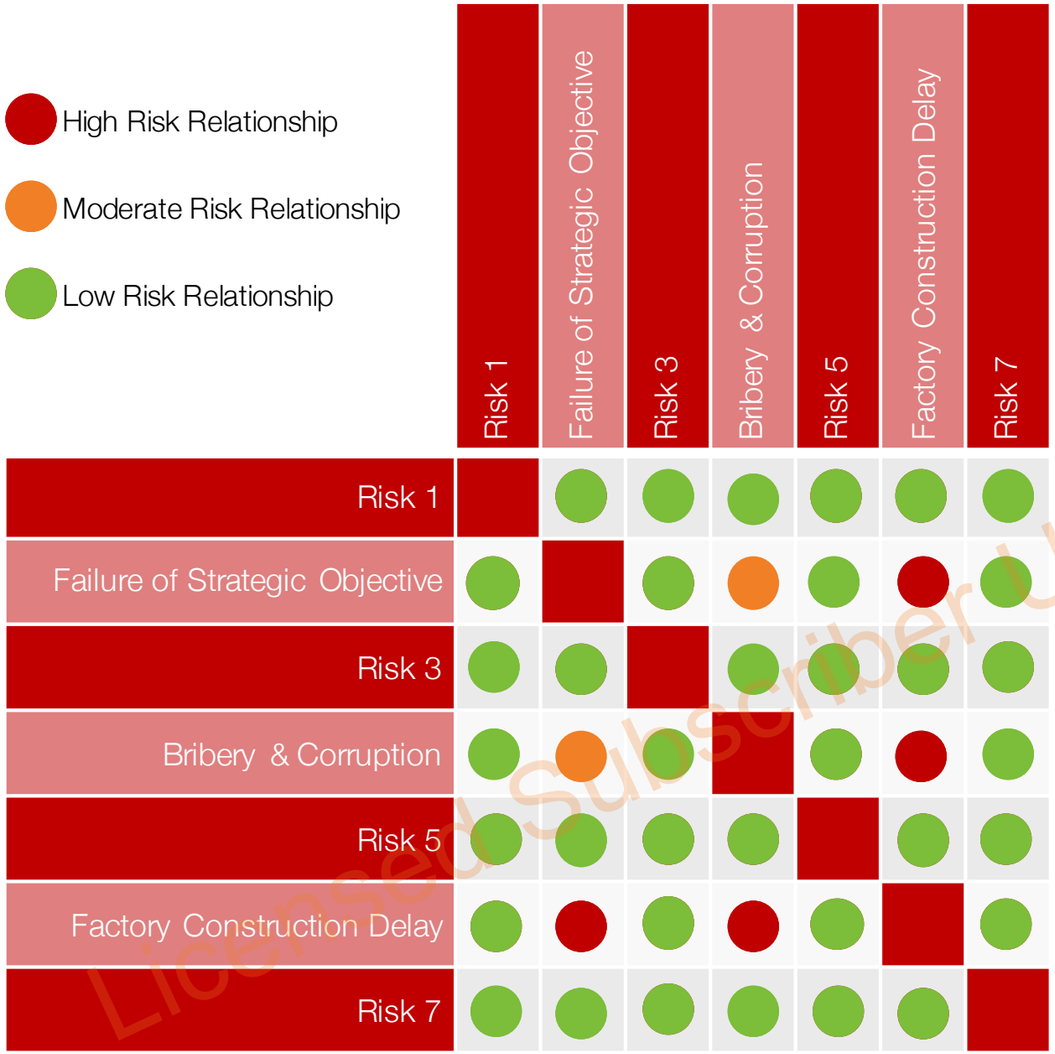
Risk Identification Capability: Mapping Risks into Different Hierarchies





Licensed Subscriber Use Only, Do Not Distribute

Risk Relationship Matrix Capability

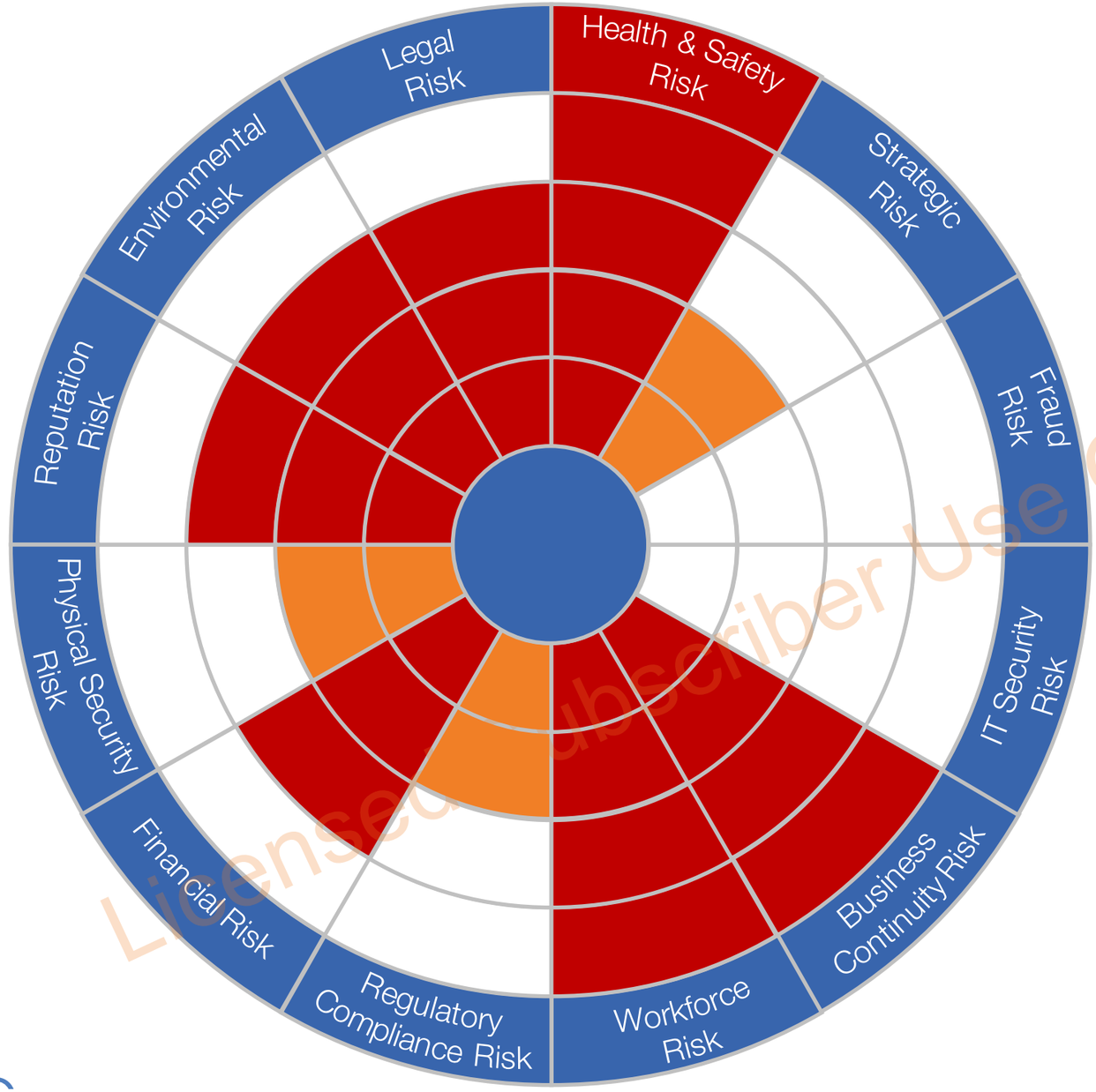


Scenario

- Strategic Objective:
  - Expand operations by building factory in Country X.
- Risks to Objectives:
  1) Failure to meet strategic objective
  2) Factory construction delay
- Related Risks:
  - By mapping risks the organization discovers risk relationships that it previously did not foresee.
  - Such as Bribery & Corruption risk when a foreign government official threatens to withhold building permits unless paid a bribe
    - This in turn has related risks of fraud, which has a related risk of IT control failure that could expose the organization to a higher fraud risk

Licensed Subscriber Use Only. Do Not Distribute

Risk Scenario Relationship Capabilities



Health & Safety Scenario

Event Scenario:

Factory plant explosion with loss of life and injuries due in part to minor negligence of company.

Significantly Related Risks:

- Business Continuity Risk
- Workforce Risk

High Related Risks:

- Financial Risk
- Reputation Risk
- Environmental Risk
- Legal Risk

Moderately Related Risks:

- Regulatory Compliance Risk
- Strategic Risk
- Physical Security Risk

Unrelated Related Risks:

- Fraud Risk
- IT Security Risk

Licensed Subscriber Use Only, Do Not Distribute

Risk Detail Capability

Risk Name:			Risk Status: Green
Reporting Period:		Subject Matter Expert:	
Risk Team:			
Risk Description			

Control Environment Evaluation to Mitigate Risk

Over-Controlled — Need Fewer Controls — Controlled — Need More Controls — Under-Controlled

Concerns Regarding Current Control Environment	Mitigation Activities	Deadline	Status

Emerging Risks / Events That Could Change Assessment of Risk	Emerging Risk Mitigation Activities	Deadline	Status

Licensed Subscriber Use Only, Do Not Distribute

Risk Detail Capability, continued

Related Risks	Related Objectives

Related Processes	Related Assets

Risk Scenarios (Types of Events That Could Cause Loss)					
Scenario	Impact	Likelihood	Velocity	Management	Systems

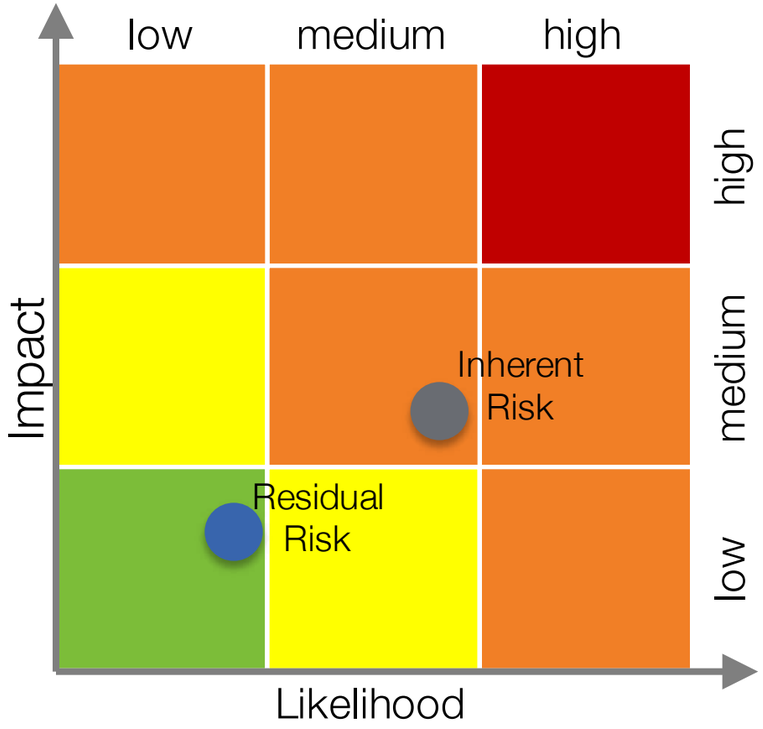
History of Risk Events (Losses)		
Event Description	When	Impact ($)

Licensed Subscriber Use Only, Do Not Distribute

Risk Detail Capability, continued

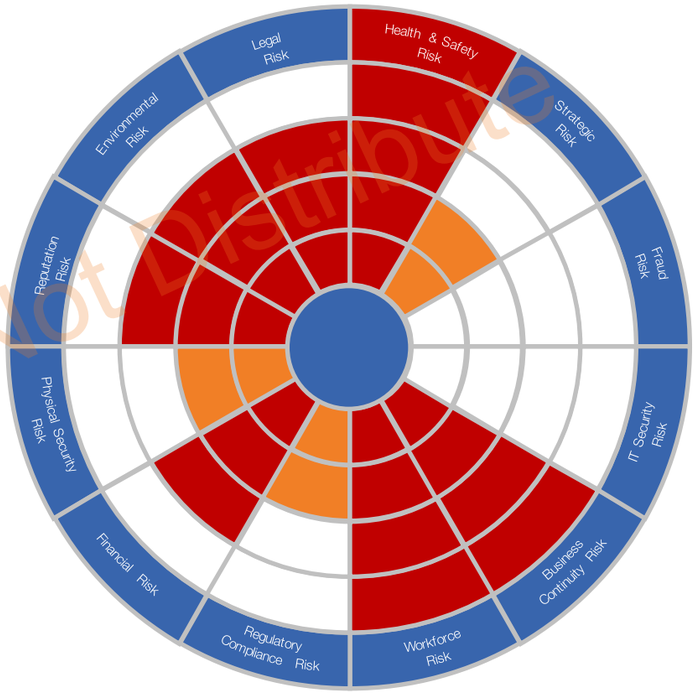
Licensed Subscriber Use Only, Do Not Distribute

