ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Hybrid Approach to IT Risk Management, Mix of Top-Down and Bottom-Up Strategies

Pranith Shetty

Information Security and Risk Lead, Cisco, New Jersey, US

ABSTRACT

Risk management framework and approach was and still is under developed in many firms, with things being kept mostly operational as BAU (Business as usual) in this domain. There is a massive need for maturing the overall Risk management approach, Risk management teams and firms relied and still rely heavily on risk assessments to evaluate their Risk posture. Risk assessments themselves come with baggage and dependencies, to run it like a well-oiled machine takes time, resources, effort and collaboration. This article firstly describes the rationale for the Hybrid approach, building towards this concept and the key pillars needed to support this concept, goes on to detail what the approaches or pillars are and how its drawn out in various firms.

In addition, this article sheds some light on positives and shortcomings of both those approaches when conducted individually, however, when both these approaches are combined organically the results are very much in favor of the firm's overall benefit, while risk assessments gets us granular details and more context its limiting in terms of overall resources and time spend.

***Corresponding author**

Pranith Shetty, Information Security and Risk Lead, Cisco, New Jersey, US.

Received: May 02, 2022; **Accepted:** May 10, 2022, **Published:** May 19, 2022

Keywords: Hybrid approach, Top-down approach, Bottom-up approach, Risk Assessments, Risk management

Introduction

Prior to doing a deep dive on this topic, it's important to understand Risk in this article's context?, risk is a very broadly used term, there are many variations of this term, its widely used and popular across varied areas of research, business and technology. And as a result, perceptions and different ideas are constantly surrounding this term.

As per NIST definitions, Risk is defined as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. On the same vein, Risk Management is the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system [1,2].

Rationale for this Study

Now that we have the definitions out of the way, let's look at the rationale behind coming up with a new strategy, organizations and firms around the world are trying to get a grip on their risk management strategies, some are working towards either maturing their already existing framework while some are starting from a baseline or scratch where they don't have an operating program, various frameworks and approaches are being considered. The most popular approach in the risk management domain is what risk practioners call as Risk assessments it's also referred to as the Bottom-up approach in some context and organizations, this involves undertaking risk assessments by dedicated risk managers or teams, interviewing stakeholders, qualitative analysis etc. This process is very time consuming and labor intensive thus putting a lot of pressure on everyone involved with respect to use of resources (mainly time and effort). More than the risk assessors, the assessees are overstretched, usually it's the engineering teams being on the hook, they have to spend time through these assessments in addition to their usual workload of engineering products and supporting them across customer portfolio.

The Hybrid approach is a combination of Bottom-up and Top-down where top down is a result of meetings and collaboration with various assessment teams across higher lines of defense residing in second, third and fourth line. This approach helps leveraging already existing control gap information collected by those afore mentioned assessment teams thus saving some time and effort on the assessors and assessees. Apart from saving time and effort, this method is also comprehensive in assessing the risk posture, ensuring we are covering all bases, we will be getting different perspectives and results into our analysis as well. However, it's not wise to rely on just top-down reports and findings since the risk teams might not have context, less control on scoping exercises, loses a sense of purpose for team's existence as well

Literature Review

As per John, there are many reasons why IT risk assessments fail and it is worth investigating those reasons and understanding the

true rationale since risk assessments are the basis of bottom up approach [3].

As per Tony No formalized process, poor timing of risk assessments are few of the major contributors to failure of risk assessments [4].

As per several independent research studies similar to this article here stakeholder teams and engineering teams do not like Risk assessments, more often than not they feel it's a waste of time and should be avoided, if possible [5].

Methods

As mentioned in the earlier section 1, Hybrid approach is a combination of Bottom-up and Top-down approaches, prior to designing and implementing this strategy, it's important to understand the Organizational context and be flexible in adapting these approaches [6].

Let's dive a little bit into, what we mean by the bottom up approach:

Bottom-Up Approach

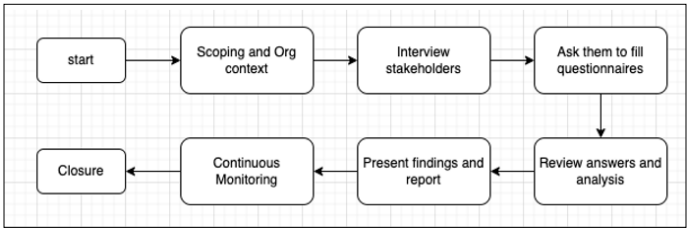

Figure 1: Bottom-Up Approach

As a Risk manager or an analyst in the risk teams working hand in glove with the engineering teams in our business unit or organization, Bottom-up approach here is intended to start with risk assessing our own teams who appear to be in the bottom most layer, meaning conducting risk assessments on staff who are responsible and accountable for products.

