

RSAC[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: RMG-T12

Effective (and Agile) Enterprise Risk Management? Yes We Can!



Vic Bhatia

Consultant – Security Risk and Compliance

A Tech Company

@VicBhatia

#RSAC


Effective (and Agile) Enterprise Risk Management

Today's Agenda

1. Review a Case Study
 - ERM Initiative at a SaaS Company Called - *OurERM: Managing Risk. Together.*
2. Apply What You Have Learned Today
 - What to Do (and Not to Do)
3. Q&A / Open Discussion

RSAConference2020

1. Review a Case Study



Presenting risk metrics to the Board of Directors is like reading the Bible to a cat.

The cat will stare at you the entire time and appear to be deeply contemplating every word you say, but it has absolutely no idea what you are talking about!

Key Business Risk Areas

Tip: Check out **Item 1A. Risk Factors** listed in 10-K SEC filings

Risk Areas	Key Factors
<ul style="list-style-type: none">• Brand and Reputational Risk	<ul style="list-style-type: none">• Catastrophic (“black swan”) events may disrupt our business• If our goodwill or amortizable intangible assets become impaired, then we could be required to record a significant charge to earnings
<ul style="list-style-type: none">• Competitive Risk	<ul style="list-style-type: none">• If we cannot continue to develop, acquire, market and offer new products and services or enhancements to existing products and services that meet customer requirements, our operating results could suffer• Failure to manage our sales and distribution channels effectively could result in a loss of revenue and harm to our business
<ul style="list-style-type: none">• Compliance and Regulatory Risk	<ul style="list-style-type: none">• We are subject to risks associated with compliance with laws and regulations globally, which may harm our business

Key Business Risk Areas (...cont'd)

Risk Areas	Key Factors
<ul style="list-style-type: none">• Financial Risk	<ul style="list-style-type: none">• If our customers fail to renew subscriptions in accordance with our expectations, our future revenue and operating results could suffer
<ul style="list-style-type: none">• Information Security and Privacy Risk	<ul style="list-style-type: none">• Security breaches in data centers we manage, or third parties manage on our behalf, may compromise the confidentiality, integrity, or availability of employee and customer data, which could expose us to liability and adversely affect our reputation and business• Security vulnerabilities in our products and systems could lead to reduced revenue or to liability claims• Increasing regulatory focus and expanding laws on privacy issues could impact our business models and expose us to increased liability

Key Business Risk Areas (...cont'd)

Risk Areas	Key Factors
<ul style="list-style-type: none">• Operational Risk	<ul style="list-style-type: none">• Introduction of new technology could harm our business and results of operations• We rely on data centers managed both by us and third parties to host and deliver our services, as well as access, collect, use, transmit, and store data, and any interruptions or delays in these hosted services, or failures in data collection or transmission could expose us to liability and harm our business and reputation• Our intellectual property portfolio is a valuable asset and we may not be able to protect our intellectual property rights, including our source code, from infringement or unauthorized copying, use or disclosure

Key Business Risk Areas (...cont'd)

Risk Areas	Key Factors
• Key Personnel Risk	• If we are unable to recruit and retain key personnel, our business may be harmed
• Market Risk	• Revenue, margin or earnings shortfalls or the volatility of the market generally may cause the market price of our stock to decline
• Supplier and Third-Party Risk	• Failure of our third-party providers to adequately address service requests could harm our business and adversely affect our financial results
• Transaction Risk	• We may not realize the anticipated benefits of past or future investments or acquisitions, and integration of acquisitions may disrupt our business and management

The Key Business Risk Areas Determine the Discussion Items for Executive Leadership

- What are **our business objectives and strategies**? What are our financial targets, e.g., profitability, size and revenue growth? What values do we want to build and reinforce?
- What markets do we choose? What relative market position do we seek? What is our **business model** for winning in our chosen markets?
- What specific possible **future events** do we face? Are they related?
- How **sensitive** are our strategies, markets, earnings and cash flow to the occurrence of future events? How risky are our tangible and intangible assets for creating value?
What are the loss drivers affecting those assets?