Risk Detail Capability, continued



Risk Mitigation Actions

Key Risk Factors Monitored



Risk Acceptance		
Date	Signature Risk Owner	Signature Risk Expert

Licensed Subscriber Use Only, Do Not Distribute

Risk Impact Analysis Capability

Scale	Impact Category	Financial	Reputation	Legal	Health & Safety	Workforce
5	Extreme	Financial loss of $X million or more3	International long-term negative media coverage; game-changing loss of market share	Significant prosecution and fines, litigation including class actions, incarceration of leadership	Significant injuries or fatalities to employees or third parties, such as customers or vendors	Multiple senior leaders leave
4	Major	Financial loss of $X million up to $X million	National long-term negative media coverage; significant loss of market share	Report to regulator requiring major project for corrective action	Limited in-patient care required for employees or third parties, such as customers or vendors	Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	Financial loss of $X million up to $X million	National short-term negative media coverage	Report of breach to regulator with immediate correction to be implemented	Out-patient medical treatment required for employees or third parties, such as customers or vendors	Widespread staff morale problems and high turnover
2	Minor	Financial loss of $X million up to $X million	Local reputational damage	Reportable incident to regulator, no follow up	No or minor injuries to employees or third parties, such as customers or vendors	General staff morale problems and increase in turnover
1	Incidental	Financial loss up to $X million	Local media attention quickly remedied	Not reportable to regulator	No injuries to employees or third parties, such as customers or vendors	Isolated staff dissatisfaction

Licensed Subscriber Use Only, Do Not Distribute

Risk Likelihood (Frequency and Probability) Analysis Capability

Scale	Frequency Category	Frequency
5	Frequent	Up to once in 2 years or more
4	Likely	Once in 2 years up to once in 25 years
3	Possible	Once in 25 years up to once in 50 years
2	Unlikely	Once in 50 years up to once in 100 years
1	Rare	Once in 100 years or less

Scale	Probability Category	Probability
5	Almost Certain	90% or greater chance of occurrence over life of asset or project
4	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	<10% chance of occurrence over life of asset or project

Licensed Subscriber

Risk Vulnerability / Exposure Analysis Capability

Scale	Impact Category	Scenario Preparedness	Process Preparedness	Incident Response	Business Continuity
5	Very High	No scenario planning performed	Lack of enterprise level/process level capabilities to address risks	Responses not implemented	No contingency or crisis management plans in place
4	High	Scenario planning for key strategic risks performed	Low enterprise level/process level capabilities to address risks	Responses partially implemented or not achieving control objectives	Some contingency or crisis management plans in place
3	Medium	Stress testing and sensitivity analysis of scenarios performed	Medium enterprise level/process level capabilities to address risks	Responses implemented and achieving objectives most of the time	Most contingency and crisis management plans in place, limited rehearsals
2	Low	Strategic options defined	Medium to high enterprise level/process level capabilities to address risks	Responses implemented and achieving objectives except under extreme conditions	Contingency and crisis management plans in place, some rehearsals
1	Very Low	Real options deployed to maximize strategic flexibility	High enterprise level/process level capabilities to address risks	Redundant response mechanisms in place and regularly tested for critical risks	Contingency and crisis management plans in place and rehearsed regularly

Licensed Subscriber Use Only, Do Not Distribute

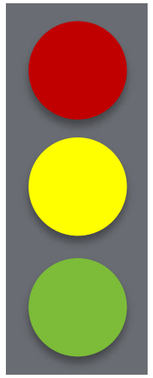
Risk Velocity & Duration Analysis Capability

Scale	Velocity Category	Speed of Onset
5	Very High	Very rapid onset, little or no warning, instantaneous
4	High	Onset occurs in a matter of days to a few weeks
3	Medium	Onset occurs in a matter of a few months
2	Low	Onset occurs in a matter of several months
1	Very Low	Very slow onset, occurs over a year or more

Scale	Duration Category	Time to Recover
5	Very High	Recovery takes up to a year
4	High	Recovery takes up to a quarter
3	Medium	Recovery takes up to a month
2	Low	Recovery takes up to a week
1	Very Low	Recovery takes up to a day

Licensed Subscriber Use Only - Not for Distribute

Qualitative Risk Analysis Capabilities



Advantages	Disadvantages
✓ Is relatively quick and easy	✓ Gives limited differentiation between levels of risk (i.e. very high, high, medium, and low)
✓ Provides rich information beyond financial impact and likelihood such as vulnerability, speed of onset, and non-financial impacts such as health and safety and reputation	✓ Is imprecise – risk events that plot within the same risk level can represent substantially different amounts of risk
✓ Is easily understood by a large number of employees who may not be trained in sophisticated quantification techniques	✓ Cannot numerically aggregate or address risk interactions and correlations
	✓ Provides limited ability to perform cost-benefit analysis

Licensed Subscriber Use Only, Do Not Distribute

Quantitative Risk Analysis Capabilities

Advantages	Disadvantages
✓ Allows numerical aggregation taking into account risk interactions when using an "at risk" measure such as Cash Flow at Risk	✓ Can be time-consuming and costly, especially at first during model development
✓ Permits cost-benefit analysis of risk response options	✓ Must choose units of measure such as dollars and annual frequency which may result in qualitative impacts being overlooked
✓ Enables risk-based capital allocation to business activities with optimal risk-return	✓ Use of numbers may imply greater precision than the uncertainty of inputs warrants
✓ Helps compute capital requirements to maintain solvency under extreme conditions	✓ Assumptions may not be apparent

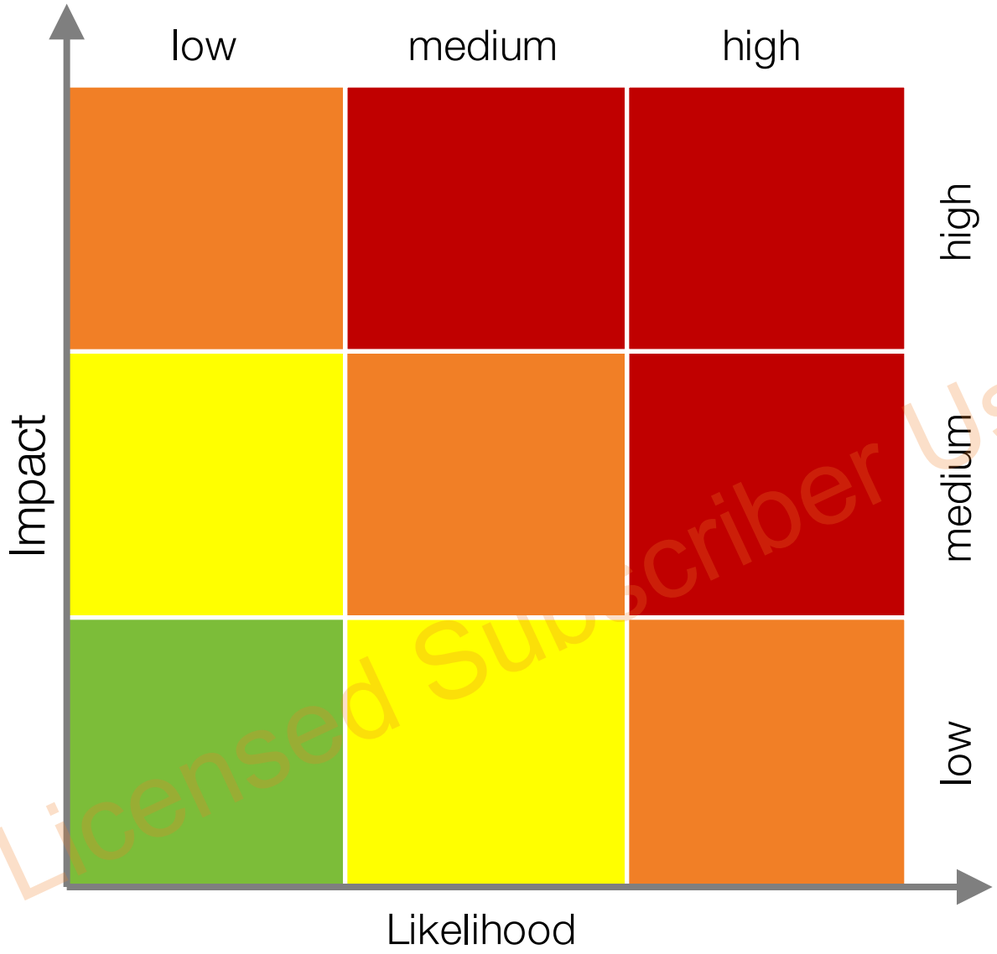
Licensed Subscriber Use Only, Do Not Distribute

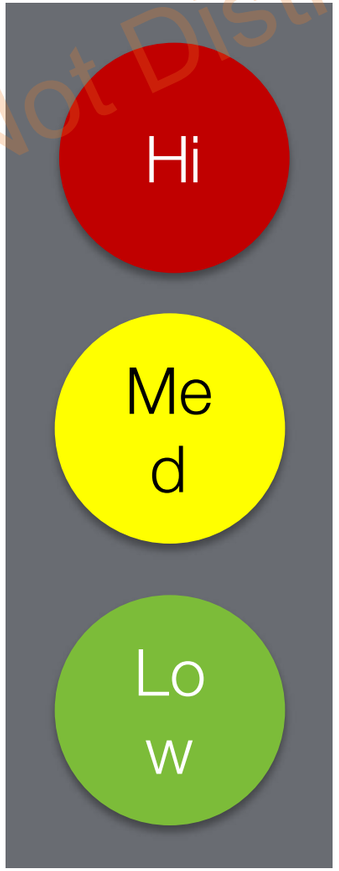
Scenario Analysis Capability

Scenario	Description	Assumptions	EBIT Impact
1	Currency changes impact competitive landscape	▪ 15% volume decrease ▪ 20% price decrease ▪ Sustained for 9 months ▪ Recovery takes additional 9 months	$500 MM Loss
2	Natural gas prices increase	▪ $5/MM Btu increase ▪ Sustained for 12 months ▪ No ability to pass through increase	$150 MM Loss
3	Crude oil prices increase	▪ 100% increase ▪ Sustained for 3 months ▪ Pass through 25% of cost increase	$15 MM Loss
4	Technology shift	▪ 15% volume decrease/year 15% price decrease/year ▪ $2MM less in R&D expenditures	$275 MM Loss
5	Competitive pressure	▪ 10% price decrease ▪ Sustained for 24 months	$200 MM Loss
6	Supply-chain disruption	▪ 10% volume decrease ▪ Sustained for 6 months	$175 MM Loss

Licensed Subscriber Use Only, Do Not Distribute

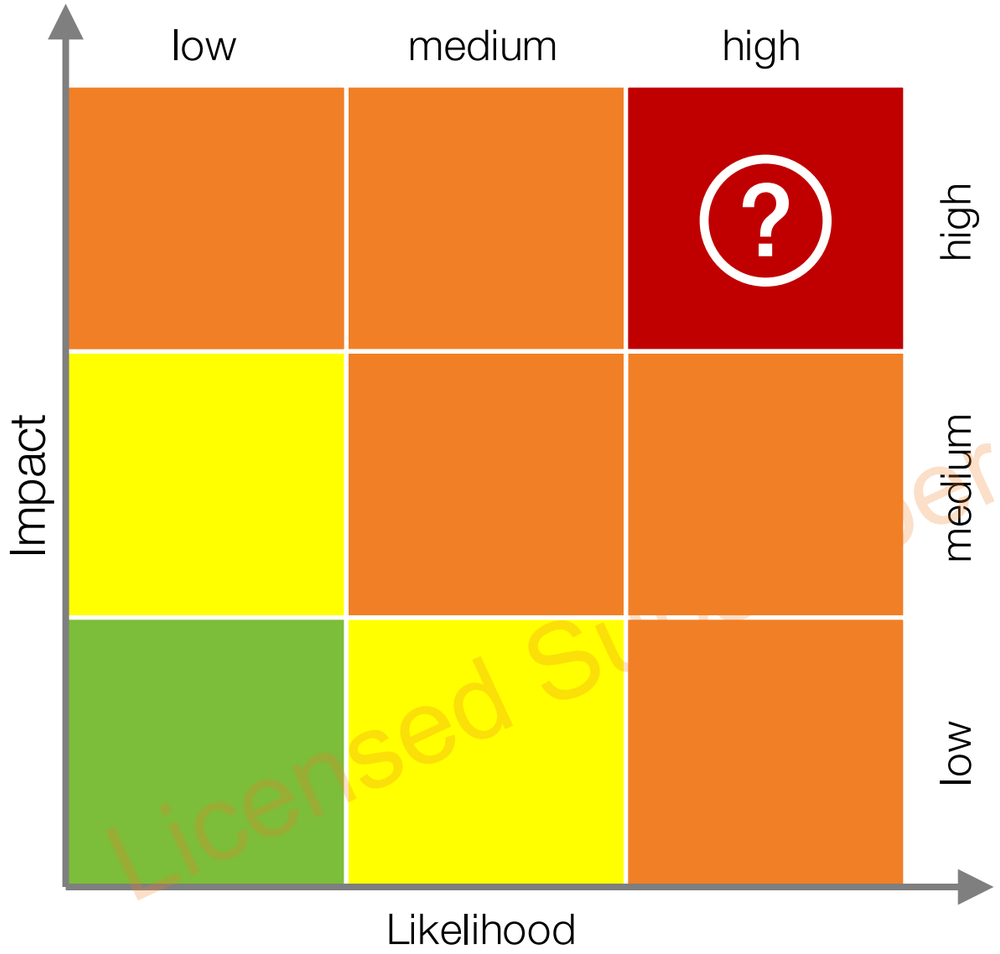
Are We Going to Limit Risk Analysis to These Approaches?