This ensures that the information received through these risk assessments are comprehensive and accurate to an extent.

a) As a Risk Manager/Lead, we would start with organizational context, learning or aligning with the firm's risk parameters around Risk Appetite, tolerance and other details that would be helpful to guide the risk teams and the owners.
b) Interviewing stakeholders would come next where Risk teams would get more context and introduce questionnaires on various control areas and critical processes
c) Questionnaires would be sent out to the assessees to get detailed information on the operating environment and to understand the risks.
d) Risk team would then collect those questionnaires and conduct a review/analysis to categorize and risk rate the findings.
e) The report with observations/findings would then be presented to the Accountable executives and senior leadership for response and next steps.
f) Risk teams would then work with the risk owning teams on mitigations and will continuously monitor the environment through frequent syncs and meetings until the next Assessment.

Top-Down Approach

To understand Top-down approach, we need to get a clear understanding of various lines of defense starting with first, Second, Third and Fourth line.

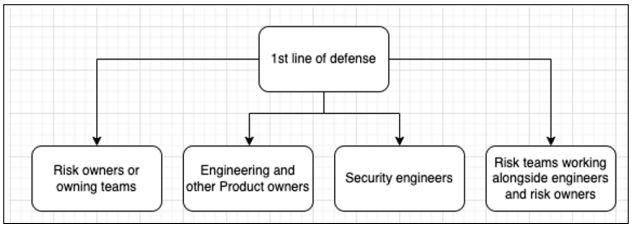

Figure 2: First Line of Defense

First line of defense: First line meaning these teams spring into action in the event of a cybersecurity threat and always first in line of action, As described in the figure 2. above, This group includes the Risk owning team(s), accountable engineering and product design teams that have designed and developed products and or services for their customers and clients, could also include system or service owners who are answerable to stakeholders in the event of system/service failures [7,8].

Security engineering teams like the Vulnerability, Incident management teams, BC/DR teams are also part of first line of defense since they have an active role in keeping systems online, ensuring customer coverage, product enhancements etc.

In some cases, like in the financial services sector there are risk teams that operate in first line working directly with engineering teams, advising them, consulting them, these risk teams don't conduct risk assessments but participate in Control self-assessments run by second line, mainly operational risk teams which are explained in the coming sub section as described in Figure 3 below. Control self-assessments are very similar to risk assessments but they are more directed towards control gaps and compliance to certain standard.

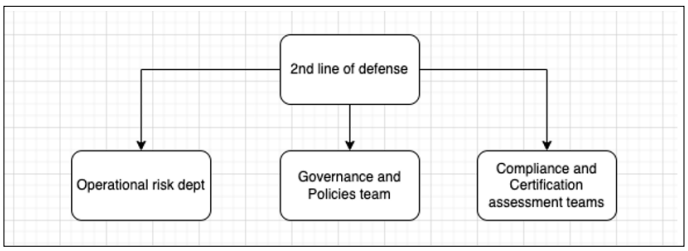

Figure 3: Second Line of Defense

Second Line of Defense

This group is mainly the group that oversees the first line and ensures they are in compliance at a high level with firstly the organization's policy and procedures, important thing to note here is this is not the assessment arm of second line, furthermore, they meet the overarching government and various governing body regulations. It consists of the operational risk department who formally operate the governance forums ensuring risks are being reported, responded by senior management personnel, the Governance and Policies team are responsible for ensuring there is policy coverage across the operating environment, and that the policies are kept updated with version history. The Compliance and certification assessment teams on the other hand assess teams within the firm to ensure teams are following the prescribed policies and procedures.

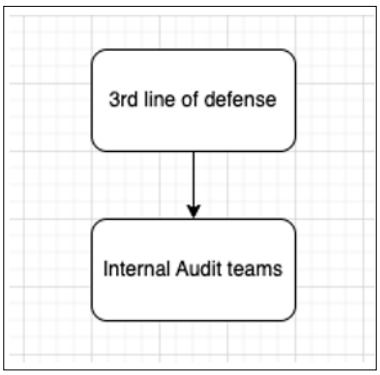

Figure 4: Third Line of Defense

Third line of Defense

Is mainly the Independent Audit arm of any organization, these teams report their observations and findings directly to the board for the sake of complete transparency and ensuring oversight from Senior leadership, this also ensure other teams to be proactive on various security related risks that could go on to impact the firm in the foreseeable future and also the risks that are being currently on track for mitigation. This team has complete control on their assessments and operate independently without any coercion or inputs. These audits or assessments take priority over other assessments with the exception of fourth line related investigations that take the highest precedence.

