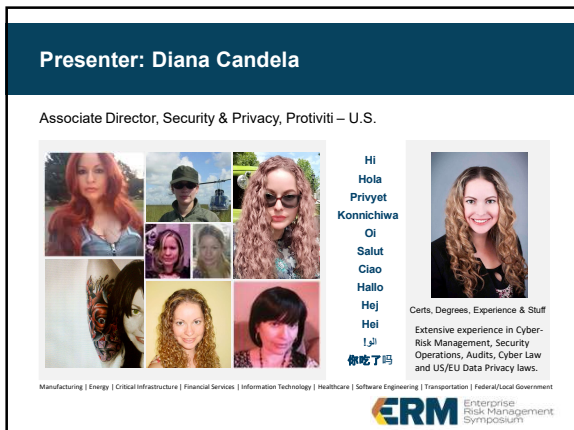




1



2



3

Presenter: Nick Lasenko



Senior Manager, Security & Privacy, Protiviti – Canada

Nick Lasenko is a Senior Manager in the Security & Privacy practice and has over 11 years of experience managing and leading projects in the areas of IT Security, Data Privacy, Risk Management and Audit. Nick's clients have been from a range of industries with a focus on Fortune 500 financial services industry in the US and Canada.


Prior to joining Protiviti Nick was a member of the Assurance practice with KPMG LLP as well as an analyst with the BMO Financial group.

Nick's prior speaking engagements included sessions on data privacy, cybersecurity and analytics. Nick also held a role as an assistant lecturer at the Schulich Executive Education Centre (SEEC) from 2010 to 2014 for Master Certificate Courses on the topic of Risk Management.



4

DISCLAIMER




The views, thoughts, and opinions expressed in this presentation are solely the speakers' own and do not express the views or opinions of their employer (Protiviti), affiliated organizations, committees or other groups or individuals.

Examples and scenarios discussed within this presentation are for illustration and educational purposes only.

Any action you take upon the information on this presentation is strictly at your own risk.

The authors are not responsible for your use of the information contained in this presentation, misuse, reuse, recycled and cited and/or uncited copies of content within this presentation.

© 2019 Protiviti Inc. This material is the confidential property of Protiviti Inc. Copying or reproducing this material is strictly prohibited.



5




protiviti
Helping You Move with Confidence

**DECIPHERING YOUR RISK APPETITE
CYBERSECURITY & PRIVACY**

THURSDAY, MAY 2, 2019
1:45 P.M. ET

PRESENTERS: DIANA CANDELA & NICK LASENKO


© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/AA/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.



6

protiviti
Face the Future with Confidence

DECIPHERING YOUR RISK APPETITE

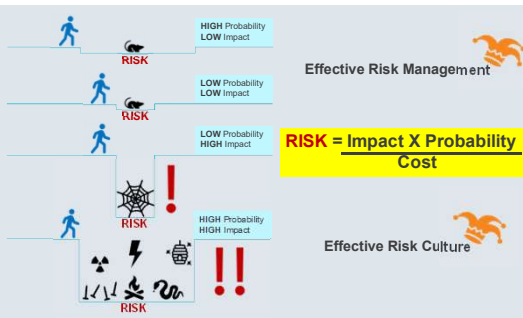


Internal Audit, Risk, Business & Technology Consulting

7

WHAT IS RISK?

The possibility of losing something of value



Effective Risk Management

RISK = Impact X Probability
Cost

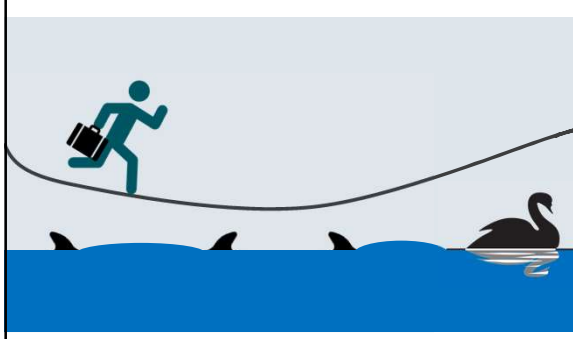
Effective Risk Culture

© 2019 Protiviti Inc. All Rights Reserved. Employee Misconduct/Innocence. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

8

RISK AVERSION EXPLAINED



© 2019 Protiviti Inc. All Rights Reserved. Employee Misconduct/Innocence. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti
The Photo by Unknown Author is

9

KEY DEFINITIONS

To establish a common nomenclature to facilitate discussions on Risk Appetite

Risk Appetite
The aggregate level and types of risk an organization is willing to assume within its Risk Capacity to achieve its strategic objectives and business plan.