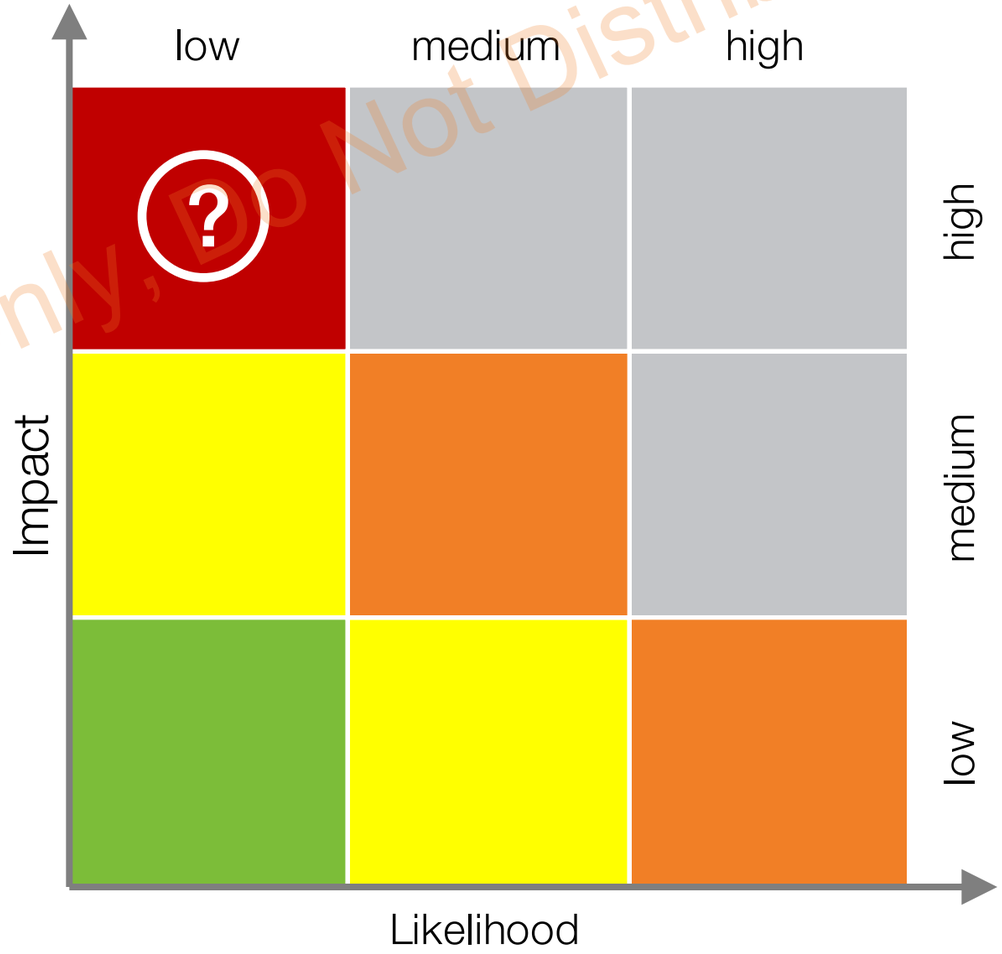




Licensed Subscriber Use Only, Do Not Distribute

Which One of These Reflects the Real World?





Licensed Subscriber Use Only, Do Not Distribute

A Wide Array of Risk Analysis Methodologies Capabilities

Risk Analysis Methodologies

- Bayesian statistics and Bayes Nets
- Bow tie analysis
- Brainstorming
- Business impact analysis
- Capital at risk
- Cause and consequence analysis
- Cause-and-effect analysis
- Check-lists
- Consequence/probability matrix
- Cost/benefit analysis
- Decision tree

Risk Analysis Methodologies

- Delphi
- Environmental risk assessment
- Event tree analysis
- Failure mode effect analysis
- Fault tree analysis
- FN curves
- Hazard Analysis and Critical Control Points (HACCP)
- Hazard and operability studies (HAZOP)
- Heatmaps
- Human reliability analysis
- Layer protection analysis (LOPA)

Licensed Subscriber Use Only - Do Not Distribute

A Wide Array of Risk Analysis Methodologies Capabilities

Risk Analysis Methodologies

- Markov analysis
- Monte Carlo simulation
- Multi-criteria decision analysis (MCDA)
- Primary hazard analysis
- Reliability centered maintenance
- Risk indices
- Root cause analysis
- Scenario analysis
- Sneak circuit analysis
- Structure « What if? » (SWIFT)
- Structured or semi-structured interviews

Risk Analysis Methodologies

- Risk Self-Assessments (Surveys)
- Value at risk
- Workshops
- MARCI - Mitigate, Assure, Redeploy & Cumulative Impact

Licensed Subscriber Use Only - Do Not Distribute

Varying Approaches to Risk Normalization & Aggregation Capabilities

None

No normalization or aggregation of risk is done. Each area (e.g., objective, department, process, asset) doing risk assessments and analysis operates independently and not in context with other risk assessments/analysis.

Impact: This allows different areas to manage risk within the context of their area, but provides little to no value for enterprise risk reporting.

Manual

The organization has no automated capability to do risk normalization and aggregation and has to manually analyze and reconcile risk scores from various areas for enterprise risk reporting.

Impact: This is resource intensive in staff time and may also lead to errors in judgment and mistake.

No Normalization

The organization aggregates risk but avoids normalization by requiring all risk assessments to conform to a single risk scoring and analysis.

Impact: This allows for accurate enterprise risk reporting, but has issues in risk management when looked at at a more granular level.

Two+ Scores

The organization avoids risk normalization by requiring every area to conduct two or more sets of assessments with different scoring scales for different contexts. One at the enterprise level, the other at the granular level. Possibly more if there are other roll-up levels like divisional.

Impact: this is more resource intensive as it requires more work, documentation, and can be prone to errors.

Calculated

The organization utilizes standard weightings and calculations to normalize risk so it can be objectively compared, evaluated, and rolled-up into enterprise risk reporting.

Impact: this allows for flexibility within one consistent risk process to provide both granular and enterprise views of risk, as well as levels in between.

Calculated + Rules

In addition to weightings and calculations, the organization applies business rules and logic to risk as it is normalized and aggregated. This allows for exceptions so a risk does not get diminished and not reported when the rule applies.

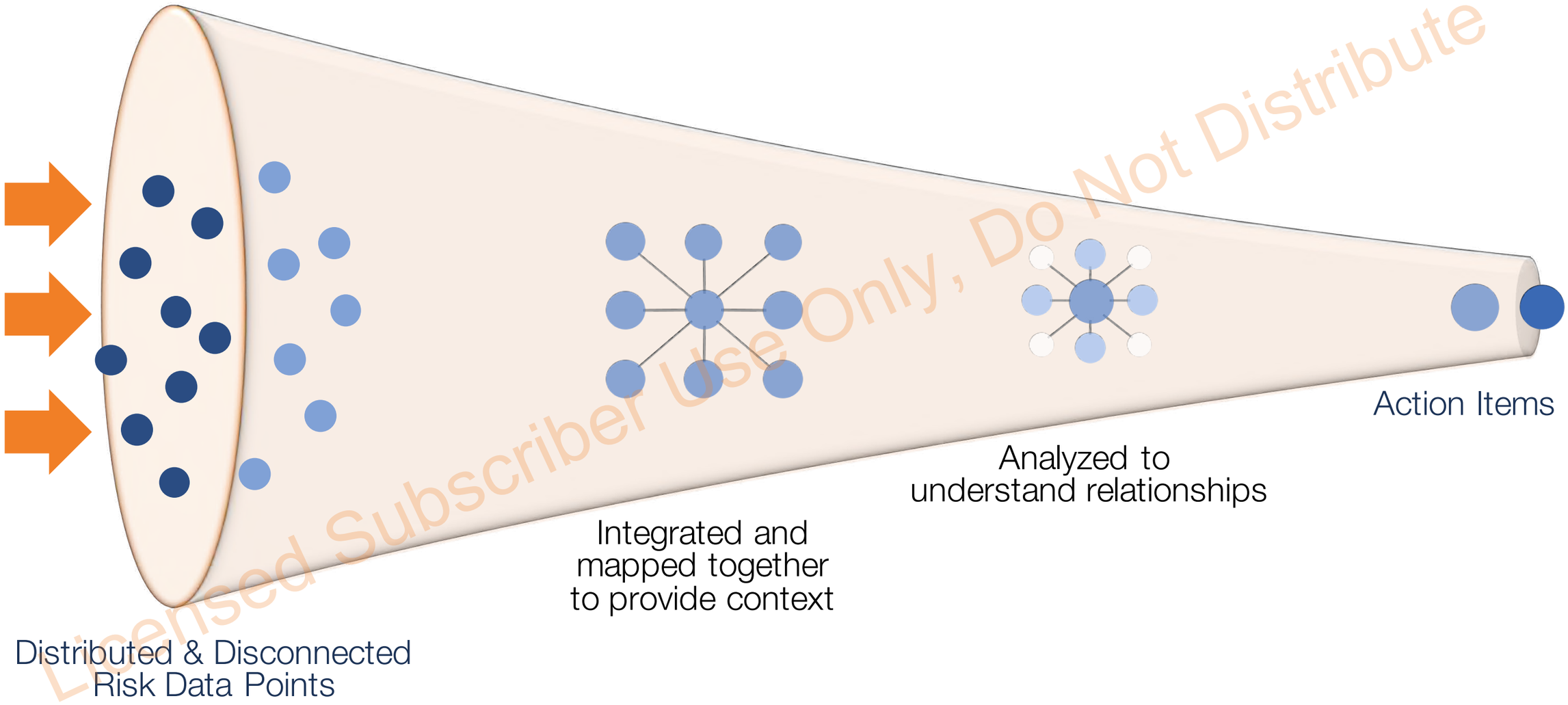
Impact: this allows for the greatest flexibility as there may be particular risks or scenarios that need to be approached uniquely.

Example Calculated Weightings . . .

- **Weighting.** A percentage or multiplier is used to a risk score to normalize it in context of other risks. Weighting can be based on attributes such as revenue of assets in context of where the risk is, or combined revenue of assets as it rolls up.
- **Simple Calculation.** Straight forward normalization of risk scores utilizing summation, average, or median of risk scores. Calculation can be done on scores such as residual risk, maximum residual risk, risk exposure in relation to risk appetite.
- **Weighted Calculation.** This combines both calculation and weighting to allow for greater flexibility in normalization and aggregation in which calculated risk scores can be further normalized through weightings.
- **Proprietary.** This involves some under the hood and non-disclosed calculation that a risk technology does to aggregate and normalize risk. Caution should be used with this if the solution provider does not disclose how this works.
- **Quantitative Analysis.** This utilizes approaches such as VaR, Monte Carlo, or Bayesian modeling to bring risk to a quantitative mathematical representation and distribution for comparing and analysis.