Discussion Items for Executive Leadership (...cont'd)

- Which specific future events could, if they occurred, affect the Company's **ability to achieve its objectives** relating to quality, innovation, timeliness, safety, compliance, etc., and to execute its strategies successfully? Which events would affect our market share?
- How **capable** are we of responding to events beyond our controls that may happen in the future?
- Do we know what our expected returns are, **as adjusted for risk**? Do risk-adjusted returns vary by business unit? By major product? By geography?

Discussion Items for Executive Leadership (...cont'd)

- Finally, if we decide to accept the exposures inherent in our business model that give rise to our existing risks, do we have **sufficient capital** to absorb significant unforeseen losses should they occur?

The Leadership Discussions Help Define the ERM Services

“What are the risks, how are they managed, and how do you know?”

NOW

1. Develop a common understanding of risk across multiple functions and business units so we can manage risk transparently and cost-effectively on an enterprise-wide basis
2. Improve capabilities to respond effectively to “black swan” risks (low probability / critical, catastrophic risks)
3. Build safeguards against earnings-related surprises

LATER

4. Link risk management to more efficient capital allocation and risk transfer decisions
5. Integrate risk management into critical management activities, e.g., strategy-setting, business planning, capital expenditure and M&A due diligence and integration processes

The ERM Services Help Define the ERM Organization...