Risk Appetite Framework
Risk Appetite Framework is an approach that includes policies, processes, controls, and systems through which Risk Appetite is established, communicated, and monitored. It outlines roles and responsibilities of those overseeing the implementation and monitoring of the Risk Appetite framework.

Risk Appetite Statement
The articulation in written form of the aggregate level and types of risk that an organization is willing to accept, or to avoid, in order to achieve its business objectives. It includes qualitative statements as well as quantitative measures expressed relative to relevant measures as appropriate.

Risk Capacity
The maximum level of risk the institution can assume given its current level of resources before breaching constraints determined by regulatory, liquidity and operational environment needs.

Risk Tolerance is a breakdown of the organization's Risk Appetite enabling personnel to consider Risk while performing their activities.

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

10

RISK MANAGEMENT EXPLAINED

This Photo by Libbyman. Author is licensed under CC BY-NC

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

11

THE PERCEPTION OF RISK

Perception is reality

Highlight

The perception that any specific focus on area and/or culture will increase the risk and therefore the liability of senior leadership.

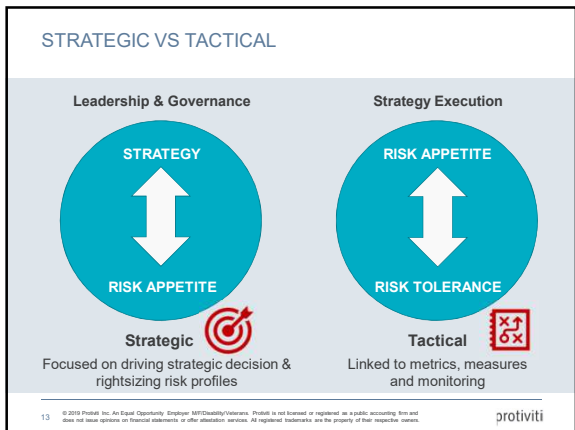
Year	Percentage
2016	67%
2017	70%
2018	73%

Components of Risk

- X% culture, ethics, integrity
- X% corporate governance, tone from the top
- X% conflicts of interest

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

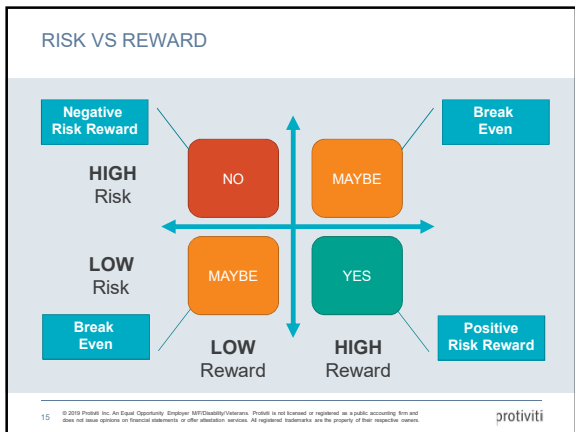
12



13



14



15

PUTTING IT ALL TOGETHER

Risk Universe **KRI** **Risk Levels** **KPI**

Risk Capacity
Risk Tolerance
Risk Appetite
Risk Tolerance
Risk Capacity

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

16

RISK APPETITE STRATEGY

Risk Appetite is a widely accepted concept, however one that **remains difficult to apply in practice**. It's really all about **defining, implementing and utilizing Risk Appetite**.

The generally recognized challenge regarding Risk Appetite is how to implement an **effective, enterprise-wide Risk Appetite Framework** which translates to Senior Leadership, high-level risk objectives into **clear, understandable guidelines and metrics** for business units and operations personnel.