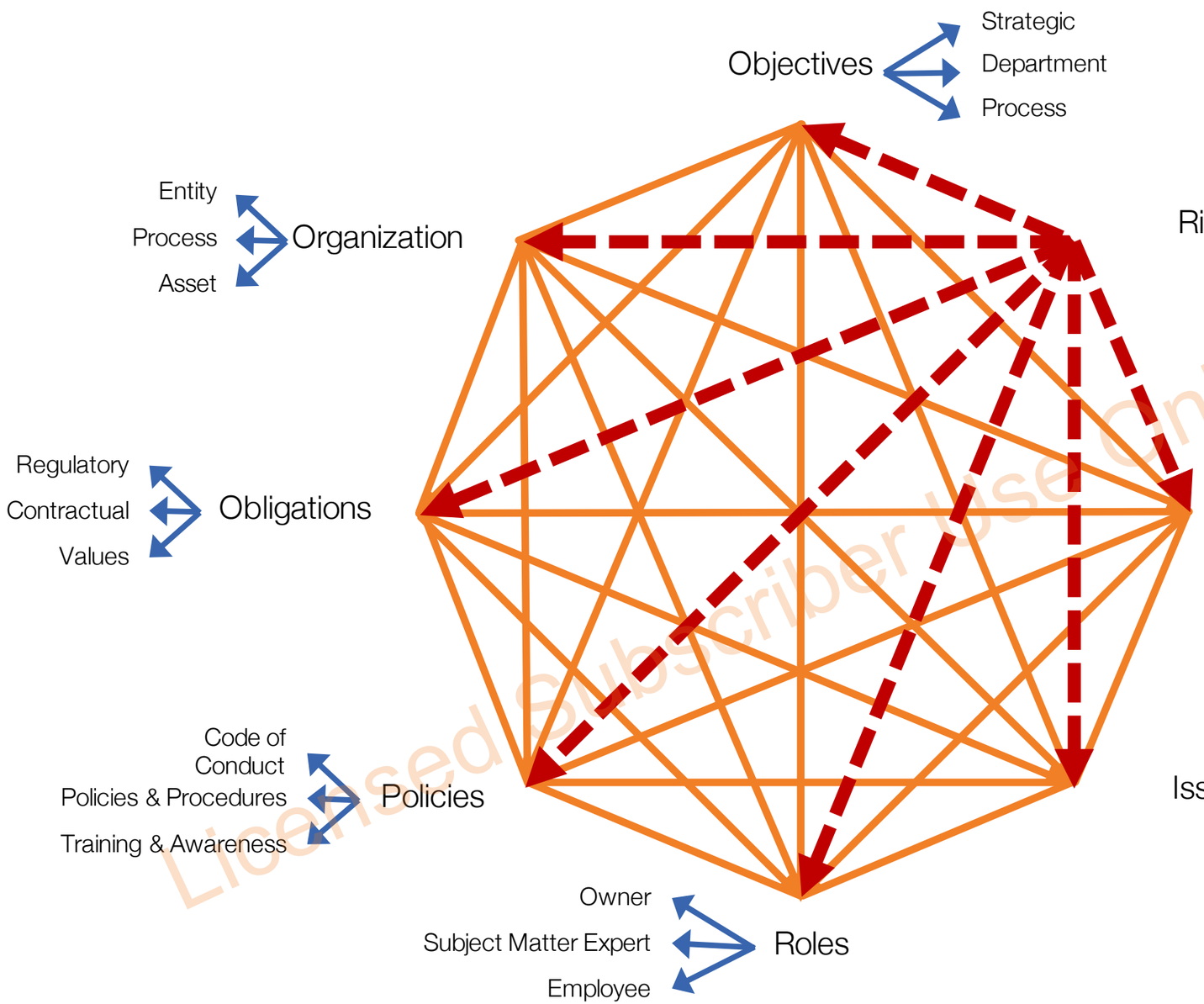
Licensed Subscriber Use Only, Do Not Distribute

360° Risk Contextual Analytics & Intelligence Capabilities



Licensed Subscriber Use Only, Do Not Distribute

Risk Information Architecture Provides 360° Contextual Intelligence Capabilities



Licensed Subscriber Use Only, Do Not Distribute

higher quality information

Integrating GRC information allows management to make more intelligent decisions, more rapidly.

process optimization

All non-value-added activities are eliminated and value-added activities are streamlined to reduce lag time and undesirable variation.

better capital allocation

Identifying areas where there are redundancies or inefficiencies allows financial and human capital to be allocated more effectively.

improved effectiveness

Overall effectiveness is improved as gaps are closed, unnecessary redundancy is reduced, and GRC activities are allocated to the right individuals and departments.

protected reputation

Reputation is protected and enhanced because risks are managed more effectively.

reduced costs

Reduced costs help to improve return on investments made in GRC activities.

Risk Management

Solution Area Definition

Risk Management solutions provide the capability to identify, assess, measure, treat, manage, monitor, and report on risks to objectives, divisions, departments, processes, assets, and projects. This enables organizations to manage:

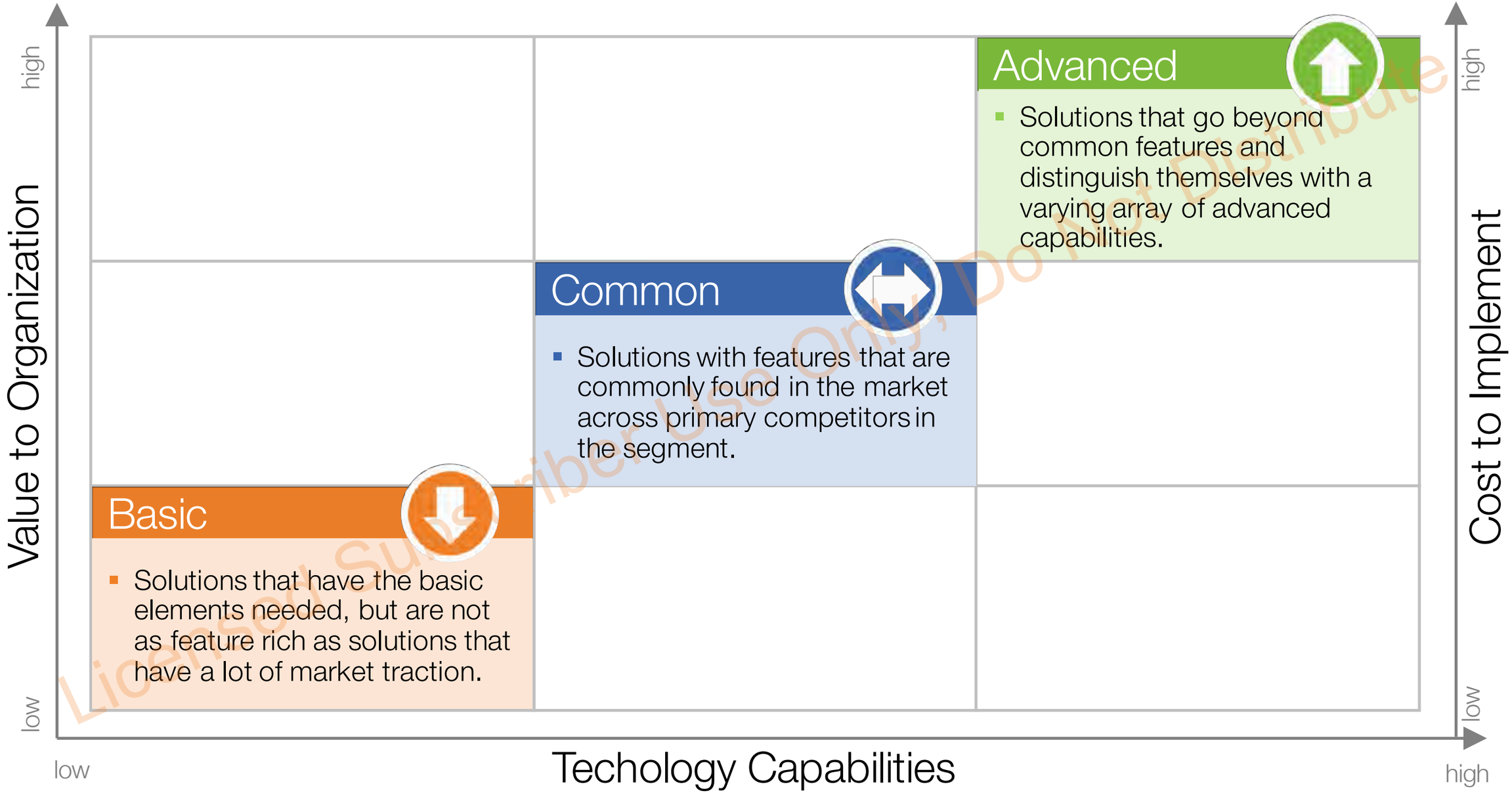
- **Risk management process** of risk identification, assessment, quantification, treatment and monitoring activities in context of objectives, including the overall management of the continual, cyclic, as well as dynamic processes of risk assessment, analysis, decision making, and response (e.g., acceptance, mitigation, transfer, avoidance).
- **Risk monitoring** on changes in external and internal contexts to alert the organization to conditions that can impact objectives.
- **Risk evaluation** to identify specific causes and evaluate historical review, simulation, interpretation and projection of impacts on an objectives and assets.

Critical Capabilities

- ❑ Manage overall risk management program planning, staff, projects/assessments, and activities
- ❑ Support for multiple risk management frameworks, methodologies, and analysis techniques
- ❑ Set and map objectives and context (e.g., internal, external) of risk
- ❑ Enable the organization to identify, categorize, map, and show risk relationships in registers
- ❑ Enable the organization to gather information and assessment of risks in a variety of approaches
- ❑ Analyze risk from different perspectives and implement risk treatment
- ❑ Provide monitoring and reporting on risk, including risk normalization and aggregation enterprise reporting
- ❑ Ability to analyze scenarios and evaluate risk losses and events, and revise risk models as necessary
- ❑ Dashboarding and metrics (e.g., KRIs) on risk

Licensed Subscriber Use Only. Do Not Distribute

Basic, Common & Advanced Solutions



Licensed Subscriber Use Only, Do Not Distribute

What Differentiates Basic, Common & Advanced Solutions?

Characteristics: Basic Risk Management Solutions

Basic risk management soliutions focus on the workflow, forms, and tasks of risk management. The value focus is on task automation by removing inefficiencies of manual approaches of documents, spreadsheets, and emails and replacing this with a solution that can collect information, manage workflow and tasks, and simplify reporting. Content, if provided, is typically in context of a single risk management area (e.g., IT risk, health & safety risk).

Capabilities

- ✓ Supports back-end process of risk management tasks
- ✓ Workflow & task management
- ✓ Risk questionnaires, surveys, self-assessments & reporting
- ✓ Notification
- ✓ Tracking risk acceptance
- ✓ Reporting and tracking risks
- ✓ Audit trail/system of record of risk management related activities
- ✓ Heatmaps and/or stoplight diagrams are typical risk reportring

Limitations

- ➢ Limited content integration, typically in context of one area and not across the organization
- ➢ Focus is rather narrow in addressing risk management
- ➢ Lacks risk normalization and aggregation capabilities
- ➢ Organization typically uses one risk model

Licensed Subscriber Use Only, Do Not Distribute

What Differentiates Basic, Common & Advanced Solutions?

Characteristics: Common Risk Management Platforms

Common risk management platforms have the range of features commonly found in enterprise risk management RFPs that span the organization's enterprise/operational risk management needs. They build upon the foundation of workflow, tasks, assessments, and forms with features to provide greater integration with other systems, and have better content integration.

Capabilities

- ✓ Has workflow, task, assessment, and content capabilities of Basic solutions
- ✓ Ability to manage the entire risk management process
- ✓ Ability to map and show interrelationships
- ✓ Basic risk normalization and aggregation capabilities
- ✓ Ability to model risk in more analysis techniques than heatmaps and stoplight diagrams
- ✓ Mapping risks to controls, to issues/incidents, etc.

Limitations

- ➢ Risk party content and intelligence sources is still often limited in scope
- ➢ More advanced risk normalization and aggregation capabilities are lacking
- ➢ Risk visualizaiton capabilities are weak
- ➢ Lack of quantitative risk analysis, focus is on qualitative

Licensed Subscriber Use Only, Do Not Distribute

What Differentiates Basic, Common & Advanced Solutions?