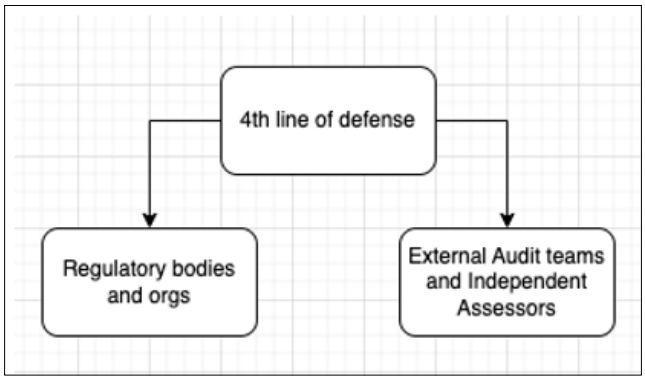

Figure 5: Fourth Line of Defense

Fourth Line of Defense: This group mainly consists of External Auditors or regulatory bodies that operate outside the organization, for example – Big 4 accounting and advisory firms that are brought in for various engagements operate in this line to provide independent reports to meet financial regulatory obligations, sometimes these firms are auditing to ensure compliance with a 3rd party certification framework like SOC2 or ISO, these firms could very well test compliance for Government specific standards if permitted by the federal authorities (For example FedRamp and other state ramp certifications).

There are various regulatory bodies like SEC, FINRA and many more that conduct investigations or random audits for different reasons. Assessments conducted by these firms are of very high priority and precede over any other audits since time is of essence for evidence submission thus in the event of overlap with internal audits, all resources are directed towards 4th line assessments.

Now that we have dived a bit further into understanding first, second, Third and fourth line of defense, please find below the detailed visual of Top-down approach in figure 6, Risk teams in this approach instead of leveraging the engineering teams and various other groups in First line which would in a way be termed as the bottom most layer, they would work with groups in higher layers or top layers like 2nd, 3rd lines of defense and in some rare cases 4th line of defense especially if they are 3rd party auditors.

Its best to draw a RACI first between these teams to ensure lines are drawn across roles and responsibilities so that there is no overlap in functional coverage across the firm. Once RACI is finalized, then based on agreements, Risk teams would obtain reports or some form of predefined and agreed form of observations or findings, leveraging assessments performed by those teams in 2nd, 3rd line et al. Analysis needs to be performed to ensure findings are aligned with the Risk management framework and are entered in the register making sure there are no duplicate entries.

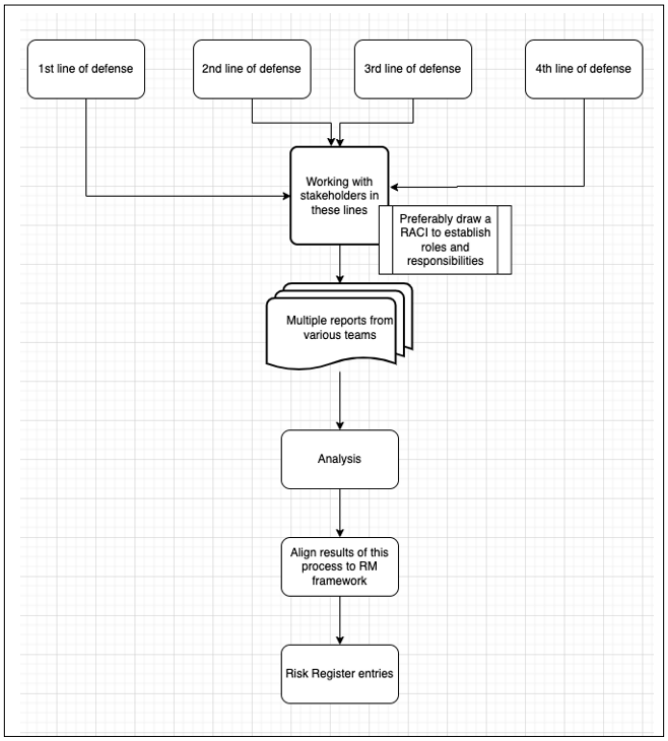

Figure 6: Top Down Approach

Hybrid Approach

Hybrid approach is an adaptable combination of both Bottom-up and Top-down approaches, while Bottom up leverages the responsible and accountable teams, gets granular and close to accurate information on the risk sources, challenges, resourcing constraints etc., the Top-down approach intends to leverage the assessments already conducted by the various assessment teams in 1st to 4th line of defense as described in the earlier sections [references]

Adaptable here meaning "to be flexible" based on the organization structure, context, relationships built with various teams in security, assessments and engineering.