The stakeholders, shareholders, investors, regulators, and general public have been **raising expectations** for risk management and corporate governance. Risk Appetite is one of the key components and an enabler of effective governance and risk management.

Stakeholders believe driving Risk Culture throughout an organization (resulting in a **shared understanding and compliance** with the risk appetite), is equally as important as having written **Risk Appetite Statements**. Especially in large organizations, where **consistency in understanding and realizing Risk Appetites** throughout business lines is critical.

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

17

RISK INDICATORS

Inherent Risks

- Vulnerability of customer base
- Complexity of products, including degree of risk transfer
- Type of distribution model
- Use of 'big data'
- Quality of initial and ongoing disclosure

Material Misstatements

Governance & Business Processes

- Extent to which customer interests are reflected in strategy and objectives
- Extent of alignment between customer interests and remuneration/incentive/performance management of staff and management
- Levels of staff training on conduct of business issues
- Quality of controls in outsourcing arrangements
- Product design/sales process
- Use of 'bundles' or add-on products

Strategic Misalignments

Economic & Environmental Factors

- Levels of consumer indebtedness in target market
- Extent of customer exposure to market performance
- Extent of involvement in high-risk market-wide practices

Liabilities, Loss Hazards, Exposure

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

18

RISK APPETITE METRICS

Measuring Risk Appetite

The establishment of Risk Appetite metrics generally coincides with strategic planning. The metrics are refined based on a dynamic risk environment. Many organizations apply a top-down and bottom-up approach to metrics, as represented in the pyramid below.

- Risk Appetite Metrics**
 - Enterprise measures reported directly to Board of Directors/Senior Leadership
 - Directly tied to Risk Appetite Statement
 - Designed to measure risk across the entire organization
- Enterprise KRIs**
 - Supplemental or additional metrics
 - Factor into risk-based decisions made at the enterprise level
 - Measured across all lines of business
- Business Unit KRIs**
 - Developed to support from Enterprise Risk Management
 - Specific to each Business Unit
 - Provide leaders with measures to manage risk in addition to risk appetite metrics

19 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

19

RISK APPETITE PROCESS

The assessment of Risk Profile against Risk Appetite is an ongoing and iterative process facilitated by continuous communication. The successful adoption of an organization will be influenced by many factors that drive Risk Culture.

20 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

20

STRONG RISK APPETITE STATEMENT

Key Characteristics

- Forward Looking**: Allows the organization to view the desired risk profile under a variety of scenarios.
- Informed**: Includes key background information and assumptions that informed the strategic and business plans at the time they were approved.
- Linked to Corporate Goals**: Has strong linkages with the short- and long-term organizational strategy, capital and financial plans. Risk metrics are aligned to this incentive compensation plan and employees are appropriately incentivized to support prudent risk taking in line with organizational goals.
- Defined Risks**: Clearly establishes the type and amount of risk the organization is prepared to accept in pursuit of its strategic objectives and business plan.
- Material Risk-Focused**: Expresses the maximum level of risk (material and overall) the organization is willing to accept within, under normal and stressed conditions.
- Quantitative**: Includes measurable, frequency based, understandable and comparable risk metrics that can be translated into risk limits applicable to business lines, legal entities and group level, and linked enterprise wide.
- Supported**: Is supported by appropriate controls and stress tests.
- Supported**: Includes qualitative statements that articulate the rationale for taking on or avoiding certain types of risks and includes a reasonable number of appropriately selected risk metrics.

21 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

21

RISK-BASED DECISIONS

There are so many!

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

22

UNDERSTANDING RESIDUAL RISK

There will always be some residual risk

There are **three** fundamental responses to risk:

Avoid	Reduce	Share
Eliminate the risk by preventing exposure to future possible events from occurring.	Implement policies and procedures to lower the risk to an acceptable level.	Shift the risk to a financially capable, independent counterparty.