Characteristics: Advanced Risk Management Platforms

Advanced risk management platforms are Common Platforms that have distinguished themselves from competitors by offering advanced capabilities in different areas. Areas of Advanced Capabilities (note, a solution might have one or more of these) include:

- ✓ **Enterprise Architecture & Business Process Modeling.** Ability to visually layout business processes in a risk context and for risk documentation.
- ✓ **Risk Analytics & Modeling.** Advanced risk analytics and modeling supporting a range of methodologies and quantification
- ✓ **Risk Mobility.** Mobile architecture capabilities that easily extends new GRC applications and interfaces to mobile devices for doing risk assessements and reporting risks
- ✓ **Risk Workshops.** Capability to facillitate and manage risk workshops and support anonymous voting on risks
- ✓ **Risk Content & Intelligence.** An array of risk content and intelligence offerings integrated as part of the platform
- ✓ **Easy to Configure & Extend.** The solution is highly extensible and can be built out to support new risk processes without coding, and does not require a high degree of IT expertise.
- ✓ **Risk Normalization & Aggregation.** The solution supports advanced capabilities to normalize and aggregate risk across the environment
- ✓ **Robust Risk Analytics & Reporting.** The solution has a strong data warehouse architecture and can aggregate and report on a range of risk analytics and reporting needs involving data gathering and analysis across disparate systems.
- ✓ **Quantitative Risk Assessment Capabilities.** Ability to do quantitative risk assessments (e.g., monte carlo, VaR, bayesian)
- ✓ **Strategy and performance.** Risk solutions that manage risk in context of business strategy, performance, and objectives.

Licensed Subscriber Use Only, Do Not Distribute

Our Agenda . . .

- ✓ **Defining & Understanding Risk Management**

  Definition, Drivers, Trends & Best Practices

- ✓ **Critical Capabilities of a Risk Management Solution/Platform**

  What Differentiates Basic, Common, & Advanced Solutions

- ❑ **Considerations in Selection of a Risk Management Solution/Platform**

  Decision Framework & Considerations to Keep in Mind

- ❑ **Building a Business Case for a Risk Management Solution/Platform**

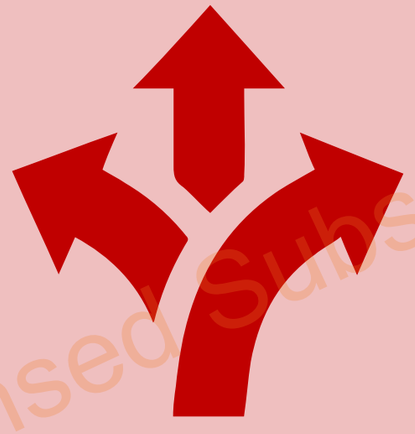
  Trajectory of Value in Effectiveness, Efficiency & Agility

Licensed Subscriber Use Only, Do Not Distribute

What is Your Approach to Risk Management?

Distributed Risk Management

- Disconnected departments managing risk in different ways with little or no collaboration with other departments



Federated Risk Management

- An integrated approach that balances risk management centralization with distributed participation and collaboration

Licensed Subscriber Use Only, Do Not Distribute

Consideration: Understand Your Risk Management Strategy & Needs

What are your needs

- Do we buy a risk assessment solution?
- Do we buy an issue-focused risk platform(s)?
- Do we buy a dedicated risk management platform at a department level?
- Do we buy enterprise/operational risk platform?
- Or do we purchase some combination of above and integrate?

grc 20/20

© GRC 20/20 Research, LLC • ww.GRC2020.com

Consideration: Understand Your Risk Management Strategy & Deployment Needs

Risk Management Strategy

- Single Platform
- Core Platform w/ Integration to Others
- Siloed Risk Solutions

Deployment Model

- Traditional Software, On-Premise
- Traditional Software, Hosted in Cloud
- Cloud, SaaS Multi-Tenant Architecture

Licensed Subscription Use Only. Do Not Distribute

Consideration: Understand Your 3rd Party Platform Needs & Integration

Risk Management Needs

- Enterprise Risk Management Needs
- Operational Risk Management Needs
- Finance/Treasury Risk Needs
- Other Department Risk Needs

GRC Integration

- Needs to be a Module in our Enterprise GRC Platform
- Needs to Integrate with Enterprise GRC Platform, but Can Be Separate
- Disconnected from GRC Platform

License Subscription Use Only - Do Not Distribute

Deployment Models

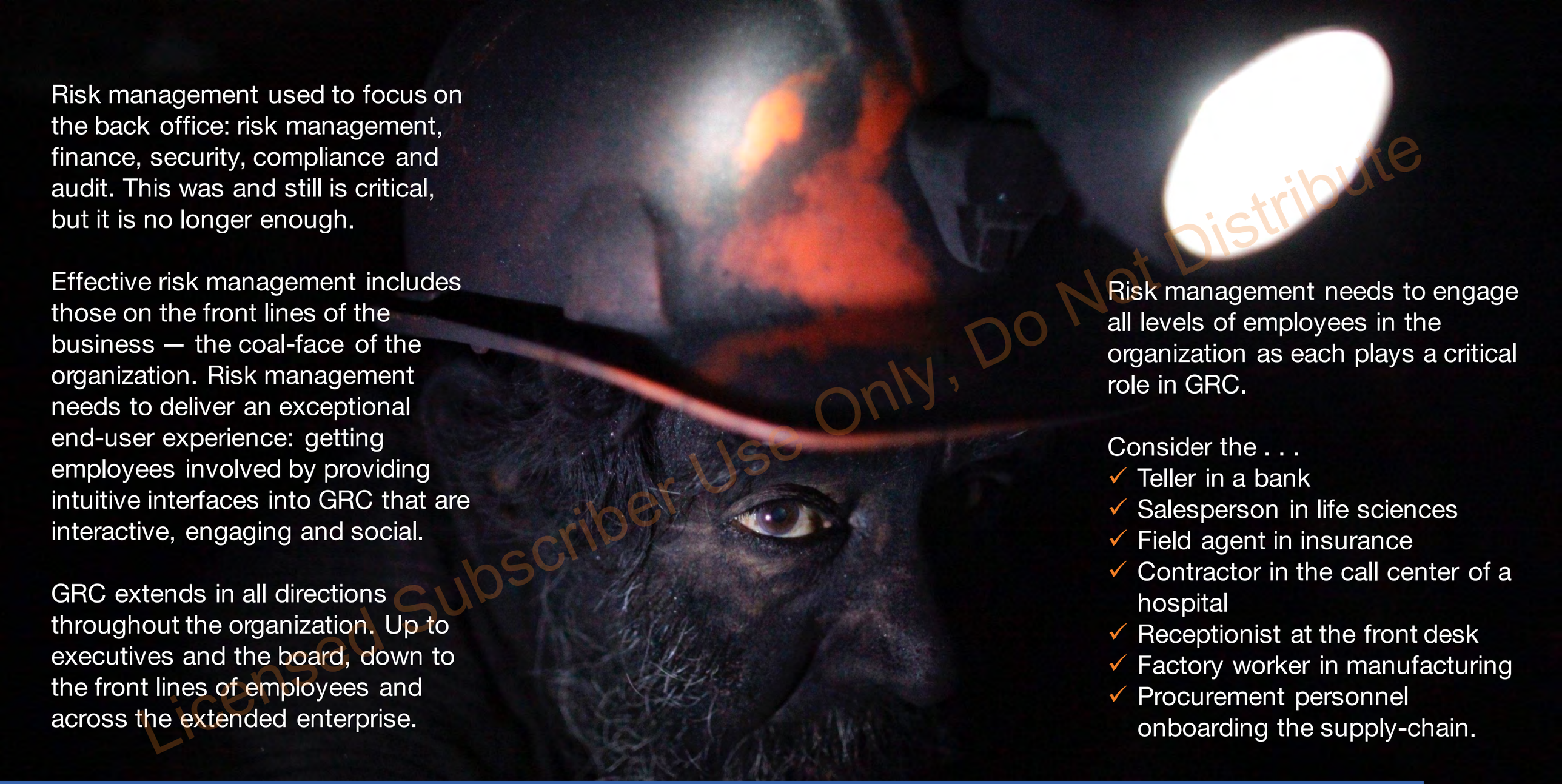
	On-Premise (Traditional)	Cloud Hosted Solution	Cloud SaaS Multi-Tenet
Overview	Installed in local data center in a client-server model, most solutions support web-browser interfaces, but some still require a thick client (application installed on user computers).	Implementation of a traditional on-premise implementation in a 3rd party data center and adds a layer of online delivery	Cloud delivering with a single code-base (multi-tenant).
Deployment	Installed on your own hardware in your own data center. Each instance of the application requires its own hardware, software, and network connectivity.	Installed on a 3rd party's hardware in a 3rd party's data center, delivered over Internet. Each instance of the application requires its hardware, software, and network connectivity (may be virtual).	Single code base supports all a solution provider's clients in a common data center, delivered over Internet.
Implementation	6 months or more	3 to 6 months	2 to 12 weeks
Customization	Often expensive and time-consuming. High risk of issues with upgrades due to customization.	Same as On-Premise	Tends to be highly configurable and avoids customization, low-risk of issues on upgrades.
Upgrades	Once a year or more	Same as On-Premise	Typically quarterly, so new features are rolled out regularly.
IT Support	Provided by customer	Mixture of customer and 3rd party hosting provider	Included in subscription and provided by solution provider
Technology Requirements	Requires IT to support a specific operating environment for the server application and database.	Same as on-premise.	Delivered by web browser over the Internet and tends to be operating system and browser agnostic.
Accountability	Solution provider is responsible for providing software updates and patches, IT is responsible for maintaining software and hardware.	Solution provider is responsible for software updates and patches as well as maintenance of software and hardware.	Solution provider is responsible for software updates and patches as well as maintenance of software and hardware.

Licensed Subscriber Use Only, Do Not Distribute

Five Key Capabilities of A Next Generation Risk Platform

1. ***Risk Engagement*** to the Frontlines of the Organization
2. ***Risk Collaboartion*** Across Roles & Departments
3. ***Risk Operationalization*** Through Defined Mapping of Business Processes
4. ***Risk Intelligence*** of External Content & Intelligence and Internal Systems & Processes
5. ***Risk Mobilization*** in Apps and Architecture for GRC

Licensed Subscriber Use Only, Do Not Distribute



Risk management used to focus on the back office: risk management, finance, security, compliance and audit. This was and still is critical, but it is no longer enough.

Effective risk management includes those on the front lines of the business — the coal-face of the organization. Risk management needs to deliver an exceptional end-user experience: getting employees involved by providing intuitive interfaces into GRC that are interactive, engaging and social.

GRC extends in all directions throughout the organization. Up to executives and the board, down to the front lines of employees and across the extended enterprise.

Licensed Subscriber Use Only, Do Not Distribute

Risk management needs to engage all levels of employees in the organization as each plays a critical role in GRC.

Consider the . . .

- ✓ Teller in a bank
- ✓ Salesperson in life sciences
- ✓ Field agent in insurance
- ✓ Contractor in the call center of a hospital
- ✓ Receptionist at the front desk
- ✓ Factory worker in manufacturing
- ✓ Procurement personnel onboarding the supply-chain.