The key essence here is to collect information from risk assessments as much as we (risk teams) can and ensuring the teams are not stretched in terms of commitments, time and resources, on the other hand working with higher governance related assessment teams, leveraging their report and findings, getting in different perspectives while populating the risk register and generating a detailed risk report for Senior management.

Results & Discussion

The hybrid approach is a tried and tested approach, I along with my team members have been successful in designing and implementing this across our business unit with the review and support system offered by my line management plus Senior leaders. We had conducted risk assessments (Bottom-up) driven by us across an offer/product, interview stakeholders about their critical processes and systems leveraging the process and framework that was already existing, while for some product teams that span across geographical locations, and that lacked a preexisting framework, conducting assessments was very challenging with the amount of time and resources we as a risk team had. In this case, we were able to leverage risk reports, findings from various assessments conducted by different central security and compliance teams, in other words Top-down approach. Their reports gave us insight into the control gaps, potential security related shortcomings and more. However, leveraging just these reports won't give a risk team an edge since they don't have their own findings or context to understand the risk posture of the organization so it's very important to perform risk assessments wherever you can.

The key point here is that the Hybrid approach which is a mix of both has to be balanced ensuring no duplicates, stakeholder expectations managed and a good relationship of trust with various governance and security teams

Not only technology firms some financial firms; I have had the experience of working in or interacting with have a similar structure in place where it's not explicitly called out as Hybrid approach but observing the governance process and risk registers would give us an idea as Risk professionals, all findings and assessments are taken into consideration while populating risk registers. Predefined cadence based or monthly governance forums do hear from both assessors and assessees on the latest thus ensuring a holistic risk posture presentation to Senior leadership.

The approach can very well be adopted by different firms spanning across technology, financial services, manufacturing et al.

Conclusion

Combining the best of both approaches i:e Top-down and Bottom-up process ensures comprehensive coverage of risk management lifecycle that is Identification, analysis to reporting this enables not only the risk teams and other teams involved but Management and Senior leadership to make the right decisions based on Risk posture of their products/services.

The top down approach as we can see provides us with inputs from accountable teams indirectly via other assessment teams, this saves time and effort of Risk teams in first line especially if they are short of time and resources, also builds in trust and faith with other assessment teams. However, this alone cannot help the organization since the first-hand account of inputs from engineering are missing and Risk management framework might not have been adopted by those assessment teams.

The bottom-up approach performing our own risk assessments gets us the context and details however it's not feasible when the risk teams are short staffed or product teams are spanned out and busy on multiple fronts, time and resources are very critical in these operations.

Hybrid approach when adopted as per organization dynamics and requirements can provide the most accurate in depth and high level visual of the Risk posture.

References

1. NIST. Information security risk - Glossary | CSRC. csrc.nist.gov https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.
2. NIST. Risk management - Glossary | CSRC. csrc.nist.gov https://csrc.nist.gov/glossary/term/risk_management.
3. John Kronick (2022) Why Do IT Risk Assessments Fail?. GRC Outlook https://grcoutlook.com/why-do-it-risk-assessments-fail/#:~:text=Risk%20assessment%20training%20played%20a.
4. Tony Ferraro (2014) 5 Most Common Reasons Why Risk Assessments Fail. Creative Safety Supply Blog https://blog.creativesafetysupply.com/5-most-common-reasons-why-risk-assessments-fail/.
5. M Sobba (2021) Are you tired of doing Risk Assessments?. https://strunkaccess.com/are-you-tired-of-doing-risk-assessments-for-your-bank/
6. E Marsden (2017) The ISO 31000 standard: Risk management: principles and guidelines. Risk Engineering https://risk-engineering.org/ISO-31000-risk-management/
7. Amelia Ho (2018) Roles of Three Lines of Defense for Information Security and Governance. ISACA https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance.
8. IANS Faculty (2022) How to Apply the Three Lines of Defense. IANS https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/01/13/how-to-apply-the-three-lines-of-defense.