Total Risk - **Avoid, Reduce, Share** = **Residual Risk**

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

23

A CONCEPTUAL RISK APPETITE FRAMEWORK

Parameters / Metrics (examples)	Possible levels to be defined
<ul style="list-style-type: none"> Strategic parameters <ul style="list-style-type: none"> Markets (allowed or not) Customers (allowed or not) New products (allowed or not) Levels of concentration of markets, products, customers MSA initiatives Strategic parameters <ul style="list-style-type: none"> EPS EBIT/EBITDA FCF Debt Rating Operating parameters <ul style="list-style-type: none"> Levels of customers & customer satisfaction Saturation of the production lines Tariffs and tariff targets Continuity of service Compliance parameters <ul style="list-style-type: none"> Requirements of health, safety and environment Other relevant compliance requirements 	<ol style="list-style-type: none"> Risk Capacity Maximum level of risk that a company is able to absorb without compromising business continuity Risk Tolerance Maximum level of risk that a company is prepared to tolerate (i.e., not expected) in the pursuit of its objectives Risk Target Optimal level of exposure to risk which strive to achieve the best balance between risks and expected returns Risk Profile Assessment and measurement, at a given time, of the exposure of the issuer to business risks

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

24

IMPLEMENTING RISK APPETITE FRAMEWORKS

Several Key Steps:

- Communicate the Risk Appetite Statement
- Allocate Risk Appetite to Different Groups
- Monitor compliance with risk appetite
- Report Relevant Risk Appetite Information
- Act and Correct
- Re-evaluate and Adjust

An effective Risk Appetite Framework is an integral part of the overall Enterprise Risk Management (ERM) methodology of an organization.

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

25

CURRENT VS. FUTURE STATE

- Unknown sources of risks
- Risk Appetite unknown and undefined

Where are you today?

Uncertainty
knowledge of risks exists but clear mechanisms not in place to help prioritize and mitigate

Risk Assessment

- Risks are identified and assessed using clear Risk Appetite Statement and Risk Tolerances
- Risks are effectively managed

Where do you need to be?

Clarity
after the Risk Appetite Framework is developed and implemented

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

26

STRATEGY EXPLAINED

"The way forward is clear."

© 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners.

protiviti

27

RISK INFORMED STRATEGY

Risk Management

A collaborative three-year strategic plan that addresses material risks and allows for continuous calibration to the evolving risk appetite of the organization. The strategic plan is focused on growth and innovation, encourages a customer-centric view and establishes a desire to provide industry-leading customer service.

Key Elements

- In consistent alignment with the Risk Appetite of the organization, addressing each risk as it emerges.
- Stakeholders are engaged throughout the strategic planning process.
- Ongoing monitoring of the strategic plan.
- Utilized by the entire organization, departmental and functional plans are aligned to the strategic plan and the plan is consistently measured against the risk appetite.

Development Cycle

- Strategic Plan Development
 - Developed by the business with collaboration, discussion and oversight from the control partners.
 - Contains the overall vision statement and strategic objectives defining the organization's Risk Appetite.
 - The Board of Directors/Senior Leadership must challenge, evaluate, and approve the written plan.
- Includes an assessment of all risks faced by organization for the past three years.
- Focuses on maximizing customer satisfaction, profitability, growth and innovation.

Evaluation Cycle

- Perform an annual assessment to determine progress made on strategic plan.
 - Create performance and risk measures.
 - Collect, analyze and report performance and risk measure metrics.
 - Compare metric performance to strategic plan.
 - To the extent that goals have changed, update the strategic plan accordingly.

28 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

28

STRATEGIC PLAN DEVELOPMENT

Participate in Strategic Plan Development

Assess and Evaluate

1
Strategic Plan Development

Annual Assessment

Alignment to Risk Appetite

Engage the right control partners

Align with company mission/vision, strategy, and risk appetite

Focus on improving customer satisfaction, profitability, growth, and innovation

Involve BU's to challenge, evaluate, and approve written plan

Details

Development Cycle

- Identify control partners and resources to assist with strategic plan development (e.g. Risk, Internal Audit, Legal, Compliance, BOD, etc.)
- Understand organizational conditions and initiatives within all business units
- Determine key metrics to be used for ongoing plan governance
- Research trends within the Internal and external environments (e.g. External: competitor activities; Internal: financial performance)
- Utilize BU's to set strong "tone at the top" through engagement in the strategic planning process and approval of final 3-year plan