Risk Engagement: Bringing GRC to the Coal-Face of the Organization

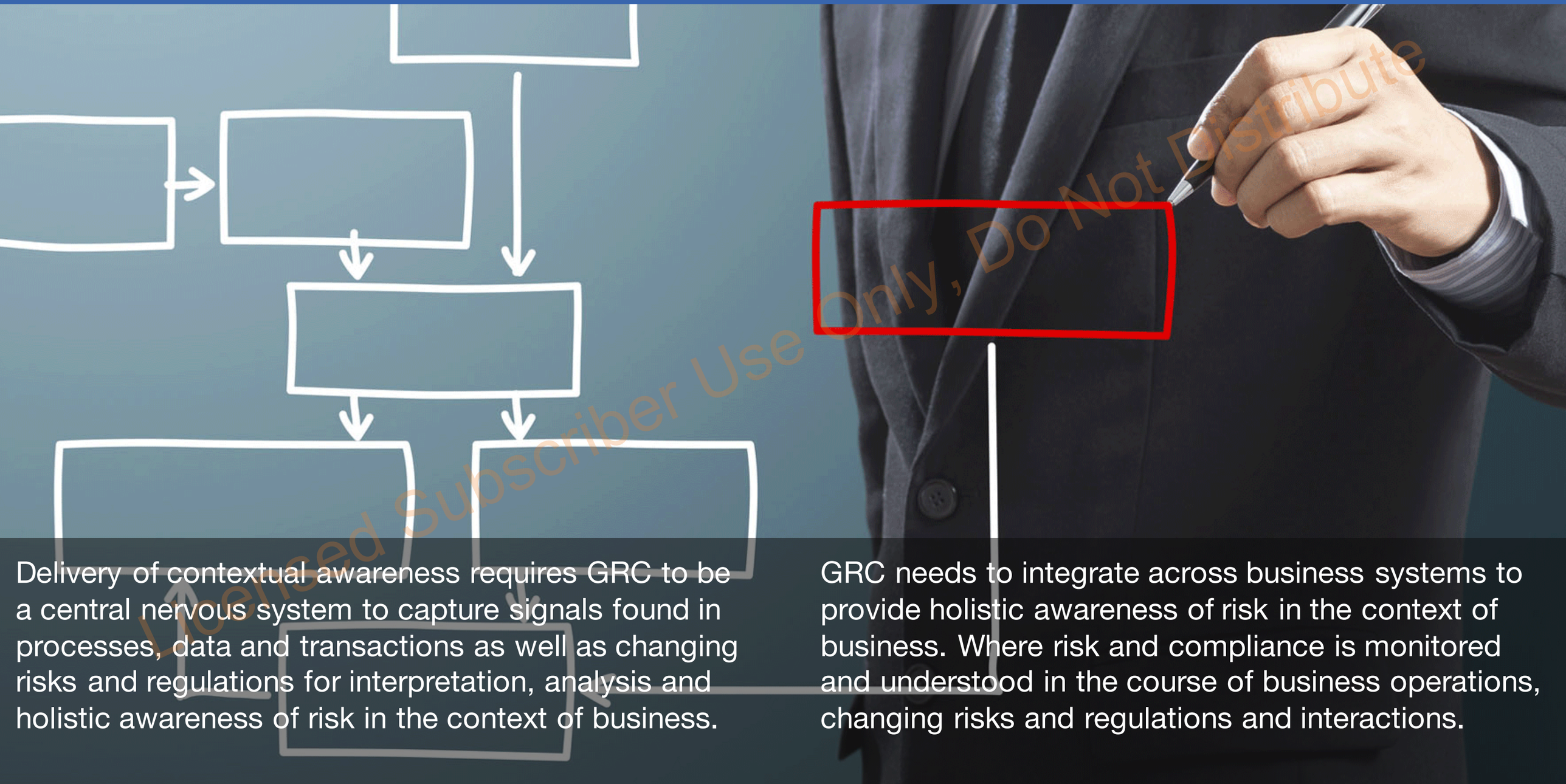
Risk Collaboration: Providing Collaboration on GRC Across the Organization

Risk management needs to provide a collaborative experience. GRC engagement is accomplished through socialization and collaboration of GRC within the organization. This involves:

- **Getting questions answered.** GRC should provide contextually relevant information as well as pathways to get questions answered.
- **Provide two-way communication.** Employees need to be able to share ideas and ways to improve GRC.
- **Sharing information.** Getting employees engaged is about sharing information allowing the organization to see what works and keeps employees engaged.
- **Connecting the dots through collaboration.** Cognitive and behavioral bias has an impact on the accuracy of results. GRC technology engages individuals in an environment in which to express true opinion, without fear of consequences.

Licensed Subscription Use Only, Do Not Distribute

Risk Operationalization: Integrating Risk Across Business Systems & Processes



Delivery of contextual awareness requires GRC to be a central nervous system to capture signals found in processes, data and transactions as well as changing risks and regulations for interpretation, analysis and holistic awareness of risk in the context of business.

GRC needs to integrate across business systems to provide holistic awareness of risk in the context of business. Where risk and compliance is monitored and understood in the course of business operations, changing risks and regulations and interactions.

Licensed Subscriber Use Only, Do Not Distribute

The integration of GRC intelligence and content sources is critical to enterprise GRC strategies of the future. This involves the delivery of content from knowledge/content providers through GRC solutions to rapidly assess changing regulations, risks, industry and geopolitical events.

Content is tagged so it can be properly routed to the right subject matter expert to establish workflow and tasks for review and analysis. Standardized formats for measuring business impact and review of existing processes, policies and controls can take place. This integration of actionable content with GRC technology delivers on GRC maturity through achievement of risk and regulatory intelligence.

Licensed Subscriber Use Only, Do Not Distribute

Risk Intelligence: Integration of Actionable Content

GRC Mobility: GRC Done & Delivered Anywhere at Anytime

GRC involves engagement through use of mobile technologies to make GRC assessable and efficient. This involves developing mobile apps for GRC that deliver:

- Policies and training
- Surveys and assessments
- Issue reporting
- Investigations
- Reporting

Licensed Subscriber Use Only. Do Not Distribute

Other Considerations to Evaluate

Organization Profile

- ❑ Company Profile
- ❑ Financial Profile
- ❑ Vision & Solution Plans
- ❑ Geographic Reach
- ❑ Industry Footprint
- ❑ Client References & Case Studies
- ❑ Brand, Reputation & Track Record
- ❑ Customer Service
- ❑ Training & Education
- ❑ Consulting & Implementation Services
- ❑ Channels, alliances, partnerships
- ❑ Demonstrated Value, Financial Benefits, & ROI
- ❑ Service Level Agreements
- ❑ Evaluation Instance & Proof of Value Support
- ❑ Post-Sales Support

Solution Architecture

- ❑ Development Platform & Technology Architecture
- ❑ Information Architecture
- ❑ Flexibility of Technology & Information Architecture
- ❑ Product Life Cycle & Updates
- ❑ Security Architecture - enterprise, entity, record, field
- ❑ Single Sign-On & LDAP
- ❑ Deployment Model – On-Premise, Hosted, SaaS
- ❑ Scalability of Solution
- ❑ Integration with Other Systems & Data
- ❑ Responsive Interface & Mobility Architecture
- ❑ Data Management & Bulk Changes
- ❑ Configuration & Customization
- ❑ Availability of Toolkits, flexibility of architecture
- ❑ Administration
- ❑ Internationalization & Contextualization
- ❑ Documentation

NOTE: these are just a selection of some common elements from GRC 20/20's RFP template containing over 500 requirements for Risk Management Platforms

Licensed Subscriber Use Only. Do Not Distribute

Other Considerations to Evaluate

Foundational Capabilities

- ❑ Workflow & Task Management
- ❑ Process Modeling
- ❑ Content & Document Management
- ❑ Cross-Referencing & Relationships of Data
- ❑ Survey & Assessment Management
- ❑ Audit Trail & Records Management
- ❑ Reporting, Dashboards & Business Intelligence
- ❑ Notifications & Alerts
- ❑ Mobility Apps
- ❑ Visualization & Analytics
- ❑ Standard & Framework Support
- ❑ Collaboration
- ❑ Business Rules Engine

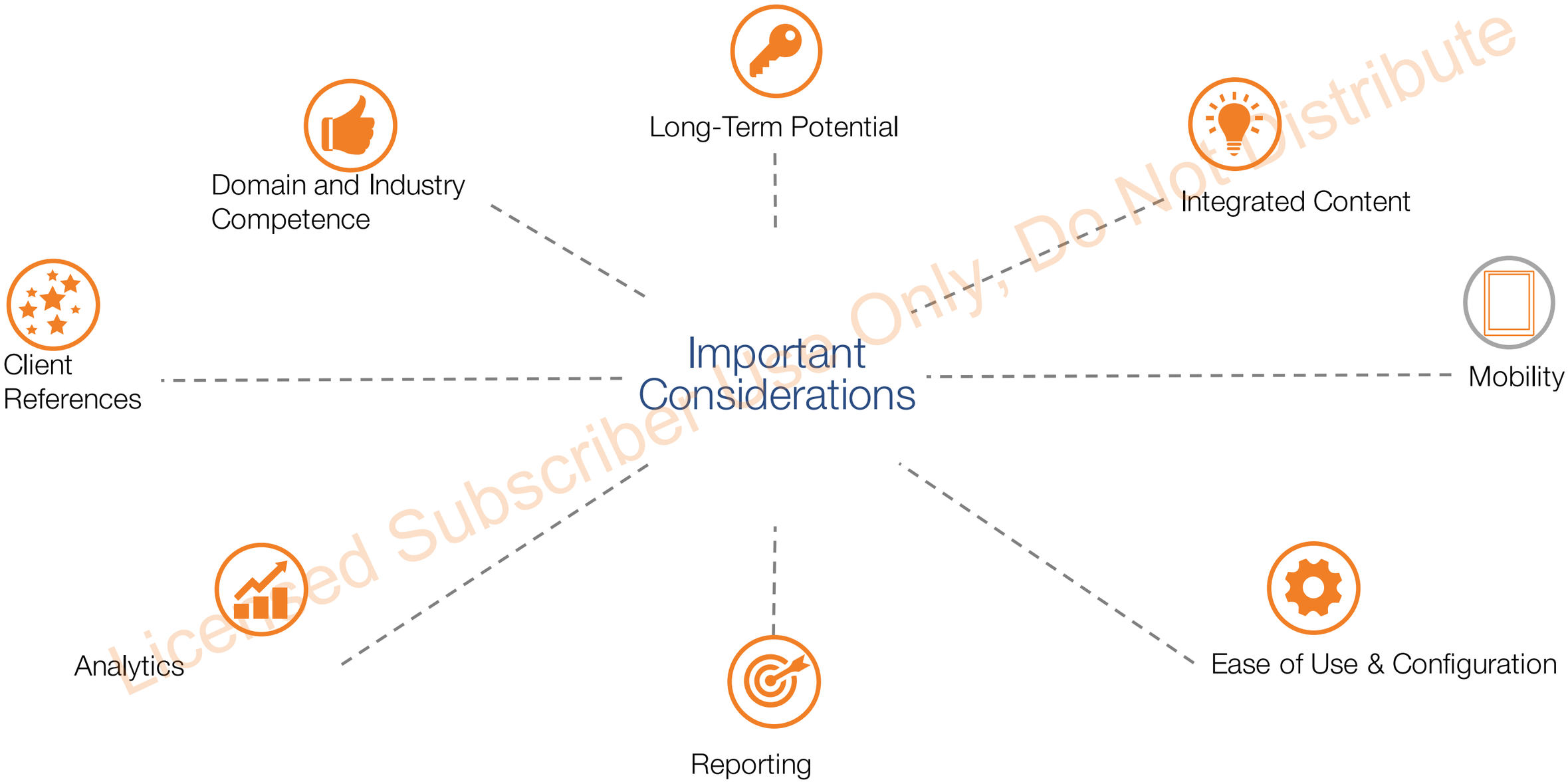
Other Topics of Consideration

- ❑ Out of the Box Features &Functionality
- ❑ Breadth of Functionality
- ❑ Depth of Functionality
- ❑ Advanced Features & Differentiators
- ❑ Usability & User Experience
- ❑ Integrated Content & Intelligence
- ❑ Embedded Domain/Industry Expertise
- ❑ R&D & Innovation
- ❑ Wizards & Contextual Help
- ❑ Role-based Experiences Devoid of Clutter

Licensed Subscriber Use Only. Do Not Distribute

NOTE: these are just a selection of some common elements from GRC 20/20's RFP template containing over 500 requirements for Risk Management Platforms

Important Considerations



Licensed Subscriber Use Only, Do Not Distribute

Key Considerations in Evaluating 3rd Party Management Platforms

Client References

Check client references. Talk to the primary reference, but also ask to talk to someone on their team that uses the solution every day.

Market Presence

Determine if the solution provider has enough market momentum or differentiating technology to be in the market for the long haul.

Enterprise Strategy

Ensure that the solution provider shares your definition and direction for your strategy for both today and tomorrow.

Business Value

The solution needs to demonstrate a clear return of value to the business in efficiency, effectiveness, and agility.

RFP Hype

Test drive the solution and asked the direct questions on features, particularly if the features are natively in the solution or have to be built out.

Solution Reach

Determine if the solution meets your industry and geographic needs to be able to support operations, languages, and content.

Licensed Subscriber Use Only, Do Not Distribute

Other Considerations in 3rd Party Management Platforms

Cost

What does the solution cost to acquire? Implement? Maintain?

Ease of Use

Does the solution bring efficiency through ease of use and intuitiveness of the platform?