Executive Sponsor
Chief Risk Officer

- **Sponsor** organizational change
- Help **mature** the Company's ERM program

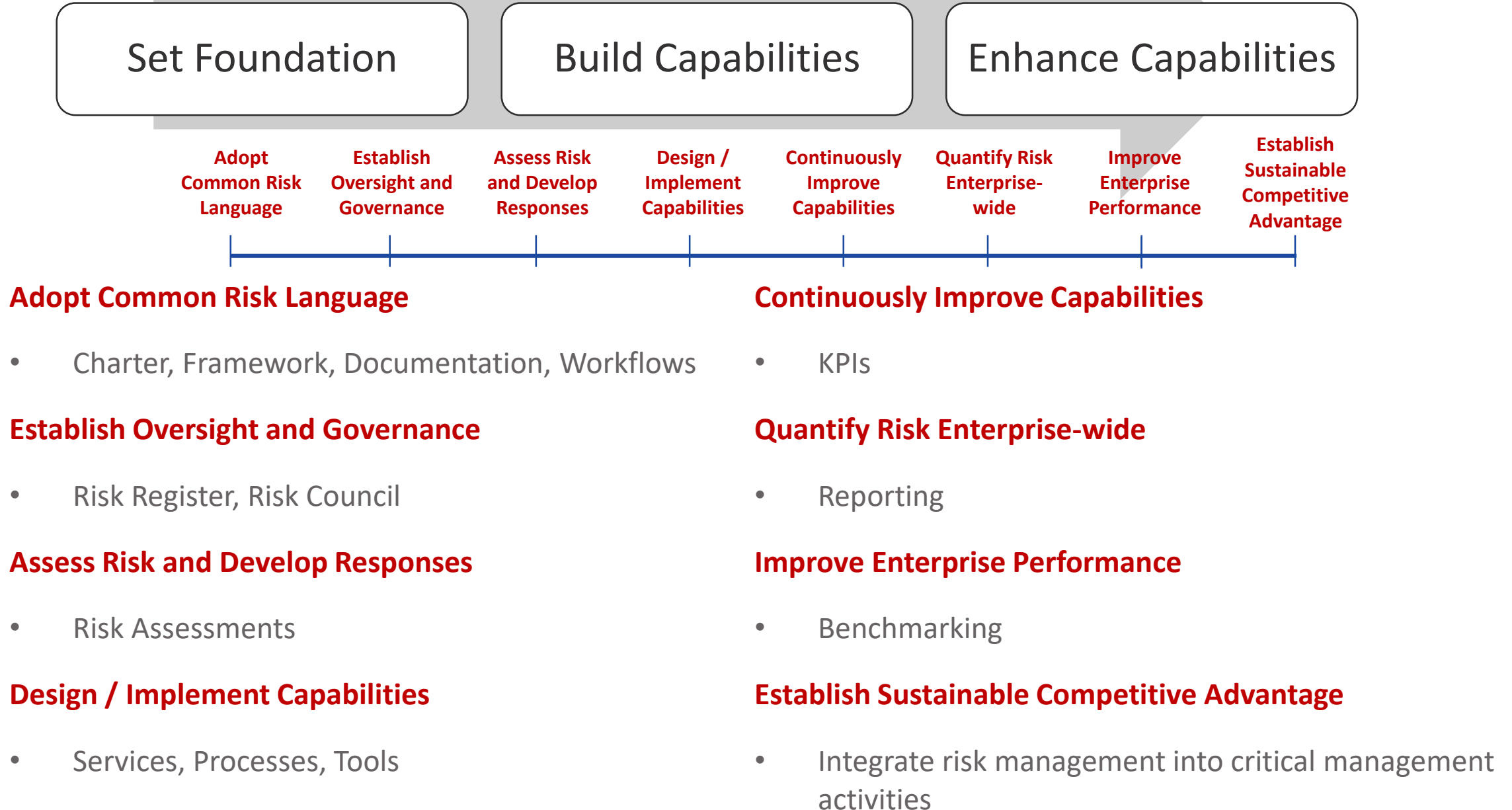
ERM
Function Leader

- Establish the **foundational elements**
- Build the **capabilities** needed

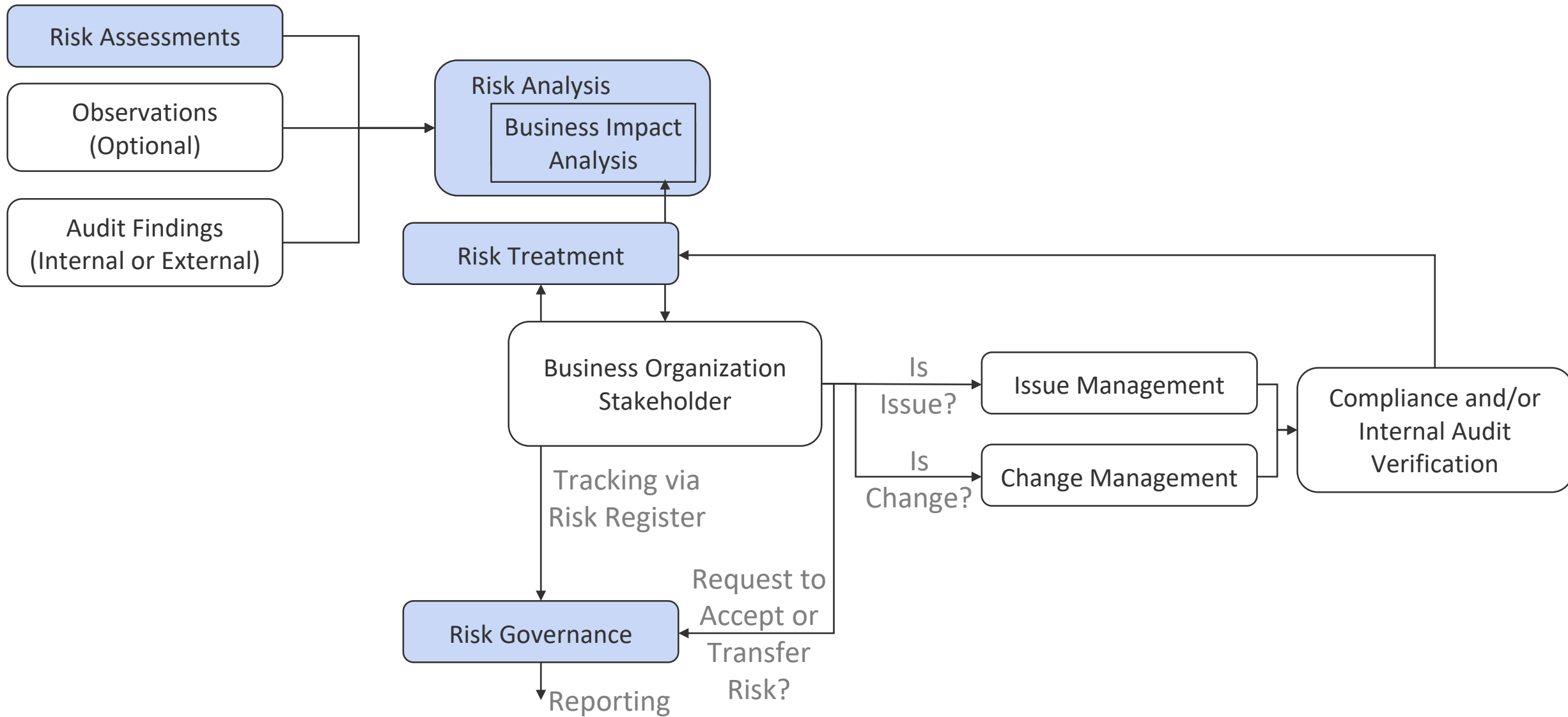
ERM
Program Manager

- Develop **intuitive** tooling and reporting
- **Onboard** stakeholders

... and the Roadmap



Which then Helps Define the Engagement Model



Long term, Internal Audit verifies that the engagement model is working end-to-end

Start with the Risk Assessments

See for additional guidance and templates:
https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment

Help make the following type of risk-based decisions:

- Is the security provided by a given platform appropriate to host a specific classification of data?
- How much should we care about maintenance, etc.?
- Is there anything obvious we should really look at fixing right now?
- Where should we focus our efforts to significantly reduce the business risks to or through the service?
- Did we forget anything, or have any blind spots we had not thought of?

Good Risk Assessments Are

- **Quick!** The risk assessment should take 30 - 60 minutes maximum.
- **Very high-level.** Can become a complete threat model over time though!
- **Concise, readable.** Short and with clear risk levels.
- **Easy to update.** Can be run during any phase of the project development and continuously updated.
- **Informative.** Collects risk impact and a data dictionary. Also collects information about how the service functions.
- **Actionable.** The assessment includes the recommendations from the enterprise risk management team with a priority for each item.

Key Attributes Tracked in a Risk Register

Assessment

- Vulnerability
- Likelihood
- Impact
- Any Applicable Controls

Issue

- Impacted **Business Process**
- Status

Treatment

- Plan {Accept, Correct, Mitigate}
- Residual Risk

RSAConference2020

2. Apply What You Learned Today

Apply What You Have Learned Today

- **Next week you should:**
 - Check out *Item 1A. Risk Factors* listed in 10-K SEC filings and identify the key business risk areas that apply to your company
- **In the first three months following this presentation you should:**
 - Have leadership discussions, and define the ERM charter
 - Use the charter to define your services. Use the services to define your organization. Use these both to then define the engagement model for collaborating with stakeholders
- **Within six months you should:**
 - Drive implementation projects to achieve the first 4 milestones of your roadmap: *Adopt Common Risk Language, Establish Oversight and Governance, Assess Risk and Develop Responses, Design and Implement Capabilities*