29 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

29

STRATEGIC PLAN DEVELOPMENT

Participate in Strategic Plan Development

Assess and Evaluate

Strategic Plan Development

2
Annual Assessment

Alignment to Risk Appetite

Collect, analyze, and report performance and risk metrics

Perform and report off-cycle assessments of company risk profile

Annually assess progress of strategic plan implementation

Update three-year risk profile/strategic plan as needed

Detailed How

- Create strategic plan refresh program that establishes refresh frequency, responsibilities, assessment and reporting guidance
- Distribute enterprise-wide governance guidelines and templates to all control partners to ensure assessments are conducted formally and consistently across business lines (e.g. Partner-specific roles & responsibilities, charter, refresh user guides, etc.)
- Present progress assessment and updated strategic plan to Board for approval after each annual assessment

30 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestation services. All registered trademarks are the property of their respective owners. protiviti

30

STRATEGIC PLAN DEVELOPMENT

Align ongoing risk appetite planning with strategic planning

Assess changes to internal and external environments and market conditions

Maximize teams' abilities to deliver and respond quickly to emerging events

Utilize partners for credible challenges

Details

- Delegate ownership responsibilities throughout the enterprise
- Clearly define forums and committees for control partners to report evolving risks and changing conditions that could have an impact on risk appetite and/or strategic plan alignment (e.g. Management-level, Committee-level, Board-level reports)
- Periodically provide credible challenge to performance and risk metrics in the strategic plan to ensure metrics are still applicable to risk in the current state.
- Through defined forums and committees, identify areas where new metrics should be implemented

31 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners. protiviti

31

ORGANIZATIONAL ALIGNMENT

Benefit: Aligned Organization –
A risk-informed strategic plan sets a strong tone at the top. It conveys the message that risk management is paramount to institutional success.

Benefit: Operational Excellence –
Opportunities are assessed through alignment to the strategic plan and Risk Appetite.

Benefit: Customer Satisfaction –
Successful anticipation and response to a rapidly changing competitive environment.

Participate in Strategic Plan Development → **Assess and Evaluate**

- Ensure plan has been developed in collaboration with control partners and addresses all material risks and allows for continual calibration to the evolving risk appetite and profile of the organization.
- Perform off-cycle risk assessment to determine whether the strategic plan adequately addresses all current risks.
- Conduct an annual assessment to determine progress made on strategic plan and if goals have changed update accordingly.
- Align strategic planning and risk appetite planning processes to ensure all risks are addressed in the strategic plan.

32 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners. protiviti

32

RISK GOVERNANCE EXPLAINED

RISK GOVERNANCE DASHBOARD

NUMBER OF MEETINGS

NUMBER OF RISKS IDENTIFIED

WEIGHT OF RISK REPORTS

AUDIT OVERSILL

LOW HIGH

WELL, THAT'S ALL RIGHT THEN.

33 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners. protiviti

33

COMMON PITFALLS

The breadth of a Risk Appetite Statement, combined with the ever-increasing size and complexity of modern organizations, can pose a number of challenges, often seen when driving the risk appetite throughout the organization. The most common pitfalls, which may lead to implementing a Risk Appetite Framework which is too theoretical, far away from the business reality, not recognized by the business lines, impracticable to implement or cumbersome to maintain.

- Not involving the key strategic personnel in the risk appetite process
- Too centralized approach where Risk appetite metrics are developed by the head-office without a bottom-up input
- Tracking an excessive number of metrics throughout the enterprise
- Data integrity issues preventing a proper consolidation to achieve enterprise wide view
- Lack of a common, clear consistent methodology for setting appetites, limits and thresholds
- Risks identified on a low granular / too specific level instead of being driven by material risk categories
- Thresholds based on inaccurate or insufficient data, and not adjusted appropriately

34 © 2019 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

34

Questions

ERM Enterprise Risk Management Symposium

35

Contact Information

- Diana Candela diana.candela@protiviti.com
- Nick Lasenko nick.lasenko@protiviti.com

ERM Enterprise Risk Management Symposium

36