Security

What is the security architecture of the platform?
How does the solution provider resolve security issues in their platform?

Information Architecture

Is the solution readily configurable and adaptable to your environment?
Does it require costly customization, programming, or consultants to adapt?

Integration

Does the solution allow for the right integration points with other analytic, control, and GRC solutions?

Agility

Does the solution meet not only your current needs but also your long term strategy over the next 3 to 5 years?

Licensed Subscriber Use Only, Do Not Distribute

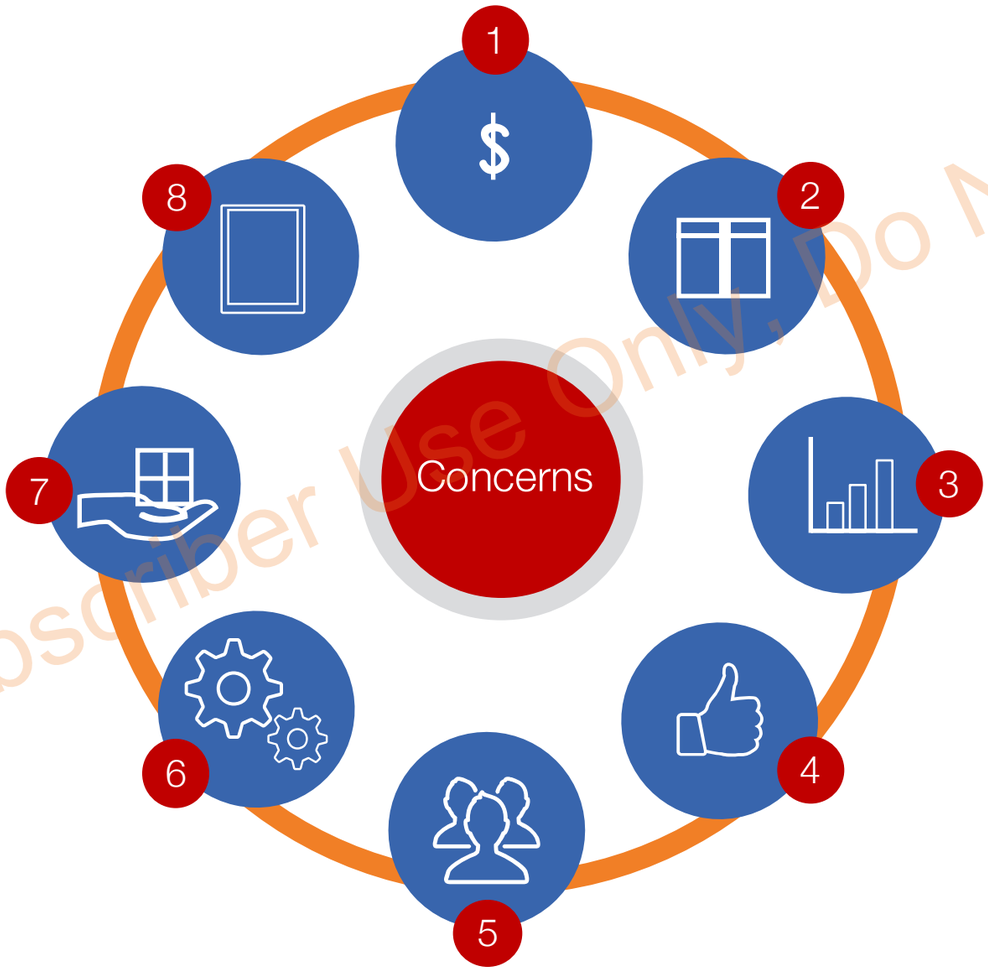
Most Significant Concerns in Evaluating Risk Management Providers

1 **Costs**
What is the reality of the acquisition and maintenance costs?

2 **Content**
Does the solution provide the right GRC content integrations?

3 **Technology Debt**
How much technology debt does the solution provider carry in promised features undelivered?

4 **RFP Responses**
Is the solution provider saying yes to everything in the RFP to win a deal?



5 **Client References**
Are the client references people actually using the solution every day?

6 **Customization**
Can you configure the solution or does it require customization & coding?

7 **Implementtion Team**
Does the implementation team have real world experience in aspects of GRC?

8 **User Experience**
Is the user experience intuitive and easy to use?

Is mobility supported?

Licensed Subscriber Use Only, Do Not Distribute

Our Agenda . . .

- ✓ **Defining & Understanding Risk Management**

  Definition, Drivers, Trends & Best Practices

- ✓ **Critical Capabilities of a Risk Management Solution/Platform**

  What Differentiates Basic, Common, & Advanced Solutions

- ✓ **Considerations in Selection of a Risk Management Solution/Platform**

  Decision Framework & Considerations to Keep in Mind

- ❑ **Building a Business Case for a Risk Management Solution/Platform**

  Trajectory of Value in Effectiveness, Efficiency & Agility

Licensed Subscriber Use Only, Do Not Distribute

Risk Management by Design: Federated Risk Management Architecture

Licensed Subscriber Use Only, Do Not Distribute

Risk Management Collaboration:
Providing Collaboration on Risk Management Across the Organization

Licensed Subscriber Use Only, Do Not Distribute

Risk Management: a Top Down Approach

- Risk Management Strategy
- Risk Management Process
- Risk Management Information
- Risk Management Technology

Licensed Subscriber Use Only Do Not Distribute

Maturing Risk Culture Through 360° Contextual Risk Intelligence Delivers . . .

1. Aware

- ✓ Have a finger on the pulse of business
- ✓ Watch for change in internal & external environment
- ✓ Turn data into information that can be, and is, analyzed
- ✓ Share information in every relevant direction

2. Aligned

- ✓ Support and inform business objectives
- ✓ Continuously align objectives and operations to risk of the entity
- ✓ Give strategic consideration to information from risk management enabling appropriate change

3. Responsive

- ✓ You can't react to something you don't sense
- ✓ Gain greater awareness and understanding of information that drives decisions and actions
- ✓ Improve transparency, but also quickly cut through the morass of data to what you need to know to make the right decisions

4. Agile

- ✓ More than fast, nimble
- ✓ Being fast isn't helpful if you are headed in the wrong direction.
- ✓ Risk management enables decisions and actions that are quick, coordinated and well thought out.
- ✓ Agility allows an entity to use risk to its advantage, grasp strategic opportunities and be confident in its ability to stay on course.

5. Resilient

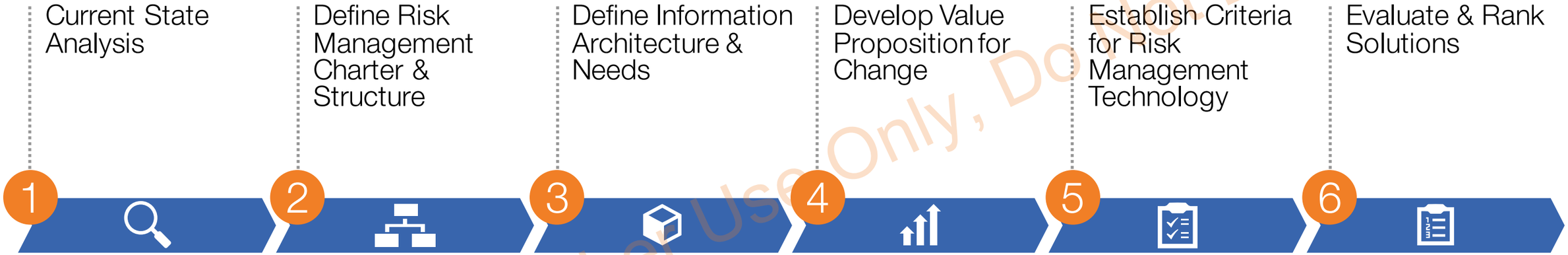
- ✓ Be able to bounce back quickly from changes in context and threats with limited business impact
- ✓ Have sufficient tolerances to allow for some missteps
- ✓ Have confidence necessary to rapidly adapt and respond to opportunities

6. Lean

- ✓ Build the muscle, trim the fat
- ✓ Get rid of expense from unnecessary duplication, redundancy and misallocation of resources within the risk management
- ✓ Lean the organization overall with enhanced capability and related decisions about application of resources

Licensed Subscriber Use Only. Do Not Distribute

Steps in Building an for Enterprise Risk Management Strategy & RFP



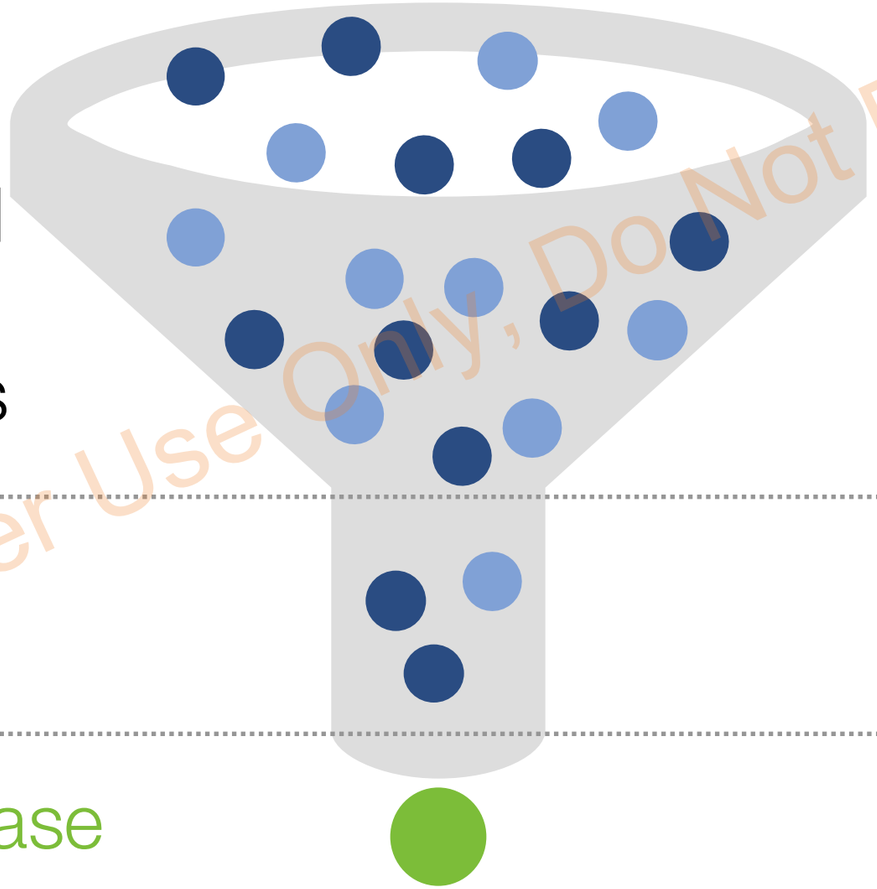
Licensed Subscriber Use Only, Do Not Distribute