Some Tips

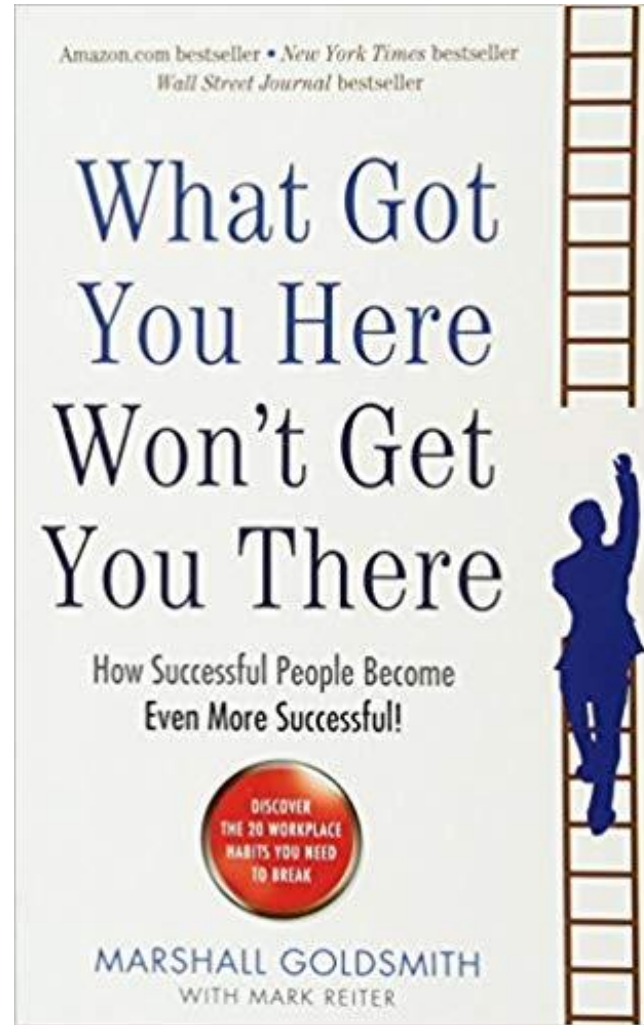
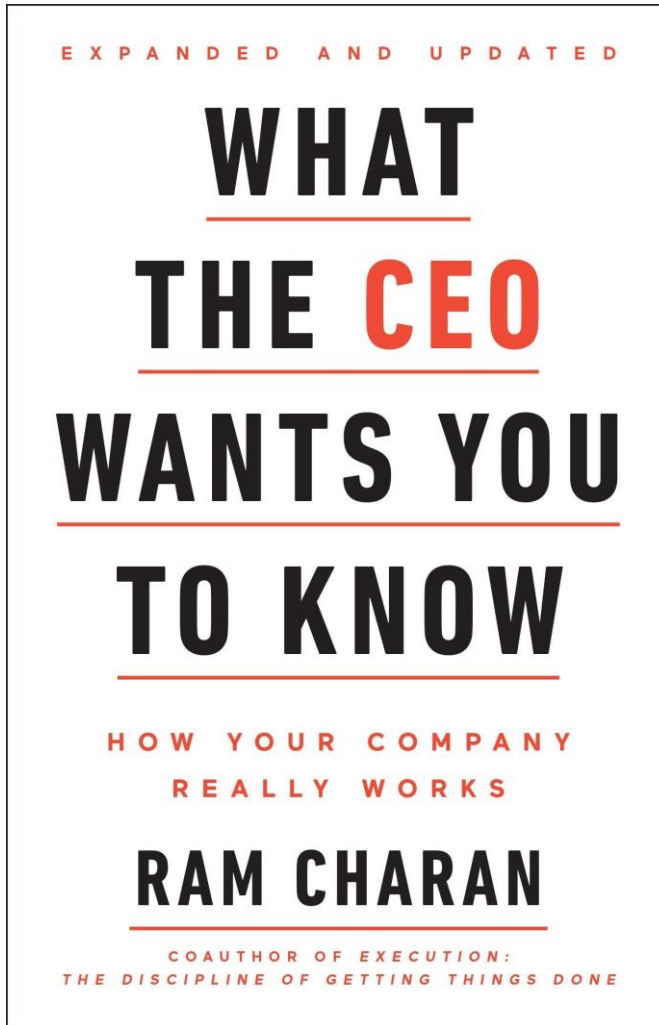
What to Do

- Determine what ERM means for ***your company*** (true enterprise-wide risk management? Or just maintaining a “risk register” for auditors?)
- Remember the Guiding Principles –
 - Perfect is the enemy of good
 - Business processes (not technology!) are the primary assets
 - Qualitative first, then quantitative
- Define your Services first, then Organizational Model, and finally the Engagement Model

(and Not to Do)

- Don't start with a “risk register” Remember, a risk register is only a tracking tool and not the ERM program itself :-)
- Don't try to solve everything together (pick low-effort business risks first. Establish processes that work for your company)
- Don't get hung up on scoring methodologies or risk management frameworks for the first year
- **Don't start without an executive sponsor who can help you drive organization-wide change.** Ideally, the Company's General Counsel is best suited for this role (Lawyers understand enterprise risk best – though some do have a tendency to make the bad news “go away”).

Some Books that I Personally Found Helpful





Q&A / Open Discussion