Understanding Fragmented Approaches to Risk Management

1 Understand fragmented approaches

2 Determine synergies

3 Business Case



Licensed Subscriber Use Only, Do Not Distribute

Risk Management Charter

Mission Statement

STATEMENT

Accountability

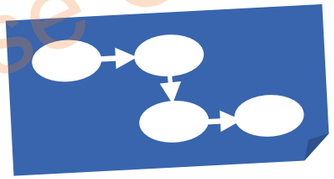
REPORTING

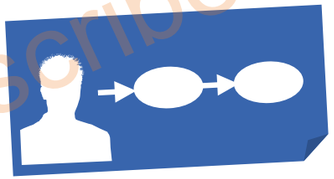
Roles Groups Involved

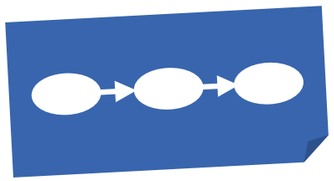
PERSONAS

Risk Management Lifecycle & Responsibilities

PROJECTS







Resources

PORTAL

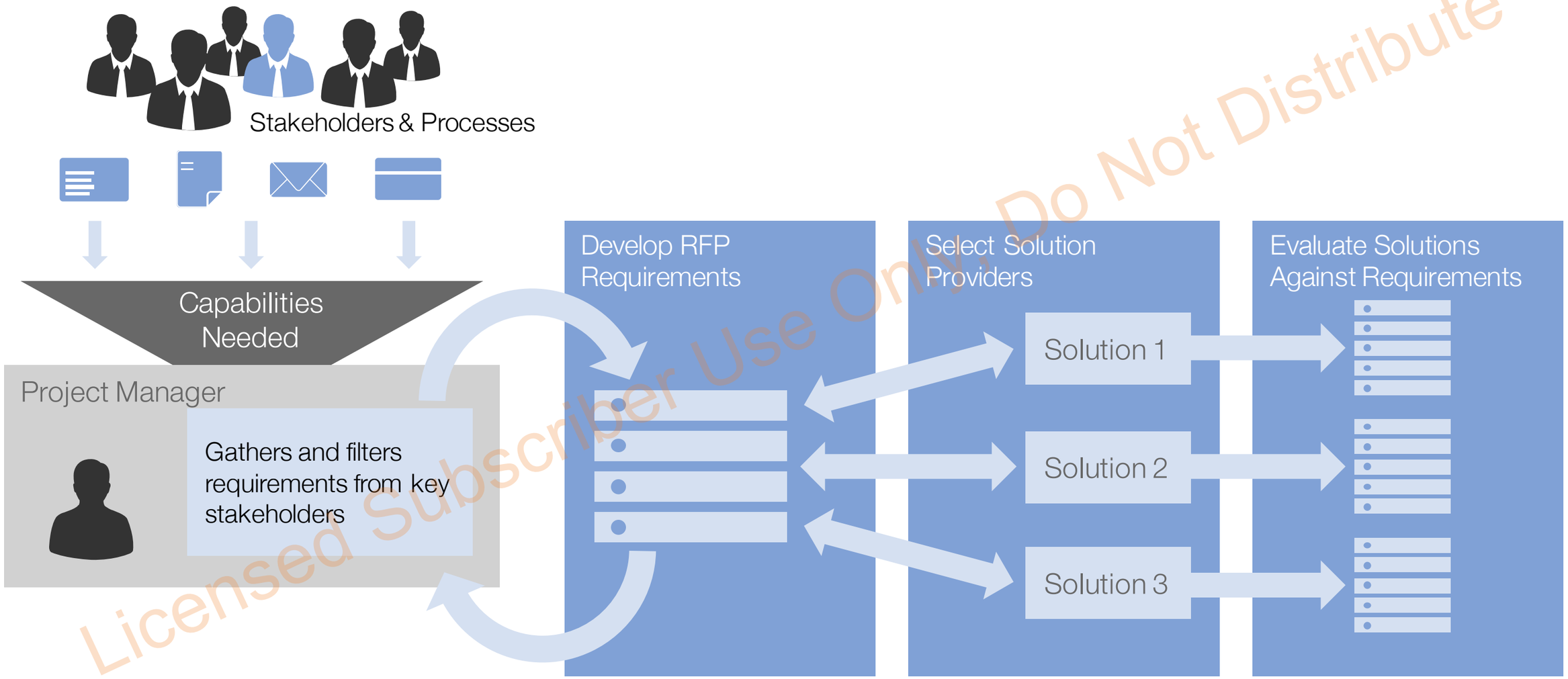
GRC

ANALYTICS

FORMS

Licensed Subscriber Use Only, Do Not Distribute

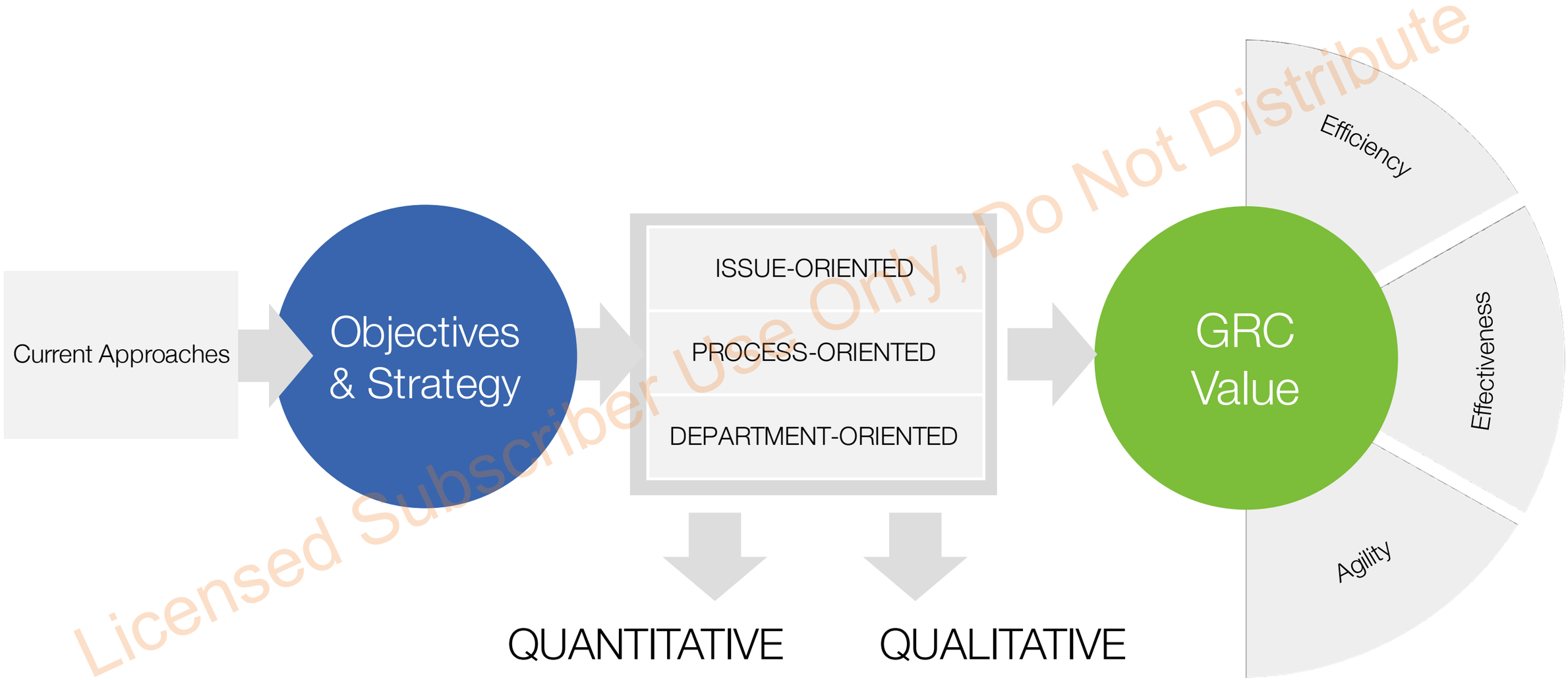
RISK Management Platform Selection Process



Licensed Subscriber Use Only, Do Not Distribute

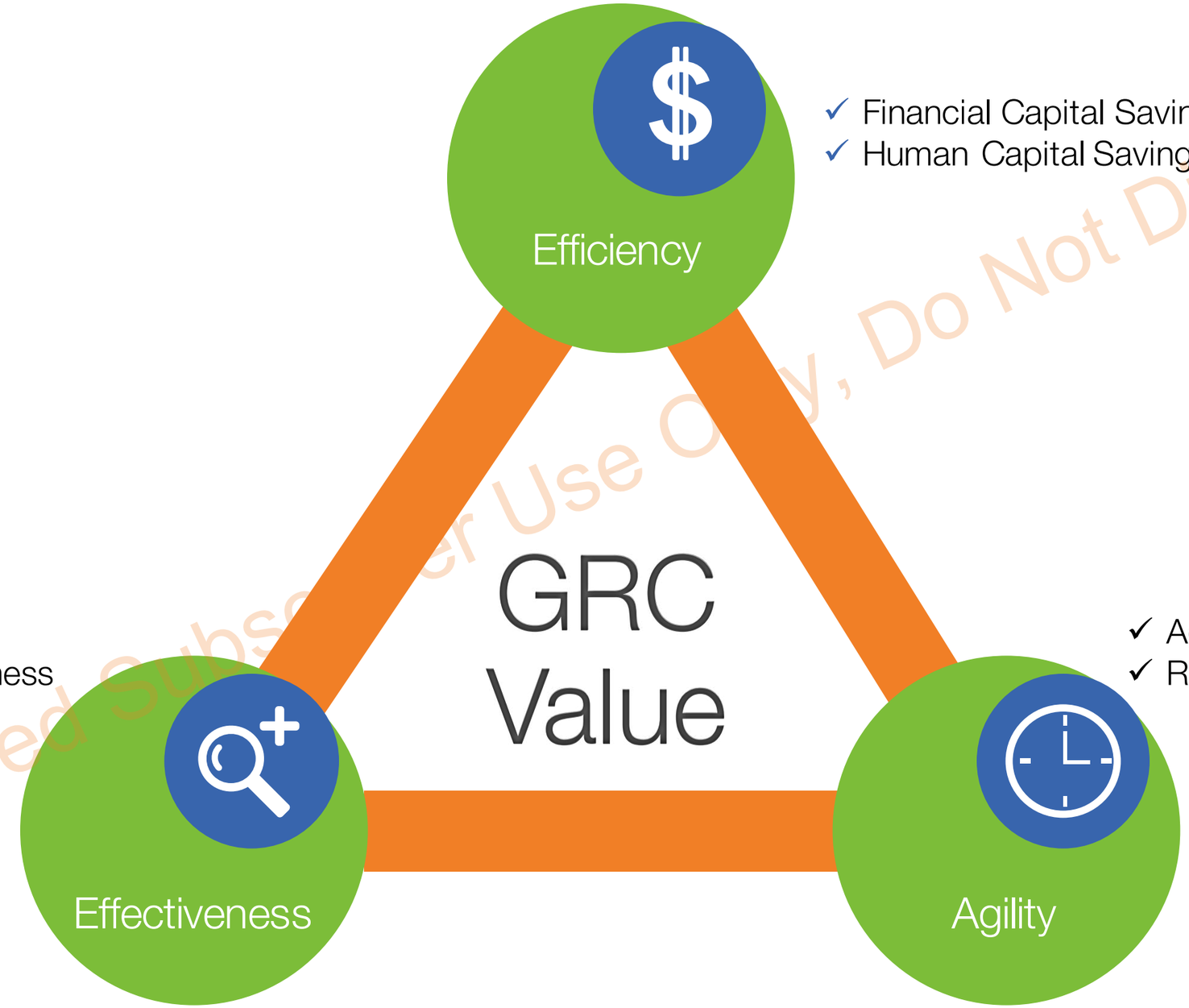
NOTE: these are just a selection of some common elements from GRC 20/20's RFP template containing over 500 requirements for Risk Management Platforms

Building a Business Case of Value



Licensed Subscriber Use Only, Do Not Distribute

GRC 20/20 Value Perspective: 3 Angles of GRC Value



- ✓ Financial Capital Savings
- ✓ Human Capital Savings

- ✓ Design Effectiveness
- ✓ Operational Effectiveness

- ✓ Agility to Change
- ✓ Responsiveness to Events

Licensed Subscriber Use Only, Do Not Distribute

Our Agenda . . .

- ✓ **Defining & Understanding Risk Management**

  Definition, Drivers, Trends & Best Practices

- ✓ **Critical Capabilities of a Risk Management Solution/Platform**

  What Differentiates Basic, Common, & Advanced Solutions

- ✓ **Considerations in Selection of a Risk Management Solution/Platform**

  Decision Framework & Considerations to Keep in Mind

- ✓ **Building a Business Case for a Risk Management Solution/Platform**

  Trajectory of Value in Effectiveness, Efficiency & Agility

Licensed Subscriber Use Only, Do Not Distribute

GRC 20/20 Offers

- ✓ **Inquiry.** Complimentary inquiry to organizations looking for GRC solutions and have straight forward questions that can be answered quickly via email or phone.

- ✓ **RFP Development.** GRC 20/20 has an extensive list of GRC related RFP requirements built over years to streamline your RFP development process.

- ✓ **Training.** GRC 20/20 is regularly engaged to come in and train organizations on GRC related strategies, processes, and architecture.

Licensed Subscriber Use Only, Do Not Distribute

Questions?

Michael Rasmussen, J.D.
The GRC Pundit & OCEG Fellow
mkras@grc2020.com
+1.888.365.4560

Subscribe GRC 20/20 Newsletter

LinkedIn: GRC 20/20

LinkedIn: Michael Rasmussen

Twitter: GRCPundit

Blog: GRC Pundit

Licensed Subscriber Use Only. Do Not Distribute

Some of the content we have evaluated is OCEG content which GRC 20/20 has an established relationship to use. Please do not copy slides or graphics without permission. GRC 20/20 highly recommends you consider OCEG membership at www.OCEG.org.